2012

Security awareness by online banking users in Western Australian of phishing attacks

Nattakant Utakrit
Edith Cowan University

Edith Cowan University

Copyright Warning

Security Awareness by

Online Banking Users in Western Australian of Phishing Attacks

by

Nattakant Utakrit BBA, M. Info Sec

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor of Information Technology

Faculty of Computing, Health and Science,

Edith Cowan University,

Mount Lawley Campus

23rd February, 2012

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

ABSTRACT

Phishing involves sending e-mails pretending to be from the legitimate financial institutions to recipients and asking for personal information such as username and password. It also redirects network traffic to malicious sites, deny network traffic to web services, and modify protection mechanisms in the targeted computer systems. Consequences of successful attacks can include identity and financial losses, and unauthorised information disclosure.

The purpose of this study was to investigate the experiences of Western Australian bank users in using online banking. The study considered the relationship between the background of the Western Australian bank users and their experience in using online banking security. The research analysed phishing through case studies that highlighted some of the experiences of phishing attacks and how to deal with the problems. Emphasis was placed on knowledge of phishing and threats and how they were actually implemented, or may be used, in undermining the security of users' online banking services. The preferences and perspectives of Western Australian bank users about the deployment of online banking security protection and about future online banking services, in order to safeguard themselves against phishing attacks, are presented. The aim was to assist such Australian bank users through exploring potential solutions and making recommendations arising from this study.

Research respondents had positive attitudes towards using online banking. Overall, they were satisfied with the security protection offered by their banks. However, although they believed that they had adequate knowledge of phishing and other online banking threats, their awareness of phishing attacks was not sufficient to protect themselves. Essentially, the respondents who had experienced a phishing attack believed it was due to weak security offered by their banks, rather than understanding that they needed more knowledge about security protection of their personal computers.

Further education is required if users are to become fully aware of the need for security within their personal online banking.

COPYRIGHT AND ACCESS DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;
(ii) Contain any material previously published or written by another person except where due reference is made in the text; or
(iii) Contain any defamatory material; or
(iv) Contain any data that has not been collected in a manner consistent with ethics approval.

I also grant permission for the Library at Edith Cowan University to make duplicate copies of my thesis as required.

Student signature

Date 23/2/2012

Principal supervisor signature

Date 23/2/2012

Associate supervisor signature

Date 23/2/2012

ACKNOWLEDGEMENT

There are many people who have contributed to the success of this thesis.

Grateful thanks go to my Principal Supervisor, Professor Craig Valli for his patient guidance and encouragement throughout my study. My Associate Supervisor, Dr. Andrew Woodward, also made valuable comments on my thesis.

Dr. Judy Clayden, Associate Supervisor, generously helped me to organise my thesis structure and overcome some writing problems. Special thanks and intended to Dr. Tapan Rai who recommended appropriate statistical procedures and helped interpret the resultant outputs, and Dr. Greg Maguire who worked with me throughout my study to improve my writing skills. Associate Professor Dr. Peng Lam, the Doctor of Information Technology (DIT) coordinator, provided helpful advice throughout this course.

I would like to extend my thanks to 3N Oriental Australia PTY, LTD. who allowed me to interview customers outside this supermarket. Similarly, Malaga and Wanneroo weekend markets provided facilities for me to conduct my survey. Moreover, Antony Portelli, Deputy Director, Paul Galea, Academic English teacher, from the Perth Institute of Business and Technology (PIBT) for allowing me to distribute my survey in their classes.

I am indebted to Ms Natalie Woodman, Principal of Alexander Language School, Ms Suviya Kladjarern, Manager, 3N Oriental Australia Pty, Ltd. and Mr. Bosco Lin, Master of Commerce Student, University of Western Australia, for e-mailing my survey to their contacts throughout Western Australia. The resultant responses were crucial to the success of the study.

I warmly acknowledge my friends from many countries who supported and encouraged me during my research. Naturally, I am grateful to all of the research participants who provided the valuable feedback and data that enabled me to complete my thesis.

Last but not least, I expressed my deep love and respect for my parents, Associate Professor (Dr.) Sobsan Utakrit and Assistant Professor (Dr.) Pranom Utakrit, and my brother, Dr. Nattavee Utakrit, who provided so much emotional and financial support throughout my life and were role models who led me to undertake my doctoral studies.

TABLE OF CONTENTS

LISTS OF FIGURES

LISTS OF TABLES

CHAPTER 1- INTRODUCTION

1.1 The Background of the study

The Australian Bureau of Statistics (ABS) (2011) reports that 83% of Australian households had access to a computer at home in 2010-11. It explains that computer access at home is more common in higher income areas in State and Territory capitals. Figure 1 .1 shows the categories of use of the home computers in 2010-11 in Australia.

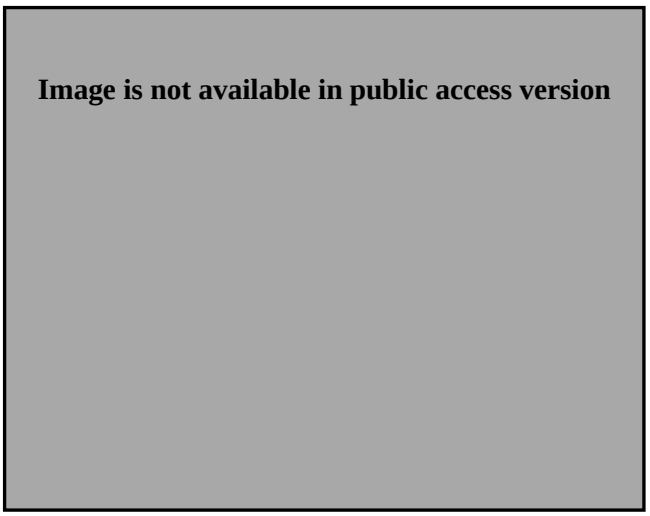


Figure1.1 Personal internet use at home, by activity (a), 2010-11
(Australian Bureau of Statistics, 2011)

Of the 13.3 million people who reported accessing the internet at home, paying bills online or online banking was the third most common activity (Australian Bureau of Statistics, 2011). This spread of home computer ownership has meant that businesses, especially banks and financial institutions which wish to reduce the need for direct customer interaction with staff, have used the Internet to develop services and provide cost effective online banking systems. Banking organisations are not only trying to support customers' online transactions and gain new customers, but also to protect them while they operate in the cyber world (Singer, Baradwaj, Flaherty, & Rugemer, 2012). Even if online banking and other services have been introduced to make customers' lives and businesses' continuity more secure, threats to online banking are still common (Anti-Phishing Working Group, 2010a).

1.2 The significance of the study

The Internet has become one of the common attack channels that criminals use to gather valuable assets, such as customer details and confidential bank information, in order to paralyse online businesses and Internet users by using simple social engineering attacks (Anti-Phishing Working Group, 2007). One of the main concerns is identity theft; while customers are online, criminals may try to gain sensitive information and use it to attack individuals and organisations. Types of attacks include social engineering, spreading malware, and phishing. (More specific definitions of these terms will be provided in Chapter 2).

While engaging in transactions on the Internet may seem to be private matters between senders and receivers, eavesdroppers might be listening to the communications. Breaches of privacy and access to confidential information may take place without users' awareness or consent. Inexperienced users may not be aware that they are liable to attack if they have not implemented adequate security measures. Recognition of the need for up-to-date security measures is an essential component of any self-protection undertaken by government, businesses and individuals.

1.2.1 Where is the phishing targeted?

Phishers deceive online users or mislead users with different techniques to gain unauthorised information with the purpose of stealing money. A detailed explanation of phishing techniques is provided in the second chapter of this thesis. The extent of phishing has increased due to the availability online of phishing tools and free hosting services, thus it is causing large losses for companies and customers (James, 2008). Phishing has become the most common threat to Internet users and web services. Martin Brinkman's blog (2012) shares the security company Avira's list of brands which experienced the most phishing attacks in 2009. It is significant that banks and other financial services, such as eBay and PayPal, were the most heavily targeted. Two Australian banks, the Commonwealth Bank and the National Australia Bank, are included in the list, as are international banks operating in Australia, such as HSBC and Citibank (Brinkmann, 2009).

Phishing attacks have increased in almost every industry all over the world. Statistics about the numbers of phishing attacks in particular countries are difficult to estimate beyond the fact that they have been increasing. A report from Symantec in 2010 shows the statistics of country of targeted brand industries in logarithmic scale as shown in figure 1.2.1.

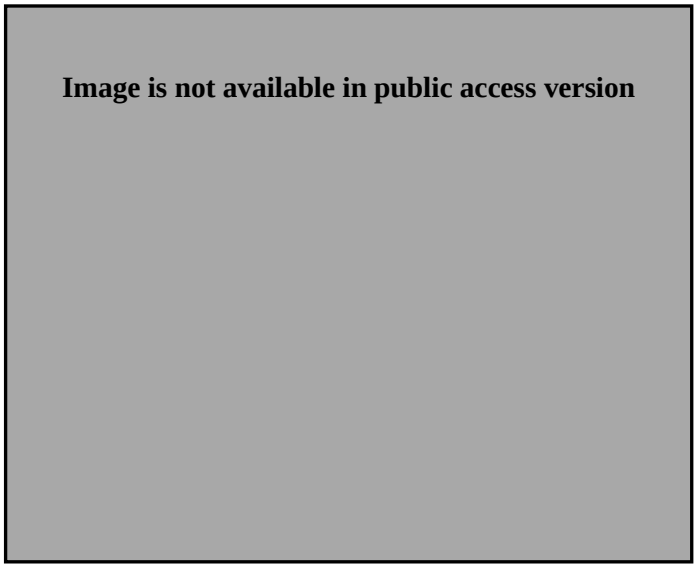


Figure 1.2.1 Numbers and types of phishing attacks per country in 2010
(Symantec, 2010)

The brand industries that phishing sites spoofed were categorised based on the country where the brand's parent company is based (Symantec, 2010). As appears in the graph, the major target of phishing attacks was banking, spread throughout all countries except China where e-commerce was a primary target and banking seemed not to appear in any sector. Organisations targeted in Australia were banks, other institutions not often being attacked.

In the United States, Gartner Inc.'s survey found that more than 4,500 online US adults, representative of the online US adult population in August 2007, lost money to the successful attacks by $3.2 billion (Gartner, 2007). "Of consumers who received phishing e-mails in 2007, 3.3% say they lost money because of the attack, compared with 2.3% who lost money in 2006, and 2.9% who did so in 2005, according to similar Gartner surveys during those years" (Gartner, 2007). Similarly in the United Kingdom,

the amount of money lost and damage caused by phishing activities rose by 14%; criminals targeting victims from the Internet banking systems (Bachelor, 2010). This increase has not been seen only in the larger countries like the US or the UK. Many Australian national banks, such as the Commonwealth Bank and the ANZ Bank, have suffered the impacts from phishing attacks when the phishers have targeted customers via the Netbanking service (Sharma, 2010). The Anti-Phishing Working Group (2010b), figure 1.2.2, reported that the percentage of computers infected (unstated the district) with banking Trojans and password stealers, in other words desktop crimeware, increased to 17.58% in quarter 2 from 15% in quarter 1 of 2010. The percentage of downloader activities rose from under 8.3% to almost 8.4 % in quarter 2, whilst malware infection was the top phishing activity at 74.05%.

Figure 1.2.2 Percentages of desktop crimeware infections cause by phishing attacks in quarter 2 in 2010 (Anti-Phishing Working Group, 2010b)

1.3 Aims and research questions

It is essential for online businesses, banks and financial institutions to develop secure systems to protect their millions of online users worldwide from unwanted risks and breaches of the confidentiality of users' information. However, responsible bank customers who are aware of the dangers are able to contribute to their own security.

The major aim of this research is to analyse the extent to which Western Australian people who use online banking and conduct online financial transactions are aware of the dangers associated with phishing attacks. An evaluation of their knowledge about such crimes may enable the subsequent publication of advice which will help many to avoid financial loss and the effects of identity theft. More specifically, this research aims to investigate the

(i) experiences of Western Australian bank users in using online banking,

(ii) relationship between the background of Western Australian bank users and their experience in using online banking security,

(iii) users' understanding of phishing attacks and effective countermeasures,

(iv) preferences of Western Australian bank users in the deployment of online banking security protection,

(v) perceptions of Western Australian bank users about future online banking and to determine what they would prefer from banking services in order to safeguard themselves against phishing attacks.

This study therefore aims to answer the following research questions:

1. What are the factors which lead people to use online banking?
2. What are users' opinions of online banking systems?
   2.1 What are users' opinions about the available online banking authentication systems?
3. Are users of online banking taking adequate steps to secure their online transactions?
4. What levels of knowledge do users of online banking have about phishing?
   4.1 Do bank customers believe that banks are taking adequate steps to prevent phishing attacks?
   4.2 What could be the vulnerable point that leads online banking users into phishing attacks?
   4.3 Do users have enough knowledge to be able to distinguish a legitimate bank's e-mail and website from a fraudulent one?

1.4 Organisation of this thesis

This thesis is divided into six chapters:

Chapter 1 presents the background, significance and purpose of this study. This chapter also identifies the research questions.

Chapter 2 will include a review of the relevant research literature, which outline the theoretical underpinnings of online banking and phishing, current issues associated with phishing, and phishing techniques that could attack banks' users.

Chapter 3 will outline the research method and research design used to conduct this study.

Chapter 4 will present the analysis of collected data from the survey.

Chapter 5 will comprise of the analysis of the data in the context of the primary and supporting research questions, leading into the recommendation of the findings based on their research questions.

Chapter 6 will consist of the concluding of the research and the potential for further research.

CHAPTER 2 - LITERATURE REVIEW

2.1 Introduction

This literature review aims to define the terminology associated with malicious attacks on online banking systems, specifically phishing attacks. It will evaluate the literature about such attacks, without being restricted to any specific locations. It will also consider various means by which attacks may be delivered to the laptops and telephones belonging to customers of online banking. Finally it will examine the literature which analyses customers' awareness of means by which they may protect themselves against identity theft and financial loss. Ways in which banks may assist customers to broaden their awareness of protective measures will be detailed.

2.2 Defining online transaction and activities including online banking threats

This section discusses terms and definitions of online banking transactions and activities, online banking threats and other related terminology.

2.2.1 Online transaction activities

Some common terms are used quite often in association with online transactions, such as e-business, e-commerce, e-payment, e-banking and online banking; the differences between them are clarified below:

Electronic business (e-business) describes the activities when technology is involved in business processes (Northern Territory Government of Australia, 2012). E-business includes sending e-mails to staff or suppliers ("Understanding E-business," n.d.), performing online transactions, using internet based interactions for selling goods to consumers, monitoring and exchanging information, auctioning surplus inventory and collaborative product design ("E-business versus e-commerce," 2012).

Electronic payment (e-payment) refers to the automated process of exchanging monetary value among parties in business transactions and transmitting this value over

the information and communication technology (ICT) networks (Ayo & Ukpere, 2010). It is a system in which financial information can be held, processed, received, and transferred in a digital form. It consists of users, issuers such as banks and financial institutions, and regulators who are involved in its potential impact on the wider economy via monetary instruments. However, "E-payment may be treated as a protocol among the payer, the payee and their respective Financial Institutions (FIs)" (Raja, velmurgan, & Seetharaman, 2008, p. 6). Examples of e-payments such that electronic cash, electronic check, electronic traveller's check (Wang, Yang, & Paik, 2011), secure electronic transactions (SET), secure socket layer (SSL), and modern credit card transactions (Raja, et al., 2008).

Electronic commerce (e-commerce) is defined as transaction activities between firms and individuals which involve in the exchange of money, good or duties (M. Hasan & Harris, 2009). It involves online transactions such as shipping, billing and payment information. E-commerce is a partnership of consumers as payers, merchants as payees and their respective financial institutions (Raja, et al., 2008).

Electronic banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic and interactive communication channels (Salehi & Alipour, 2010). E-banking includes telephone banking, NetBank (Internet Banking), mobile phone applications, BPAY and BPAY view, ATM, Debit MasterCard, key card (debit card), EFTPOS terminals, Maestro/Cirrus, MasterCard and Visa Plus networks, AFT (Automated Funds Transfer), and Deal direct (Commonwealth Bank of Australia, 2011).

Online-banking or Internet-banking is used for a new age banking system with the internet technology as a delivery channel to conduct banking activities (Singhal & Padhmanabhan, 2008). The system supports customers who prefer to manage their finances, such as money transfers, bill payments, personal information updating, and balance checking via the Internet, from anywhere, and at any time when that access is available. This service is becoming more helpful because bank branches alone are no

longer able to offer services to meet the needs of today's highly demanding and challenging customers (Bradley & Stewart, 2003 cited by Qureshi, Zafar, & Khan, 2008).

2.2.2 Online banking threats

The following threats are claimed in association with online transactions, such as e-business, e-commerce, e-payment, and online banking; the differences between them are clarified below:

Phishing is a jargon, another type of scam. It comes from the analogy that Internet scammers use e-mails to 'fish' Internet user for personal identity (Anti-Phishing Working Group, n.d.). Phishing may have developed its tactics from money laundering based on electronic transfers. The process of transferring funds through electronic messages between banks is known as wire transfers and was first declared as a crime under the Money Laundering Control Act of 1986 of the U.S. Code (Raja, et al., 2008). Phishing employs social engineering and subterfuge techniques to steal consumers' personal identity and financial account credentials (Anti-Phishing Working Group, 2007). It also refers to an act of an Internet swindler who uses e-mails to lure Internet users by asking for password and financial data. Phisher may also send a SMS to consumers which seems to come from legitimate businesses, normal banks or other financial institutions or telecommunications providers (Commonwealth of Australia, 2012).

Malware is a term for any malicious software which enters system without user or system authorisation (Vinod, Laxmi, & Gaur, 2009). It can also be defined as a software that is harmful to other software and possibly and indirectly control other hardware by (affected) driver application (Kramer & Bradfield, 2010). It is designed to infiltrate a computer system without an owner's informed consent (Queensland. Department of Education, Training and Employment Policy and Procedure, 2012). Malware has ability to infect other executable codes, files, boot partitions of drives. Malware can modify data, disclose confidential information, monitor and transfer user's

information to the software sender. Malware includes Trojans, adware, spyware, rootkit, virus, worm, botnet and backdoor. All these terms are defined in the Appendix A.

Social engineering definitions can be drawn upon several social psychological aspects. According to Kessem (2012) claims social engineering is involved with a route of persuasion as below:

- A central route to persuasion, which involves the recipient thinking about the message.
- And a peripheral route to persuasion, relying on superficial clues within a message to get a person to purposefully not think - but rather react emotionally and react immediately.
- Again, neither is new. That peripheral route to persuasion has been and still is, vastly used in confidence scams and in telemarketing fraud.

It also means an art of persuasion (Mosin Hasan, Prajapati, & Vohara, 2010) that allows an attacker to detour technical controls and attack human in an organisation (Major, 2009). Some common techniques used in social engineering include: persuasion, reverse social engineering, shoulder surfing, dumpster diving, phishing e-mail, and phone phishing. It can be summed up that the concept of social engineering is an attempt to elicit a victim into provides information for illicit purposes. Cyber attackers use social engineering, phishing, and malware to commit online crimes especially in online banking services with the purposes of identity fraud and money transferring. The issue of online banking attack is becoming more serious to financial institutions and their customers.

2.3 Current issues of the exploited vulnerabilities in online banking

Going to a branch or ATM or paying bills by paper cheques, mailing them, and balancing a cheque book, are all time-consuming tasks. In today's world of emerging technologies, enterprises are relying more on the Internet for business. People are adapting e-commerce applications for their day-to-day needs. Meanwhile, banks and financial institutions have cost-effectively provided faster and more convenient online banking services so customers may do their business anywhere an Internet connection is accessible. It is both an opportunity and a challenge to traditional banking and has become a necessity for many customers.

2.3.1 Is bank really a target by phishers?

The numbers of phishing and malware threats attacking customers increase every year. While the picture just painted generally depicts the impact on larger financial institutions, community banks are not immune. More phishers are targeting clients because of the ease in achieving. According to a cybercrime researcher, international organised crime groups launched the first wide-scale phishing attacks in 2003 on the customers of the Commonwealth Bank of Australia, one of Australia's major banks (Sharma, 2010). Online banking services, such as Netbank, were the channels used to target the bank's customers. The attack was carried out by sending out a mass of e-mails, which attempted to persuade customers to provide their credentials. The following banks targeted by attacks were the ANZ bank in April 2003, the Bank of America in May and Westpac in July (Sharma, 2010).

The number of people who use online banking and have experience in online banking attack has increased. Australian Bureau Statistics (2010a) disclosed that in identity fraud cases in the 12 months prior to the survey, 3% or nearly half a million (499,500) people in Australia were victims of identity fraud, of whom 54% of the victims were male and 46% were female. More interestingly, just over 800,000 Australians aged 15 years and over, which equated to 5% of the population, were victims of at least one incident of personal fraud in the 12 months (Australian Bureau Statistics, 2010a).

The fraudulent e-mails and websites that created by phishers are intended to deceive users into disclosing personal information (Mell, Kent, & Nusbaum, 2005). Information such as user names, passwords, social identification, credit card details, bank accounts, and date of birth are the personal identity details frequently sought by phishers. Phishers can also install malware and attacker tools to detect users' computer and mobile devices for data recording and unknowing of data transferring and send it back to the senders. These stolen identities may also be used to commit further crimes; for instance, they may enable phishers to avoid being caught by the police if they use the stolen identity as a suspected perpetrator during illegal activities.

Cyber criminals attempt to bypass the security measures employed by the bank and aim to attack the banks' customers instead because they are an easy target which could be compromised easily. The technique used is often a social engineering attack that is used to trick people to reveal confidential information. Users' computers were infected with malware every 20 minutes, in which each of the infected computers hosted 3.5 threats; these were defined mainly as actual malware or clues that a successful attack had been launched against the machine (Keizer, 2011). In addition, Keizer (2011) mentioned that Java-based exploits were one of the top 10 threats which created vulnerability in users' computers. Not only financial services staffs have experience of phishing attacks, end users also have more chances to get attacked from phishing. The research found that 7% of victims that were compromised the website was used for e-merchant purposes (Piscitello, 2011). In addition, Security Week News ("ZeuS-Style Attacks Trump Phishing as Greatest Threat to Online Banking," 2010) revealed a survey which was conducted in November 2010, included responses from financial services professionals at more than 70 banks about greatest threat to online banking that:

Real-time attacks from online banking Trojans (ZeuS, Clampi, etc), also referred to as man-in-the-middle attacks, are seen as the greatest threat to online banking today for more than half (51%) of survey respondents, and 69% indicated an increase in the frequency of these attacks over the last 12 months. In fact, 37% of respondents or one-third of data stealing were attacked by Trojans (Phifer, 2010) which was the most prevalent type of online banking attack. The following threats were worms, phone frauds, diallers, and other forms of malicious codes (Phifer, 2010).

The above information is showing that more than one attack method was successful in compromising or accessing online banking service illegally. Phishing e-mails may not only mimic themselves to unidentical look to bank' e-mails and ask customer's information but also attach malicious codes or malware to silently install in user's computer if they open the infected e-mail besides. Some of the common threats were discussed as they were part of the interview question. Also, it shows the significant of phishing threats to online banking users. More details about threats that

are associated with online banking attack on the client side are discussed below.

2.4 How users get attacked by phishers?

There are many types of phishing attacks. Even though the forms may vary, the purpose of the attack is the same. The following paragraphs describe some common techniques of phishing that could harm online banking users.

2.4.1 Phishing e-mails

"According to McAfee, 95 percent of phishing e-mails pretend to be from Amazon, eBay, or banks. Targets can also be seasonal (e.g., IRS) or capitalize upon social trends (e.g., Facebook)" (Phifer, 2010). Phishing e-mail uses social engineering techniques to compromise recipients with interesting or fear-causing subject lines or e-mail content, for example password disclosed, money lost, or work from home and get $200 a day (Nattakant Utakrit, 2008). Other common motivators and emotional e-mail subjects include tax refunds, greetings from lottery winnings and 419-scam deals, false accusations from tax frauds, curiosity searching people, fake order confirmations from online merchants or shopping sites, fake e-mails from banks and financial institutions (Kessem, 2012).

Recently, the American Banker Association reported that an online miscreant used automated diallers, text messages and e-mail to lure bank's customers into entering their credit card information due to the fraud alert closed account (Moscaritolo, 2012). Recipients may respond to the sender with the required information because of fear or interest. As soon as e-mail addresses have been obtained, phishers may use communication channels such as e-mail, instant messaging, and web page to launch the phishing attacks by using social engineering technique. The phishers must impersonate their victims by using trusted sources such as the help desk of banks or automated support responses from the victims' favourite online retailers in order to create credibility for the forged messages.

2.4.1.1 Spoof E-mails with false senders

Spoof e-mail is one of the common techniques. E-mail pretends to come from a legitimate bank or someone the recipient knows, informs recipients pretended to be an e-mail alert of someone has left a message or in the guise of confirmation notification (GMA Network Inc., 2012). E-mail content asks the user to identify their status with user's account number, pin number, or credit card number through the friendly automated bank's operation system. Trend Micro reported ways that fake messages use sender addresses which appear legitimate starting with *confirm@...* or *noreply@...*,for example (GMA Network Inc., 2012). Cases in which e-mail addresses are adjusted, they may be either modified via the top level domain (eg., from .com to .net) or by adding an additional letter to the user's name (eg., *abcd@abc.com* to *abcdd@abc.com*) or in an addition to changing a letter into a number or vice versa (eg., *abc@0123.com* to *abc@.O123.com*) (Financial Services Information Sharing and Analysis Center & Internet Crime Complaint Center, 2012). This spoof e-mail can cause a problem to customers if banks choose to send e-mails to contact their customers for any issues.

A case was found in 2009 when a bank's customer clicked on links within a phishing e-mail that pretended to be from the legitimate bank that customer was a member. She claimed that her bank always sent e-mails to their customers regarding a security upgrading. As a result, more than $550,000 was transferred from her account to various accounts in many countries. This crime is known as a 'wire transfer'(Financial Services Information Sharing and Analysis Center & Internet Crime Complaint Center, 2012). This incident happened even though the bank had 'two-factor authentication using digital certificates for its online banking portal', the phisher was able to circumvent bank's security measure (McGlasson, 2010).

2.4.1.2 Spoof E-mails with HTML attachment

Although the number of phishing e-mails attached with malicious attachments has been decreased (Help Net Security, 2012), yet they are still significant because of the increasing in sophisticated phishing attacks. Phishers have combined social engineering attack and malicious code to entice customers into clicking the attached file

and providing users' credentials. A new class of cyberattack is threatening e-mail that infects users' computers without openning an attachment (Cole, 2012). Users do not need to open the attached file, as soon as the e-mail is loading to open, it downloads malicious software into their computers automatically.

Help Net Security (2012) reveals the way that attackers avoid built-in phishing detection installed in customers' computer browsers by "attaching HTML version of banking websites to e-mails rather than linking victims to bogus banking sites". The spoofed webpage which is attached in the e-mails can avoid the HTTP GET, which formed as a link, to the phishing site, thus the attached file cannot be detected by the browser (Mendrez, 2011, October 4). The upper level of phishing e-mail contains a HTML e-mail attched which automatically downloads malware and stores into users' computers when the e-mail is opened (Cole, 2012). The HTML attachment may be inserted with the malicious JavaScript that exploits the customers to Trojan software to steal their information (Internet Crime Complaint Center's (IC3), 2012) or the information can be collected and sent over to the phishing's server using the HTTP Post Request method (Kulkarni, 2009).

Cole (2012) claims from a security company that uers can avoid phishing e-mails by switching all security settings in e-mails to maximum, and updating browsers to the latest versions. In fact, there are more types of phishing can attack users especially bank customers. Techniques and tools used are more sophisticated and consequence in more severe impacts. One of the most successful technique is 'man-in-the-middle attack'.

2.4.2 Man-in-the-middle attacks

Man-in-the-middle (MITM) attacks occur when an attacker acts as a gateway in the traffic stream (Callegati, Cerroni, & Ramilli, 2009) and compromises the connection between clients and legitimate servers. While performing the attacks, the attacker may monitor and record confidential information such as usernames and passwords, bank account details, or social security numbers. In addition, they can alter information or

relocate the destination of information or finance away from the user's intended site. Specific types of MITM are discussed below.

2.4.2.1 Web spoofing

Phishing attack through websites is more sophisticated than phishing e-mails. It needs various techniques and tools to induce customers into believing that they are accessing to the legitimate bank websites. This may enable phishers to record users' information more easily.

A man-in-the-middle through web spoofing claimed by Hyde (2012) where he mentions this severe attack to HSBC bank's users with a total fraud of £22.6 million in 2007, rose up to £52.5 million in 2008, £58.7 million in 2009 and £46.7 million in 2010. It resulted in 32% year-on-year fall in the first six months of 2011. Even though the bank customers had used a new 'Secure Key and Barclays' PINentry' authentication to protect crimes, a new virus was found over the ordinary anti-virus protection. The attacker sent malicious codes to masquerade as a real bank website and lure customers to participate the 'upgrade security system' training. There was no doubt for unwitting customers to get money stealth by signing in the system. This attack was discovered further once the users opened an e-mail, the hidden virus was immediate resided in their computers without opening the attached file.

This is another form of MITM in which the attacker can install malicious software known as a Trojan horse on the user's computer, monitor the victim's activity and record usernames and passwords (Wells, Hutchinson, & Pierce, 2008) from the online financial website. The Trojan horse infects a user's computer; its malicious program is installed in the browser and then waits for the browser to be opened before it begins operation. The intruder will filter the website and target the links to online banking. The attacker waits until user logs in into their account and performs money transaction in which the amount of money and the destination of the recipient can be manipulated without user consents as shown in figure 2.4.2.1 (Nattakant Utakrit, 2009).

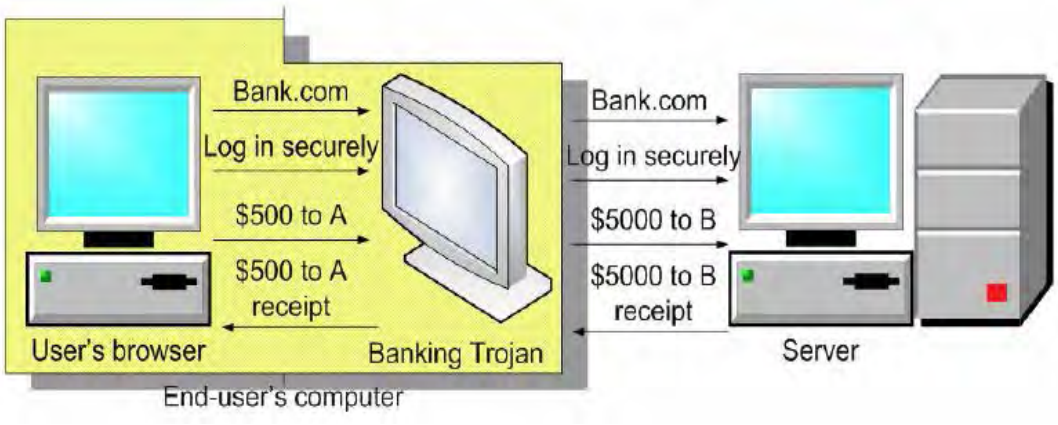


Figure 2.4.2.1 The form of man-in-the-browser attack (Nattakant Utakrit, 2009)

Another MITM attack revealed by Higgins (2012) about the phishing tool 'Zeus and SpyEye' bypassed the two-factor authentication such as SMS and withdrew funds from a victims' account without monitoring the process. This attack is called an 'automatic transfer system' (ATS) in which the attack used WebInject files to create pop-up windows and conducted a wire transfer. The attacker employed a phony login page to bypass the authentication once the log in process was achieved, and sent a message to invite the victim to participate in security training with bank's upgraded security system. The victim was asked to provide the information and make a fund transfer and confirm his transaction using the mobile confirmation code.

2.4.2.2 URL spoofing

The attackers mislead client's connection to a phishing proxy server instead of a real server. Example of URL spoofing with the spelling mistake or misplaced of a root domain can be illustrated below:

Legitimate domain = *www. moneybank.com.au*

Mimic domain example 1= *www.moneybank.au.com*

Mimic domain example 2= *www.nnoneybank.com.au*

The above example shows that the root domain of the original bank is misplaced from *.com.au* to *.au.com* in mimic domain example 1. Similarly, the word '*money*' is replaced with '*nn*' (lower-case of alphabet N is used twice). If the customers do not check the URL carefully or do not type the full domain name manually and carefully

every time they visit their bank, they may fall to phish easily. One technique that the phishers also use to lure bank customers is replacing the domain name by an IP address to hide the domain name of the visited website (Gastellier-Prevost, Granadillo, & Laurent, 2011). For instance, a URL address: *http:// 74.220.215.65* instead of *http://volleyballplayerz.com/* which is a phishing website that fakes Natwest bank site (Gastellier-Prevost, et al., 2011).

Many web browsers have included authentication information such as username and password in the domain as *URL://username:password@server/resource.ext*. Phishers may use this URL syntax to "create a hyperlink that appears to open a legitimate website but actually opens a deceptive website" (Microsoft Support, 2012) by adding @ and targeting website after the original website. In addition, this syntax can be used to automatically send username and password fields to a target organisation that supports the basic authentication method (Microsoft Support, 2012). For example, the phishers may trick customers to believe that they are visiting the legitimate '*Commbank*' website; therefore, the replacement would be, *username = commbank*, *password = e-banking*, and the target domain name is *moneyonline.com*. As a result, the entire format of the URL would be *http://commbank.com:-ebanking@moneyonline.com/*.

Another technique found in phishing attack is URL shortening. Phishers may use URL shortening service to shorten the URL which may contain malware or lead customers to the phishing sites (Gibson, 2011). For example, a URL address: *http://www.phishingyoutobanksite.com.au* has a length of 39 characters. The phishing may user TinyURL web service to shortening the characters into 26 characters as: *http://tinyurl.com/c22yn36*. By clicking the URL, customers are routed to a webpage which looks like the legitimate bank login page. URL spoofing also can be exploited by redirecting a website from an original link to a destination link, for example ***http://originalweb.com/redirect.html****?q=http://destination.fake.com/destination_page.html* became location=*http://destination.fake.com/destination_page.html*; with the redirect script. A URL redirect or URL redirection usually refers to when a web page redirects to another web page as soon as it is loaded. This technique is useful if the

content on user's page has moved to another page according to the code that use to load a page are the same. However, the attackers are successful using this technique when the victim visits a malicious webpage, or receives a malicious e-mail message (Babu, Bhaskari, & Satyanarayana, 2010).

2.4.2.3 DNS spoofing

Domain name system (DNS) is a resolution service which helps users to locate computer and other resources easily on a TCP/IP based network (Microsoft, 2011). Basically, the system host files contain domain match information to various types of data such as Internet Protocol (IP) addresses (Microsoft, 2011). When a user wants to access a website, the machine sends a request to DNS to get an IP of the particular domain. Once the request is sent to the server, it will match the pattern of the IP request with its host name in databases and sent the request back to the user's browser with readable mode of host name such as www.abcdf.com.au. DNS spoofing is performed by the attackers to make a DNS entry to point to another IP (Singh, Sharma, & Kumar, 2012). To perform a spoofing attack an attacker will introduce forged DNS information into the cache of a domain server (US-CERT, 2008). The DNS spoofing allows a router to acts a proxy DNS server and replies to any DNS queries using either the configured IP address in the IP DNS spoofing or the incoming interface for the query (Singh, et al., 2012). In other words, he or she can create obstacles to traffic routing by infusing false IP addresses into real domain names as displayed in figure 2.4.2.3. The DNS protocol contains a transaction ID of 16 bits wide requires up to 32,768 attempts to predict the ID field (US-CERT, 2008).

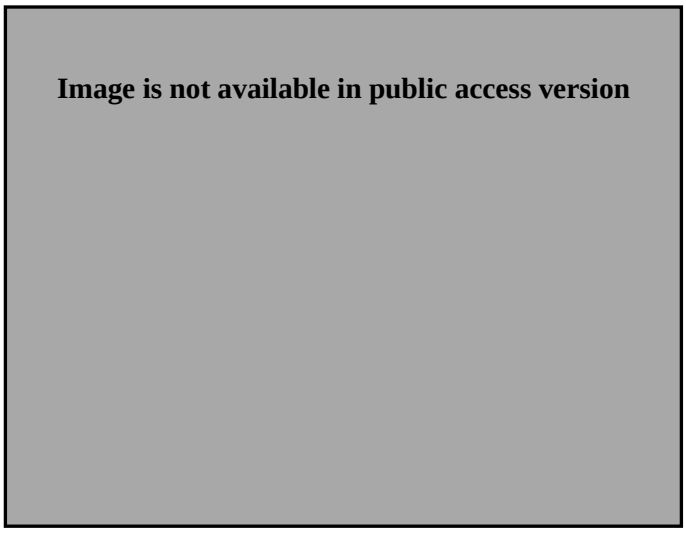


Figure 2.4.2.3 DNS cache poisoning (TCT Solutions, 2011)

DNS cache poisoning then modifies the IP address and redirects the user to the attacker server. DNS cache poisoning may cause an incorrect domain server connection and thereby a malicious attack on the clients. In addition, it may use redirect techniques to transfer the wrong traffic connection to attack the clients. Once the user's computer is controlled, the attacker can create a malicious file to embed inside the computer and start monitoring and stealing the user's confidential information.

Example of DNS attack claimed by Zorz (2012) occurred when Latin American bank customers were constantly attacked by the phishers duped the customers to download a Trojan that redirected them to the phishing sites. The phishers installed Trojan quietly contacted another domain to retrieve a Host file that was used to redirect customers to the legitimate bank sites to the phishing counterparts instead.

2.4.2.4 HTTPS spoofing

One of the challenged attacks is exploiting Hypertext Transfer Protocol Secure (HTTPS) on the address bar which tends to rate high on severity scale. HTTPS is a protocol for secure communication that adds a sub-layer of security under regular HTTP application layering through a secure socket layer (SSL) or transport layer security (TLS) protocol connection (Sharpe, 2008). Many online banking systems employ a SSL

and a transport layer security TLS protocols that use to authenticate web server and to establish a cryptographically secure channel between users' browser and the web server. HTTPS is widely-used for e-business or e-commerce websites such as eBay, Amazon, e-payment such as PayPal, and e-banking such as Internet banking. However the effectiveness of HTTPS depends on the robustness of browser or server software (Sharpe, 2008). Poor customers who rely on the HTTPS evidence (https://) may be in risk of phishing attack by providing their confidential data to a malicious website that looks similar to the real website (Kolsek, 2011). Figure 2.4.2.4, most people consider HTTPS-based (port 443) data exchange is safer that HTTP-based (port 80) because when the protocol is secure, the lock symbol (Callegati, et al., 2009) and sometimes comes with the green highlighted covered the padlock area appear in the clients' address bar. Kolsek (2011) mentioned that the spoofing URL may be noticed by the hawk-eyed if the left pad lock is grey instead of green for the valid HTTPS addresses. Also, HTTPS:// starting in the URL may less likely to notice the absence of a lock icon because the web browsers are different.

HTTPS can be compromised by the attackers in bypassing HTTPS security warning as the attackers exploit the integration of SSL/TLS into the browser and browser's presentation of security-relevant information to the user without breaking the cryptographic model (Kolsek, 2011). Online banking security's system relies on a valid certificate that initiates the SSL/TLS connection to the fact that HTTPS cryptography can secure page contents from modifications (Prandini, Ramilli, Cerroni, & Callegati, 2010). Certificate Authorities (CA) are companies that issue a variety of SSL certificates for the organisations and individuals to purchase (K. Thomas, 2011) to authenticate websites (Babu, et al., 2010; Fung & Cheung, 2010; K. Thomas, 2011). "Digital certificates are documents that combine a public key and an identity" (Seltzer, 2009, p. 9).

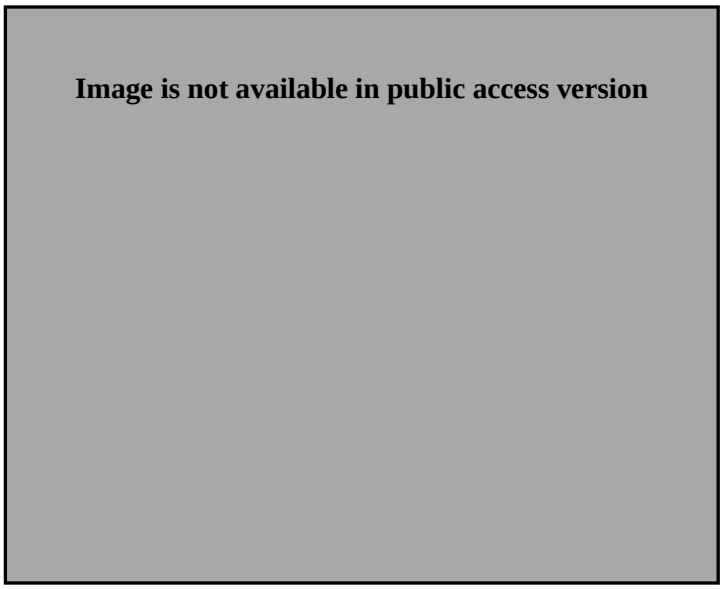


Figure 2.4.2.4 Extended validation secure socket layer differences in various web browsers (Online Trust Alliance, 2011)

Certificate Authorities (CA) are companies that issue a variety of SSL certificates for the organisations and individuals to purchase (K. Thomas, 2011) to authenticate websites (Babu, et al., 2010; Fung & Cheung, 2010; K. Thomas, 2011). "Digital certificates are documents that combine a public key and an identity" (Seltzer, 2009, p. 9). The very basic certificate is used to ensure that the company is the same one that registered the domain whereas the more rigorous certificate, which is the extended validation certificate is required to prove the physical location of the company in the real world (K. Thomas, 2011). With such a different level of CA, the organisations who use the basic certificate may fail to man-in the-middle attack. Investigations have shown that 531 fraudulent certificates were issued from DigiNotar (McAfee® Labs™, 2012), a Dutch Certificate Authority.

A case of man-in-the-middle-attacker compromised Comodo, the second largest CA in the world was found in March 2011 claimed by David (2012). Moxie Marlinspike, computer security researcher said that the attacker was found when he made a connection to the Comodo website. He was trailed back to the Hak5 website where he previously visited for a video on using SSLstrip tutorial. The attacker followed the video tutorials on the internet to begin hacking and was able to make off with a

number of rogue certificates such as mail.google.com, login.yahoo.com and Skype (David B., 2012). Another attack was found when Stuxnet and Duqu worms used rogue certificates to evade detection (McAfee® Labs™, 2012) as well as Flame malware that used forged Microsoft certificates. The compromised CA shows that there is no 100% security on cyber space even though the clients may believe that the certificate is from the trustworthy company.

Forms and channels of attacks have been spread to phone based attack, from the traditional as landline device to a smart mobile devices such as smart mobile phones and iPads.

2.4.4 Phones based technology attacks on online banking

In the early 1970s, Jon Draper invented an emitted device called 'Blue Box' which was known as 'phone phreaking', to hack telephone systems; hacking allowed a user to control the phone switches for free long distance calls or to bill calls to someone else's phone number. Phishing began to be used in the 1996 by hackers who were stealing America On-Line (AOL, an American global online Internet services and media company) accounts by scamming passwords from unsuspecting users. Phishing has become increasingly popular, and has developed since 2006 from simply stealing AOL dialup accounts into an ominous criminal enterprise (Anti-Phishing Working Group, n.d.).

Vishing or phishing VoIP, another variant of phishing is known as voice-phishing, which is a method that combines phone-based social engineering and the development of low-cost VoIP, to attack users over the phone. The combination of an Internet Protocol private branch exchange (IP-PBX) system with a VoIP telephone service requires minimal hardware; a sound card, speakers and a microphone, and a cheaper calling rate with downloadable free software such as Skype or Asterisk to set up with in a small business ("Why VoIP Should Get VIP Treatment in Your Small Business," 2008). VoIP service can be used to make both national and international calls between two computers or from a PC to a landline, or have a VoIP account on a mobile

phone while the VoIP number can be used from any country where a broadband Internet connection is available. “Many VoIP systems are rich in features. Some common features include: off-site call forwarding, extension dialling, voice-mail boxes, audio conferencing, and auto attendants to answer the phone and direct calls” ("Why VoIP Should Get VIP Treatment in Your Small Business," 2008).

In addition to phone phishing, the Australian Bankers’ Association (ABA) (2011) warned of a telephone survey scam which is using its name in an attempt to defraud bank customers. The bogus survey telephone operator may inform the person that they are completing a customer satisfaction survey on behalf of the ABA. The phony operator may also ask a series of questions regarding the person’s banking provider, such as: name of the bank, membership activating period since, and satisfaction with the service. One example is spear phishing which operates when e-mails release by a legitimate bank have been overwhelmed by forged ones, which is likely to become a popular technique. The e-mails contain phony contact numbers and ask customers to call back regarding the installation of software and/or confirm the details of their accounts. Spear phishing can occur even when an attacker pretends to be a member of the organisation and uses an apparently nearby phone number to call a customer when it actually comes from across the country or from another continent.

Phone attack is not limiting within traditional connections, with a fast moving technology of telephone spreading to mobile device, many mobile phone companies are integrating themselves into a smart mobiles. It enables users to entertain with mobile applications and be convenience and feel safety with personal mobile banking. iPhone application had launched mobile banking when users can deposit a check by taking photo of it and be secure with the application that is limited to credit-approved military personnel (USAA) customer (Larkin, 2009). Other facilities of mobile banking provided by iPhones include: downloading a dedicated program on cell phones, using phones' browser to access a mobile version of users’ banks, or simply sending an SMS message (Larkin, 2009). The convenience of mobile banking may have a myth of its insecurity

when mobile phone may be easy to lose and also get attacked by malware stealing bank user' identity and make a financial transfer.

Malicious mobile code can be programmed with some popular languages such as Java, ActiveX, JavaScript, and VBScript. Nimda is one of the best-known mobile worm codes. It used JavaScript for multiple infection or transmission methods to e-mail, Windows shares, web servers, and web clients. Nimda exploits e-mails by using HTML-based e-mail to look for e-mail addresses on the host and then sent copies of itself to those addresses. Windows Shares is interrupted due to the infected host which contains Nimda, of unsecured Windows files shared that is sent from NetBIOS. Whilst, web server is occurrence when a vulnerable server is found and get the infected code reside in the server (Ruggiero & Foote, 2011).

The act of malware explosion had spread parallel the new mobile technology. 63.39% of malware that targets mobile device is spyware and 36.43% are SMS Trojan (Juniper Networks, 2012). A case of URL spoofing was tested and founded in mobile operating systems such as iPhone 4, iPhone 4S, iPad 2 and third-generation iPad, iOS 5.0 and 5.1 (AppleInsider Staff, 2012). This explosion occurred because of the JavaScript code `window.open() method` that directs a user to a user to a forged online banking or shopping site. In addition, a new technology attacking mobile was claimed by Hyde (2012) about a Spanish hackers sent a virus to modify customers' mobile phone numbers registered to reinforce customers in receiving the text messages passcodes to verify their online payments. Furthermore, Mickey Boodaei, Trusteer CEO writers, posed on the Data Chain's blog ("Mobile Users Three Times More Vulnerable to Phishing Attacks," 2012) that users who always leave their mobile status on to read e-mail messages as soon as they arrive were more likely to be attack by the fraudulent e-mails. Secondly, users who accidentally accessed phishing websites via BlackBerry and iPhone are more vulnerable to phishing website. These are because their personal information will be submitted automatically from the second access to the website apart from the web appearance in the mobiles which is difficult to spot phishing. Finally,

iPhone users are eight times accessed to phishing websites compared to BlackBerry because of the market share in mobile business.

What can be seen from the cases is that mobile users are also in risk of phishing attack. It is not only because of the mobile browser vulnerabilities, but the trust that users have towards mobile security and mobile banking application. The attackers still use social engineering and the used of poor mobile security and its weak algorithm that allow cybercriminal to gain access and take control of traditional phone and smart phone in revealing personal information. Therefore, it is important that additional protection be used, such as checking the enterprises PBX (private branch exchange) or call manager software to see if it has any capabilities for detecting and filtering repeated calls from an outside number. This complements security awareness, policies used, and social engineering defensive techniques.

2.5 Why phishing still works?

Why is this older and well-known threat still so prevalent today? "A few years ago, the phishing e-mails and spoofed websites were easy to spot," Baumhof says. "Today, it's not so easy. They look legitimate, and end-users are easily fooled." (Kitten, 2012). Phishing therefore is still one of the top threats on the Internet. Its direct and indirect costs tax the global economy with billions of dollars in fraud damages every year.

While the level of spam is declined cybercriminals continue to enhance the level of sophisticated techniques to get over phishing detection. For example, the combination of embedded files or HTML attachment in e-mails (Help Net Security, 2012) with the use of encoded JavaScript to bypass the browser protection. In fact there are other loopholes that users may fail to beware such as visiting Facebook and Twitter websites which may increase the level of phishing unenticingly. In addition, the art of deception and persuasion that derived from social engineering concept is still deeply rooted in many fundamental social psychology principles and thus its perpetual success (Kessem, 2012).

As the level of trust in the information received is high in the motivation and emotion, any topic relating to tax, tax fraud, bank confirmation, security upgrading are such influential to financial users. There is no doubt why phishing is still successful. According to Microsoft Security Intelligence Report claimed by Kessem (2012) found that social engineering tactics had increased to 84.5% in 2011 from 8.3% of all phishing attacks in 2010. That means the impact of trust abuse enhance people to be at risk.

Phishing is not a new threat, yet it can be effective especially those who have 'bad habits' (Rashid, 2012), and naïve in security protection. From the incidents it can be seen that although the bank has strong and sophisticated security measures to protect their customers; failing in bank e-mail policy, user education and user awareness practices (Worthen, 2012) can cause a severe impact. This research investigated the knowledge about online banking security and their security or alertness in phishing threats and ways to mitigate the risks that financial institutions can be serious control to strengthen their services and understand what customers need.

2.6 Summary

Phishing may appear in various forms of attacks, depending on the target, such as on bank services or customers. However, this research focuses on the customers' side where the target is weaker and perhaps is more vulnerable to an overwhelming attack. Therefore the attack methods phishers use are different. One may be as a file attached to customers' e-mail, or pop-up windows appearing together with a webpage or an attack may be embedded in commercial or non-commercial websites. For example, if a customer accesses an infected website, the phisher can generate two files to create a counterfeit e-mail which could be used to spoof e-mail from the bank and create a fraudulent webpage which looks similar to the bank's actual website. Such pages may include attack codes to permit the sending of e-mails from the spoofed page to massive lists of addresses, providing a link to a malicious website which requests users to provide their personal banking information.

This chapter has examined and outlined the issues relating to the online banking threats that could have serious impacts on banks' end users. There are many types of cyber threats which could harm users when they are accessing their online banking. Each threat performs its unique tasks but they all still work towards similar illegal purposes. In addition, phishers or malware use different attacks to gain access to users' computers and cause them problems, particularly targeting online banking. More discussion of phishing attack methods will be presented in the next chapter.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

The purpose of this study is to investigate bank users' awareness about phishing, their online banking activities and their perceptions of the security measures recommended and offered by their banks. The selected methodology in this study was approached by descriptive research and comparative research. Descriptive research can require either or both quantitative or qualitative method to find out 'what is', might be applied to investigate the collecting questions (The Association for Educational Communications and Technology, 2001). Example of descriptive research in this study is a survey research where the investigator attempted to examine situations to establish the norm under the same circumstances (Walliman, 2006). Comparative research or analysis is designed to search for similarity and variance for universals or underlies general processes across different contexts (Mills, Bunt, & Bruijn, 2006). It highlights differences and similarities between two or more cross-sectional studies, shares the same issues of reliability, validity, replicability and generalisability to a better understanding of social phenomena (Walliman, 2006). Partial data colleting from this survey may be compared the differences or similarities with the similar studies from Australian Bureau Statistics, Australian Departmentt of Broadband, Communication and the Digital Economy, or from other formal statistics resources within or outside Australia where is possible to enhance the data validity and generalisability. The results of the study may be used for theory building which may be improved that "the research is more able to establish the extent to which the theory will or will not hold" (Walliman, 2006) under the existing theoretical literature and its practice, and inserting any recommendations arise from this study. This chapter includes discussion of the following topics:

Research paradigms and methods,

Research design,

Ethical considerations, and

Limitations of the study

3.2 Research paradigm and research methods

Thomas S. Kuhn's (1970) philosophical discussion of the nature of the history of science introduced the concept of the research paradigm, "a concept [which] has been heavily criticized" (Bloor, 1983, p. 313). Kuhn (1970, p. 23), in introducing "paradigm" as "an accepted model or pattern" attributes the acceptance of a paradigm by a community of researchers to its success in "increasing the extent of the match between ... [accepted] facts and the paradigm's predictions" (Kuhn, 1970, p. 24) and by further development of the paradigm itself. One accepted use of the term is as a "model or a framework that is derived from belief systems of individual knowledge (ontological assumption) and existence or multiple realities" that could be acquired (Olson, 1995, Dobson, 2002 quoted by Krauss, 2005) or, more simply, as "a holistic approach underlying a research methodology" (Kassim, 2001 quoted by Hamid, 2006, p. 92).

Quantitative and qualitative research paradigms are commonly described as the basic frameworks for academic social researchers, although the distinctions between the two must be understood. The goal of quantitative research is to "measure and analyze causal relationships between variables within a value-free framework" (Denzin and Lincoln, 1994 quoted by Sale, Lohfeld, & Brazil, 2002, p. 44). On the other hands, many qualitative researchers believe that a qualitative approach can make it easier to understand any phenomenon that needs to be viewed within its context (Krauss, 2005). "For example, statistical data collected from a quantitative method can often shape interview questions for the qualitative portion of one's study" (Hesse-Biber, 2010, p. 5).

3.2.1 Quantitative research

In general, quantitative research focuses on the numerical form of data obtained from the participants. Examples of quantitative data include the number of items recalled, reaction times, or the number of aggressive acts (Psychology Press Ltd., 2004). Thomas (2006) defined the quantitative approach with a survey method: "Quantitative surveys aim to measure demographic and personal attributes, living conditions and circumstances, behaviour, opinions, attitudes, values". Sample sizes in quantitative research are much larger than those used in qualitative research because it is necessary

to ensure that a representative sample can be used (Carey, 1993 quoted by Sale, et al., 2002). Research questions using quantitative methods ask participants the same questions and offer choices between answers, so that the gathered data can be used in statistical analysis (Mersdorf, 2009). Quantitative methods thus use statistical analysis to measure data from a large number of respondents. Examples of quantitative research methods are questionnaires/surveys, pre and post examinations and interrogation of existing statistical databases (Center for Civic Partnerships, 2007). Statistical modelling is used when researchers are measuring descriptive statistics and inferential statistics to find the distribution of central tendency, variability, and skewness (Center for Civic Partnerships, 2007).

The aim of the quantitative components of this research is to identify the extent to which a gap exists in terms of respondents' experience of security precautions. In particular, this is also to evaluate their knowledge and behaviours in accessing online banking with their current authentication methods and to identify their expectations about the security systems that they should be offered through their banks' websites.

3.2.2 Qualitative research

Qualitative research, on the other hand, aims on "experiences of participants and on the stated meaning they attach to themselves, to other people, and to their environment" (Psychology Press Ltd., 2004, p. 4). It also emphasises processes and meanings based on interpretivism and reality constructivism (Sale, et al., 2002). The use of meticulous qualitative research methods can improve the quality of data measuring, the comparative quality reports dissemination, as well as quality improvement efforts (Sofaer, 2002). According to Hayllar and Veal (2000 quoted by Nattavee Utakrit, 2006, p. 27), qualitative research methods are "concerned with collecting information which does not involve numbers. They typically focus on a small number of people, to be able to provide important information (Sale, et al., 2002), and produce large amounts of information about these people." Techniques used in qualitative studies include in-depth and focus group interviews, case studies, and participant observations (Sale, et al., 2002). Qualitative research is used for any method other than the survey such as

observations, interviews, focus group discussions, the collection of primary materials include transcripts, documents, photographs, sketches, and video or tape recordings.

The purpose of the qualitative aspects of this research is thus to gain insights into respondents' perceptions and knowledge about online banking threats and the security implementations of online banking systems. The sample group is selected from bank clients in WA who use and/or wish to use Internet banking. The purpose is to collect information about bank clients' attitudes, thoughts, behaviours in order to know how the group (Lanthier, 2002) as a whole thinks and what they understand about phishing attacks on Internet banking systems. So that the sample group represents the whole population (Neill, 2003), participants in this research were selected randomly from people of different ages, genders, and careers.

3.2.3 Mixed methods research

Mixed methods have been used widely in research projects, to assist the researcher to consider research questions from different perspectives. In practical research, mixed methods research combines quantitative and qualitative data gathering and analysis to achieve answers to research questions (Hesse-Biber, 2010). There are several reasons why qualitative and quantitative methods can be combined. Firstly, the two approaches can be combined because they share a unified logic (King et al., 1994 quoted by Sale, et al., 2002), and the goal of understanding the world people inhabit (Haase and Myers, 1988 quoted by Sale, et al., 2002). An example of a way that quantitative method is used to help explain qualitative findings is revealed in the following sentence: "The observation that women are reluctant to participate in exercise is qualified by a survey which reveals that it is older women who participate least" (Stecker, McLeroy, Goodman, Bird & McCormick, 1992, quoted by Nattavee Utakrit, 2006). Secondly, achieving similar results may be merely a matter of perception. In order to synthesise results obtained via multiple research methods, people often simplify the situation under study, highlighting and packaging results to reflect what they think is happening. They may combine two or more theories or sources of data from cross-

validation or triangulation to study the same phenomenon, in order to gain a more complete understanding of the research (Denzin, 1970 quoted by Sale, et al., 2002).

3.3 Research Design

Selecting the right investigative methods is an essential part in a developing an appropriate research design. A research design, which is a function of the research objectives, is defined as "…a set of advance decisions that makes up the master plan specifying the methods and procedures for collecting and analysing the needed information" (Burns & Bush, 2002 quoted by Hamid, 2006, p. 120). An appropriate research design is vital as it determines type of data, data collection techniques, and sample group, and approximate duration of data collecting. Primarily, it helps to align the planned methodology to the research problems (Churchill & Iacobucci 2004; Malhotra 1999 quoted by Hamid, 2006).

To achieve its objectives, this study was conducted in eight phases. Phase one was an exploratory study, including a literature review. Phase two focused on designing techniques and tools to be used in the study. Phase three evaluated reliability and validity of a pilot test. Phase four executed a pilot test. Phase five completed the actual data gathering. Data was collected from various sources, from publications and government statistics databases, and from a questionnaire administered to a sample of respondents. This phase involved description and statistical data analysis, concluding with cross-tabulations. The last two phases were devoted to writing a thesis based on findings and suggesting possible solutions to solve the problem. The phases of the study are represented diagrammatically in figure 3.3 and discussed in the following sections of this chapter.

3.3.1 Review and do a research of literature

The researcher began with an exploratory study to collect existing information, which provided the essential background information needed to precede a descriptive study. The exploratory study reviewed previous studies and explored new and related information which then was incorporated into this research. In turn, information

obtained from the descriptive study helped the researcher to design a causal experiment (Burns & Bush, 2002 quoted by Hamid, 2006). Lastly, the researcher established the scope of the study by forming questions. The questions were about the problems or the situation of events or conditions and their inter-relationships between the respondents' knowledge and behaviour in online banking and the threats they encountered from phishing attacks.

3.3.2 Designing and developing research approaches

This step involved selecting appropriate techniques and tools to be used in the study. Selecting a sample group was also part of this phase. The paragraphs below describe data collecting techniques, tools, and details of selecting a sample group.

3.3.2.1 Data collection techniques/ tools

"Data-collection techniques allow us to systematically collect information about our objects of study (people, objects, phenomena) and about the settings in which they occur" (Varkevisser, Pathmanathan, & Brownlee, 2003, p. 144). The systematic collection of existing data has been described in 3.3.1 above. In addition, a variety of participatory communication tools have been developed and implemented to enhance, contribute, and support research techniques (United Nations World Food Programme, n.d.). They also aim to stimulate interactions and make research approaches more participatory and fruitful. To avoid confusion in the use of terms, the following table points out the distinction between techniques and tools applied in data collection.

Table 3.3.2.1 Data collection techniques and tools

Data collection techniques	Data collection tools
Using available information	Archived records, online and offline publications
Administering written questionnaires	Questionnaire
Interviewing (focus group and individual)	Questionnaire, structured interviews, focused interview, open-ended interview
Case study	Questionnaire, semi-structured interviews, focused interviews, open-ended interviews

(Varkevisser, et al., 2003)

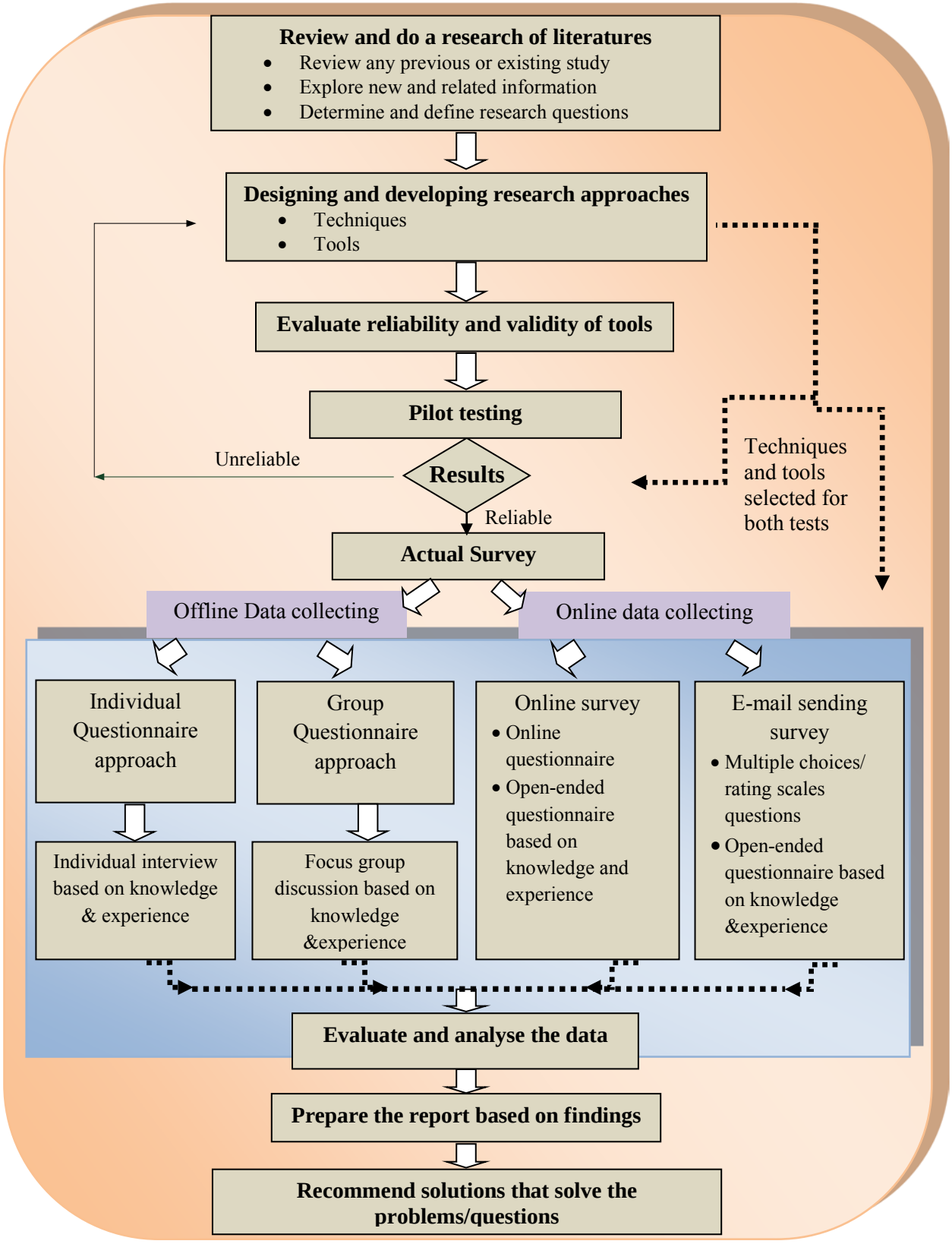


Figure 3.3 Research plan

(i) Administering written questionnaires

The planned structured survey involved several steps, from deciding on question wording, content and sequence, to devising measurement scales and response formats and assessing the reliability of the measurement used.

(ii) E-mail Survey

A number of researchers have begun to explore the advantages of conducting research via the Internet using e-mail (Smith, 1997; Murray & Sixsmith, 1998 quoted by Fox, Murray, & Warm, 2003). E-mail surveys may allow extra time for participants to answer the questions, which may increase self-esteem and allow them to brainstorm ideas, while reducing their social anxiety (Joinson, 1999 quoted by Fox, et al., 2003), and the feeling of pressure when someone is monitoring their performances. In this research, multiple copies of the questionnaire were sent to many known recipients. Some of these recipients had forwarded the e-mail to their contacts and asked them also to complete the survey. Of the 55 e-mail respondents, only 50 were used for further analysis, as some were incomplete. The questionnaire included multiple choices, rating scales, filling in the gaps, and open-ended questions. The open-ended questions that were sent via e-mail and used for online survey also used as interview questions for the individual and focus group interviews in this study.

(iii) Online Surveys

Internet or online survey conduction is becoming more effective in terms of getting quick responses and a high number of participants. The advantages are low costs, ease, and speed of administration (Schmidt, 1997; Buchanan & Smith, 1999 quoted by Fox, et al., 2003). In addition, it is inexpensive to establish an online survey and more convenient to launch the survey over the global network, where a number of online tools are available to assist the researchers to accomplish their tasks. Many researchers are interested in using the virtual community to conduct survey research. “Virtual communities have flourished online, and hundreds of thousands of people regularly participate in discussions about almost every conceivable issue and interest” (Wright, 2005). The Internet gives researchers the opportunity to target either large or

small populations, depending on the research project, who may have difficulty accessing offline survey channels. Lastly, the online environment also offers a high level of anonymity (Coomber, 1997 quoted by Fox, et al., 2003) for the respondent who may not want to identify himself. The investigator will not see the respondents' faces, or be aware of any other identifying aspects, apart from the IP addresses of their computers. An example of such online research is creating a questionnaire by using trusted and well known tools, such as 'SurveyMonkey'.

The online questionnaire for this study consisted of an introduction to the research, a questionnaire, with some open-ended questions. The introduction to the project was provided on the first page of the site, before participants were able to start the actual survey. Once the questionnaire was created, the link to the online survey was redirected to a social network or virtual community website, that is, Facebook. Facebook settings were used to restrict its display only to members of the WA community. There were 33 respondents who participated in this online survey. Only 30 responses were useable.

(iv) Personal Approach

This is a method of hand-delivering questionnaires to respondents and collecting them later (Varkevisser, et al., 2003). In addition, the idea of administering written questionnaire can also be referred to as "gathering all or part of the respondents in one place at one time, giving oral or written instructions, and letting the respondents fill out the questionnaires" (Varkevisser, et al., 2003, p. 147).The personal approach helps the investigator to target the sample group directly and to have an almost immediate response after the questionnaire is completed. A personal approach is best used when participants are willing to spend their time to answer questions immediately. It often means that the participants need have no further contact with the investigator. Some of the participants in this study preferred to answer the questionnaire, which included open-ended questions, without wishing to clarify any of their answers with an interviewer.

(v) Personal Interviews

"An interview is a data-collection technique that involves oral questioning of respondents, either individually or as a group" (Varkevisser, et al., 2003, p. 146). Boyce and Neale (2006) defined the goal of interview as "… to deeply explore the respondent's point of view, feelings and perspectives". In this sense, the individual interview may help researcher to gather more information about the interviewee's experiences or opinions related to the question. Individual interviewees are encouraged to "expand upon their answers to specific questions by providing explanations, rationale, and additional context and related issues" (United Nations World Food Programme, n.d., p. 23). The benefit of the individual interview is that the respondent could express their opinion freely without social censure. Besides, individuals may not want to share their personal opinion in front of a group or in public. However, this method is time consuming if the researcher needs to consult a number of participants in a limited time.

(vi) Focus group discussions

This technique provides "data on group interaction, on realities defined in a group context, and on interpretations of events that reflect group input" (Frey and Fontana, 1993 quoted by Waite & Harrison, 2004, p. 70). A focus group is influenced by word-of-mouth. Therefore, it is appropriate to utilise group discussion to explore the extremes of views expressed, the interaction between these views and the consensus achieved (Rogers, 1995 quoted by Waite & Harrison, 2004). The benefit of group discussion is that it can reduce the time spent, in comparison to a series of individual interviews. However, the participants' answers could be influenced by their peers, particularly in the situation when everyone in the group can hear what other people said.

The researcher recruited focus group volunteers by designing a poster and advertising in many public places such as university libraries, government council libraries, and other public notice boards. Participants were invited to information sessions where they were able to voice their opinions and then to learn how to avoid phishing scams. A copy of the invitation is attached as Appendix A of this thesis. Respondents were asked to tell their direct and/or indirect experiences of online

phishing attacks and how they solved the problems these attacks caused. Two focus groups were conducted, in which a total of 20 participants shared their knowledge and opinions about online banking threats and security implementation via online banking authentication measures.

(vii) Case study

"Case study research relates to an empirical inquiry that investigates a contemporary phenomenon within its real life context using multiple sources of evidence" (Noor, 2008 quoted from Yin, 1993). A case study is not always intended as a study of the entire population, rather it is often used to focus on a particular group, feature or unit of analysis. In order to understand and examine the processes of group activity, the case study approach was chosen specifically. A multiple case study was employed in this research study to enhance generalisations. The benefit of a multiple case approach is that it stimulates the research and distinguishes replication data in the cases examined without generalising the findings due to the multivariate nature of the cases (Valli, 2003). Noor (2008, p. 1603 quoted from Yin, 1993) emphasised that "The development of consistent findings, over multiple cases, can then be considered a very robust finding". This means that multiple cases of phishing attacks were included in the same study in an attempt to enhance research credibility. Variations in the findings of case studies based on individual phishing attacks added necessary detail to the countermeasures planned in research questions. The researcher therefore needed to identify different types of phishing attacks and to understand how they affected online bank users. Consequences of each attack method will be presented in chapter 5. Incidents of phishing attacks that have occurred with Australian bank users were investigated to evaluate the vulnerabilities and find the appropriate solutions or recommendations to mitigate the threats. If high levels of replication are found in several cases of attack, the researcher may be confident that the need for countermeasures has been thoroughly investigated in the future.

3.3.3 Sampling

The sample population was comprised of bank clients who are resident in Western Australia (WA). To ensure that only participants who were bank clients in WA responded to the online survey, participants were asked for their postcode in section A6 of the questionnaire. WA postcodes cannot be used to link individuals to specific addresses, so this question did not compromise the confidentiality promised to respondents. People included in the sample may vary in career, age, sex, nationality, educational background, or location. Bank clients may or may not have used online banking. They may or may not also have direct and/or indirect experience of a phishing attack.

For the pilot test, 45 questionnaires were distributed in Perth, Western Australia and resulted in the return of 30 completed questionnaires used for statistical analyses during 3 months data collecting started from November 2009 to January 2010. Several pilot tests had been conducted when the reliability statistics of the data was failed to meet the minimum satisfaction score due to errors with questionnaire design. Factors were tested using reliability analyses to calculate with Cronbach's Alpha formula, results of which are given in Table 3.2.4.1.

For the actual test, this data collecting process acquired 8 months to reach such numbers started from February 2010 to September 2010. 266 respondents completed the actual survey, but results from only 209 were analysed. Some were excluded because it was clear that they lacked understanding and were unable to answer the questions accurately. Within this number, only 99 respondents participated in the interviews. Individuals' responses related to the various banking institutions which offered them the ability to conduct online banking. Students and other professionals in Western Australia were among those who responded online. The sample focused on people in Western Australia, who had participated in online banking activities and may also have had experience of online banking threats. It also included those who had no experience of online banking activities, but may have received phishing e-mails which pretended to be from their existing bank and asked for personal information.

3.3.4 Evaluate reliability and validity of tools

Prior to pre-testing, the researcher's academic supervisors were asked to review the questions and gave their opinions about the questions' content validity. Typically the questions were standard and structured. In other words, a formal questionnaire was prepared and questions were asked in a prearranged order. The structured survey involved several steps from designing the questions to field work and assessing the reliability of the measurement used. After the review process, the questionnaire was ready to be pre-tested in an exploratory survey. Statistical tests of reliability will be discussed in 3.4.3.2 below.

3.3.5 Exploratory (pre-test) survey and revise questionnaire

The questionnaire was then distributed by different means, online, in print and as an e-mail attachment, in order to conduct a preliminary test. The aim of the pre-test was to ensure that the questions were eliciting the responses required, to uncover ambiguous wording or errors before the survey was launched at large (Burns & Bush, 2002; Zikmund, 2000 quoted by Hamid, 2006). If the test result had been below the standard score, revision of the test would have been carried out to find any loopholes and the text of the questions would again have been revised to ensure the correctness of the questionnaire.

3.3.6 Reliability Statistics

The empirical data collected from individual consumers were examined using the reliability test and multiple regression analysis using the SPSS program. Survey respondents were comprised of online banking users in the Western Australia. The respondents' profile was representative of the general population with equal split on gender and age groups between 18 and 65+. The reliability test results in that the Cronbach alpha (α) values should be at least .70 or higher (a lenient cut-off of .60 is common in exploratory research) to retain an item in an adequate scale, the standard error of measurement will be over half (0.55) a standard deviation (Garson, 2008). The following tables illustrate the results of reliabilities from the pilot test.

Table 3.3.6 Reliability statistics results from the pilot test

Description	Cronbach's Alpha	95% Confidence Interval		N of Items	Total population
		Lower Bound	Upper Bound		
Reliability statistics of respondents about their safety of using online banking (D9)	.82			8	30
Single measures		.23	.55		
Average measures		.71	.91		
Reliability statistics of respondents about their preferences of securing online banking offered by bank (D10)	.76	7		7	30
Single measures		.18	.50		
Average measures		.60	.87		

Table 3.3.6 illustrates reliability statistics results from the pilot test. The tests were analysed from rating scale sections which were used to calculate the Cronbach's Alpha (α) values. The confidence interval of data collected is 95%. It shows that α in both results are over the minimum standard score of .70 (α >.70). The opinion of 30 respondents about their safety of using online banking was 0.82 (α = .82) whereas opinion of 30 respondents about their preferences of securing online banking offered by bank was 0.76 (α = .76). This can be seen that this questionnaire was reliable and compatible among their groups.

3.3.7 Survey method and administration

This step involves the administration of the final version of the questionnaire after the pilot had been tested and found to be correct. In this survey, respondents were asked verbally, in writing or via a computer, a variety of questions regarding their behaviour, attitudes, demographics and lifestyle characteristics in relation to assessing online banking and their knowledge of online banking threats, including their direct or indirect experience of online banking attacks.

In order to acquire data from focused group sampling based on survey approaches, surveys can generally categorised into two broads of questionnaire and interview (Mersdorf, 2009). The form of questionnaires used in the focus group

interviews and individual interviews were the same as the online survey and e-mail survey. Therefore, the researcher collected data with multiple approaches, as described above, to gain a high volume of respondents.

The questionnaire was circulated in both online and offline formats. A link to the online survey was included in e-mail, so that potential respondents could forward it to others who might be interested. This encouraged participation by those who felt they did not have the time to complete a hard copy questionnaire. Participants were free to choose their preferred questionnaire format. A benefit of this decision is that more thoroughly-considered answers are sometimes provided.

3.3.8 Evaluate and analyse the data

This stage involved the use of standard analysis tools, *SPSS* and *Microsoft Excel*, to examine the data collected about participants' activities involving online banking systems.

3.3.9 Prepare the report based on findings

All the findings were documented and evaluated, the problems which were reported by participants being analysed and compared with other academic, public, and government information.

3.3.10 Suggest solutions that solve the problem/question

In this phase the key incidents and risks were communicated along with recommendations for minimising the impact of phishing attacks. What respondents felt they needed or preferred in their future use of online banking security was analysed. In addition, this study attempted to investigate the extent to which online banking security features affected consumer assessment of satisfaction, retention and trust.

3.4 Ethical Considerations

"Ensuring the well-being of respondents is of paramount importance in any study" (Fox, et al., 2003, p. 177). When dealing with sensitive information, such as

passwords, authentication security, and money, high-level precautions must be maintained. Fox et al. (2003) mentioned two aspects of protecting respondents from harm:

The first relates to ensuring that the information that the respondent have entrusted to the researchers is dealt with in a sensitive way. The second involves ensuring participation in the study does not affect the respondent in any adverse manner.

To secure the respondents' privacy, personal respondents' information such as contact details, social security number, and bank account number were not required, and all information gathered was kept securely and not revealed to anyone. Only the researcher had access to the information collected. In addition, Varkevisser et al. (2003, p. 153) recommended several points to consider for ethical research behaviour:

- Obtaining informed consent before the study or the interviewing begins;
- Not exploring sensitive issues before a good relationship has been established with the informant;
- Ensuring the confidentiality of the data obtained; and
- Learning enough about the culture of informants to ensure it is respected during the data collection process.

Thus, no research took place unless participants had previously signed a consent form or, in the case of the online survey, read and accepted the introductory material provided. Name and postcode of research participants were kept militarily secret. Documentary records were stored in a locked filling cabinet in the supervisor's office. The data on the laptop were secured with passwords known only to the researcher. According to University requirements, this data will be stored and retained for five years after the research project has been completed. Once this period is over, any printed documents will be shredded securely and recordings will be destroyed. Electronic data will be deleted by formatting and multiple overwriting and thereby written off the devices.

3.5 Limitations of the study

None of the methods could satisfy all the needs of the researcher (Hawthorne, 1992 quoted by Nattavee Utakrit, 2006). There is a factor which may limit the research. First of all, a case study that happened to the respondents may involve just a single real case; therefore, the result may not be representative of all the ideas of the general group or population. Also, "much of the information collected is retrospective data, recollections of past events, and is therefore subject to the problems inherent to memory" (Rickards & Ritsert, 2011, p. 941). Case studies often rely on descriptive information provided by different people. Some details may be overlooked unintentionally. For example, if online incident attacked to the respondents for several years ago, the given information may not be as complete as what the research expected to obtain. Consideration of maximum participants in research survey may enhance the quality of the research. Lastly, this study was limited to the Western Australian region where a number of populations may not as large as those in other states. Therefore, it may result in a number of people who use online banking, of which a consequence may be a population with few experiences of receiving phishing e-mails or being concerned about online banking attack incidents.

3.6 Summary

This chapter has provided a summary of the research methods employed in this study and justifications for the research approach utilised. Mixed method research, including quantitative and qualitative tools and techniques, has been described and details provided of the ways in which participants were recruited. Detailed results will be presented in Chapter 4.

CHAPTER 4: RESULTS

4.1 Introduction

This chapter presents the analysis of the quantitative data and qualitative data derived from the questionnaire survey, open-ended questions and semi-structured interviews in order to find answers to the research questions. This chapter contains descriptive results for five main factors:

4.2 Respondents' backgrounds.

4.3 Respondents' experiences in using online banking.

4.4 Respondents' experiences in relation to online banking security.

4.5 Respondents' perceptions of a deployment of online banking security protection.

4.6 Respondents' perceptions and experiences in online banking attacks.

In addition, results for research questions 1 and 2 have been cross-tabulated.

4.2 Respondents' backgrounds

Of the 226 questionnaires completed and submitted, 209 were analysed and divided by 21 respondents from focus group discussion, 33 from online survey, 45 from e-mail attached, and 110 from personal approaches. A significant group of completed questionnaires was excluded because, although the demographic questions were completed accurately, answers to the remaining questions in several cases revealed that the respondents either misunderstood the questions or did not have the knowledge required to offer valid responses. Although it was made clear, through the consent process, to participants that they could have stopped doing the questionnaire at any time, it is possible that some continued, despite limited knowledge of the topic, in the hope of being helpful. This may be regarded as a tentative indication of the lack of understanding of the need for highly secure means of utilising online banking.

Answers from open-ended questions and from semi-structured interviews were also used in this analysis. The researcher used qualitative evaluation processes to organise and categorise data by adapting Dey's (1993) structure to manage the data. Once the raw data was obtained, the researcher, firstly, needed to find a main focus of individual answers which matched the questions. Secondly, data was read and annotated several times to ensure the understanding of the answers. Thirdly, categories of the data were created to group similar answers into each category. Then, answers were assigned to the created categories. Data splitting and splicing were used to create sup-groups or levels of the similar answers to enhance the clarity of the data. "Categorizing the data allows us to compare the observations in terms of relations of similarity and difference" (Dey, 1993, p. 161). This helps the researcher to construct theoretical 'edifices' and combine them with existing further sources to create relationships between different parts of the data (Dey, 1993). Once the evidence was corroborated, the use of cross-tabulation statistical analysis was applied to compare results from the two datasets and make an aggregation between the quantitative and qualitative variables. In the meantime, other more random data was also analysed with descriptive and inference statistics such as central tendency measurement and chi-square analysis

4.2.1 Gender of respondents

The distributions of the demographic characteristics of the questionnaire respondents are summarised in the table below. All respondents were residents of Western Australia.

Table 4.2.1 Genders of the respondents

Genders	Frequency	Percent
Male	109	52.2
Female	99	47.4
Valid total	208	99.5
No answer	1	0.5
Total	209	100.0

From the data above, it can be seen that the percentage of males and females in the sample were 52.2% and 47.4% respectively. This shows that the population surveyed has a gender distribution closely resembling the distribution of males and females in the Western Australian population. According to data from the National Regional Profile of the Australian Bureau of Statistics in 2010, the estimated resident population of Perth Statistical Division at 30 June 2009 was 1.65 million. This number consisted of 833,110 (50.22%) male and 825,882 (49.78%) female (Australian Bureau Statistics, 2010e).

4.2.2. Age of respondents

Table 4.2.2 Age distribution of the survey respondents

Age	Frequency	Percent
Under 20	7	3.3
20 - 24	29	13.9
25 -29	35	16.7
30 - 34	26	12.4
35 -39	11	5.3
40 - 44	19	9.1
45 - 49	21	10.0
Above 50	58	27.8
Total	206	98.6
No answer	3	1.4
Total of respondents	209	100.0

Table 4.2.2.1 Estimates of the Perth resident population by age group at 30th June, 2010

Population by age group	percentages
0 to 14 years	19.2
15 years to 24 years	15.2
25 years to 34 years	14.8
35 years to 44 years	14.5
45 years to 54 years	13.8
55 years to 64 years	10.9
65 years to 74 years	6.4
75 years to 84 years	3.9
85 years and over	1.5

(Australian Bureau Statistics, 2010e)

In table 4.2.2, it can be seen that most of the respondents were aged above 50 which equated to 27.8% followed by the group aged between 25-29 at 16.7%, and the 20-24 years at 13.9%. The percentage of the elderly group compared to the ABS data in table 4.2.2.1 had similar results, with 22.7% of people who were above 54. The next largest sample by age group was 25-29 years which presented at 16.7% of all age groups. Data from ABS found that 15-24 years and 25-34 years age groups were the second and the third highest in the population, excluding 0-14 years, because this age group was not able to use online banking services. Obviously, the sample by age groups of 15-24 years and 25-34 years were overlapped at the second highest percentage of all samples. It thus appears that there is no direct statistical comparison between the population sampled and the ABS data.

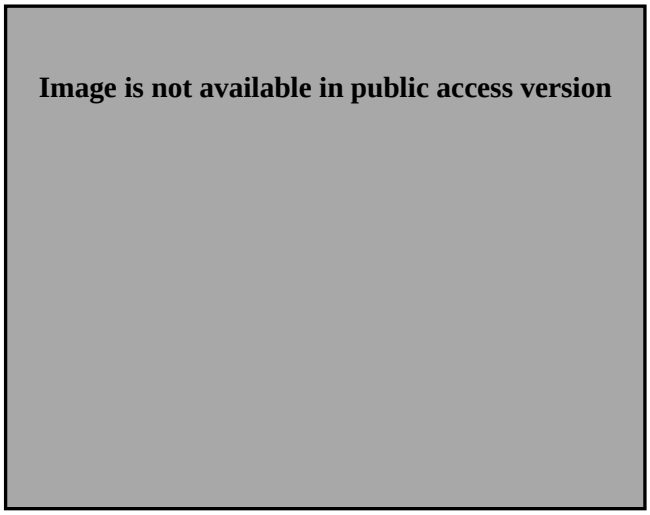


Figure 4.2.2 Paying bills online or online banking by each age group
(Australian Bureau Statistics, 2011a)

Figure 4.2.2 shows that people who are 25-34 accessed the internet from home to pay bills online or use online banking most often. This study found that the largest group of respondents who accessed online banking were in the same age groups, i.e. 25-29 at 16.7% and 30-34 at 12.4%, totalling 29.1%. Percentages of use by age groups are shown in table 4.2.2.

4.2.3 Annual income of respondents

Table 4.2.3 Respondents' annual incomes

Annual Income	Frequency	Percent
< 20,000	49	23.4
20,001-30,000	17	8.1
30,001-50,000	34	16.3
50,001-100,000	61	29.2
> 100,000	10	4.8
I prefer not to answer	32	15.3
Total	203	97.1
No answer	6	2.9
Total of respondents	209	100.0

The data in table 4.2.3 shows the estimation of personal annual income of the respondents. It indicates that 61 respondents had an annual income between $50,001and $100,000, which resulted in 29.2%. The next largest group was comprised of respondents who earned less than $20,000 annually or 23.4%, which included 40 respondents. According to the compiled data from the Australian Taxation Office's (ATO) Individual Income Tax Return Database, which was provided to the ABS at the Statistical Local Area level in the 2010 report, the estimated personal income of Perth Statistical Division in the last four years from June 2005 to June 2008 is shown in table 4.2.3.1.

Table 4.2.3.1 Estimation of personal income at year ended 30th June during 2005-2009

		2005	2006	2007	2008	2009
Average wage & salary income	$	38 712	41 095	43 785	46 804	-

(Australian Bureau Statistics, 2010c)

The above table reveals that the annual average income had increased $8,092 in the five years between 2005 and 2008. Due to the lack of official published data for 2009 and 2010, an approximate prediction therefore has been carried out to forecast 2 years' future trends. An extrapolated graph for 2009 and 2010 was plotted, as shown in figure 2.4.4.

Figure 4.2.3.1 Approximate growth prediction for the average wage and salary during 2005-2010

Figure 2.4.3.1 shows the average annual income of the majority of Perth residents. The 2-year predictions of the annual growth trend had indicated that, in 2009 and 2010, the average of the annual income would be approximately $49,000 and $52,000 respectively. Thus, it can be concluded that the approximate annual incomes of the respondents appears to be very similar to the expected incomes of the majority of the Perth population.

4.2.4. Respondents' occupation classifications

Table 4.2.4 Classifications of respondents' occupations partly adapted from Australian Standard Classification of Occupations

Occupation	Frequency	Percent
Professionals	50	23.9
Students	46	22.0
Technicians and trades workers	19	9.1
Retired	11	5.3
Clerical and administrative workers	10	4.8
Managers	8	3.8
Sales workers	8	3.8
Labourers	8	3.8
Community and personal service workers	6	2.9
Home duties	5	2.4
Machinery operators and drivers	4	1.9
Miscellaneous	7	3.3
Valid total	182	87.1
No answer	27	12.9
Total	209	100.0

Table 4.2.4 displays the occupations of the respondents. Part of the occupational classifications have been categorised according to the Australian Standard Classification of Occupations (ASCO) of 2001. If excluding unpaid occupations, such as student, retired, and home duties, and inadequately described occupations (miscellaneous), professional groups such as academic lecturers, IT specialists, consultants, and building engineers, comprised the highest percentage of occupations gathered from the sample: 50 respondents or 23.9% of the total belonged to this group. They were followed by the technicians and trades workers groups, related to food, automotive engineering, electrical and electronics, which was made up of 19 respondents (9.1%). Clerical and administrative workers were the third highest number of respondents at 10 respondents (4.8%) of the sample. This data correlated with the ABS database of Western Australian population statistics as below:

- According to data from the estimated occupations of employed persons: percentage of total employed persons in the census of the year ended 30th June, 2006 (Australian Bureau Statistics, 2010e), the professionals' group was ranked first, followed by technicians and trades workers, and clerical and administrative workers with the percentages of 20.6%, 15.9%, and 15.7% respectively. Machinery operators and drivers formed the lowest percentage of all paid occupations.

There is no adequate public record of the unpaid occupations such as retired, students, and housewives; therefore, the chi-square test cannot be used to find the significance of the study compared with ABS data. However, this research result appears to be consistent with the government data available for comparison with the sample population.

4.2.5. Education levels of respondents

Table 4.2.5 Highest of current education level of the respondents

Education	Frequency	Percent
PhD/Dr.	6	2.9
Master degree	44	21.1
Bachelor degree	70	33.5
Diploma	28	13.4
High school graduation	53	25.4
Others	5	2.4
Total	206	98.6
No answer	3	1.4
Total	209	100.0

In table 4.2.5, it can be seen that the highest current education level of the respondents in this sample were bachelor degree (33.5%) followed by high school level (25.4%) and master level (21.1%). In contrast, data from ABS indicated that:

> … in 2009, 62% aged 25-64 years in WA had obtained a non-school educational qualification, increasing from 59% in 2008. Of these, almost one quarter (25%) had obtained a Bachelor degree or above while 38%

had an Advanced diploma or lower qualification (Australian Bureau Statistics, 2011b).

However, it appears that there are no adequate public records about the overall graduation levels of the WA population, which means that there is no way of comparing the total data between the sample population and the government statistics. However, from the survey results it can be seen that a combination of the diploma and lower qualification/ high school levels in table 4.2.5, would give a percentage of 38.8%, which would give a very similar result to the ABS statistics. In addition, the percentages of respondents having a bachelor degree and the ABS results are also very similar. The total percentage of the respondents who have been educated to degree level is 57.5%, and for non-degree is 41.2%. It can be seen that the overall education level of the respondents to the survey is relatively high.

4.2.6. Geographical distribution of respondents

In figure 4.2.6.2, the red highlighting illustrates the area where most respondents were living, which mainly covered the Perth metropolitan area. Residential respondents' postcodes illustrated in table 4.2.6 have been grouped according to the TransPerth zone boundary as shown in figure 4.2.6.1.

According to the data from the Australian Bureau of Statistics in 2010, the estimated resident population of Western Australia (WA) at 30 June 2009 was 2.25 million, and almost three-quarters or 73.9% of the state's population resided in the Perth metropolitan area. A further 11% resided in the South West (Australian Bureau Statistics, 2010f). Generally, people are more likely to live close to the city. In relation to Internet access, factors such as level of income, education, population age, lifestyle and interests could cause the level of Internet access differences between metropolitan and other areas of Australia (Australia Government. Department of Broadband, Communications and the Digital Economy, 2008).

Figure 4.2.6.1 Residential areas defined by TransPerth zone boundaries (TransPerth, 2010)

Table 4.2.6.1 Postcode and living zone of the respondents

Zone	Postcode	Frequency	Percent
1	6000, 6003, 6006, 6014, 6103, 6151, 6152, 6009, 6060, 6019, 6153, 6104, 6100, 6101, 6052, 6059, 6051, 6007, 6008, 6010, 6016	80	38.6
2	6015, 6020, 6023, 6107, 6108, 6155, 6150, 6055, 6061, 6062, 6063, 6147, 6021, 6023, 6022, 6066, 6011, 6012, 6156, 6157, 6163, 6018, 6019, 6024, 6064	72	34.6
3	6026, 6027, 6919, 6025, 6069, 6065	26	12.4
4	6112, 6028, 6030	4	2
Outside zone 4	6169, 6430, 6053	5	2.5
Unknown	N/A	1	0.5
	Approximate total	188	90.0
Missing	No answer	21	10.0
	Total	209	100.0

Figure 4.2.6.2 Residential areas from which respondents were drawn

(Optus, n.d.)

The Australian Government, Department of Broadband, Communications and the Digital Economy (2008) reported that metro Internet users aged 14 years and over were likely to have accessed the Internet more than residents of other areas; percentages of 73% and 65% respectively were recorded in June 2006. From this, we may infer that

ease of Internet access is associated with living area, which can be reflected in the number of online banking access. This research covers respondents in the Perth metropolitan areas and was extended to some parts of the city's outer boundaries, which indicated the high significance of the sample used in the research.

4.2.7 Summary of description of respondents' backgrounds

Section 4.2.1-4.2.6 describes the respondents' backgrounds in terms of genders, ages, annual incomes, occupations, education levels, and usual places of residence. The overall results have been analysed and compared for data consistency with relevant information from public records to ensure the satisfactory results. The findings revealed that male respondents used online banking more than females. The majority of the respondents in this survey were above 50 and most respondents had annual incomes between $50,000 and $100,000. Professional workers and bachelor degree graduates were the main groups of the respondents. In addition, most respondents lived close to Perth city. An interesting finding was that the results of the demographic characteristics were highly reflective of the government statistics. This positive significance could enhance the reliability and the credibility of the data that needed to be analysed from the survey throughout this research.

4.3 Respondents' experiences in using online banking services

This section discusses the respondents' behaviours in accessing online banking services.

4.3.1 General purposes of using online banking services

This survey collected 209 responses; 185 respondents or 88.5% had experience in accessing online banking services, whilst 24 respondents (11.5%) had never experienced online banking as shown in figure 4.3.1. Of the non-online banking respondents, 21 provided their reasons for not using online banking services. Their comments are discussed in the following paragraph.

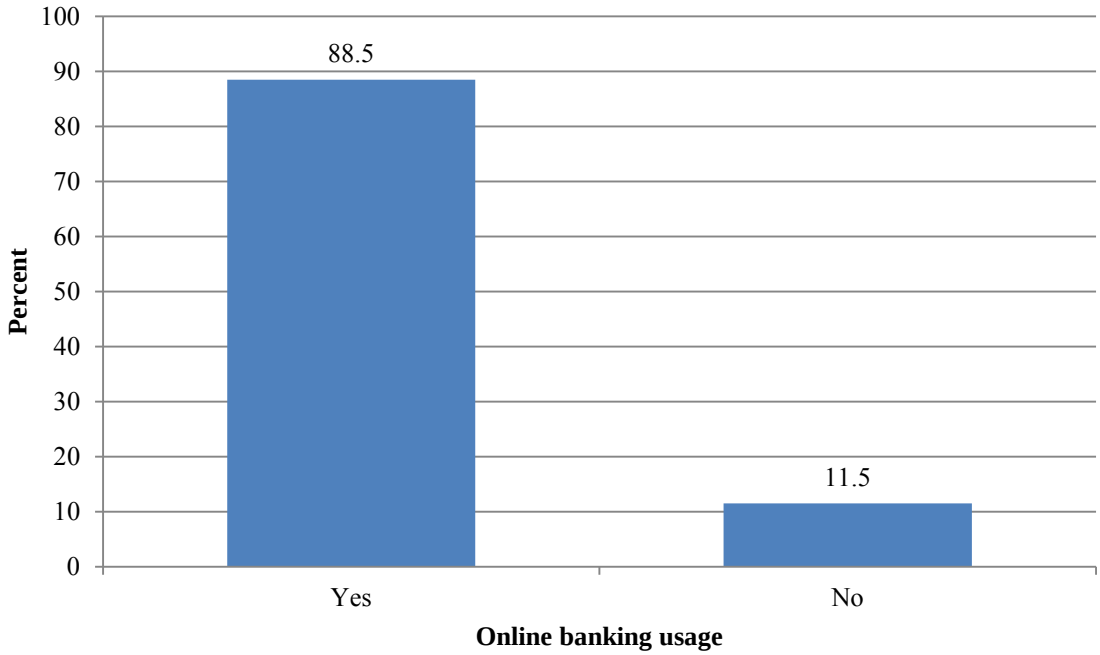


Figure 4.3.1 Monthly frequency of accessing online banking websites

Table 4.3.1 illustrates reasons why some people had not used online banking services. Questionnaire respondents could provide more than one reason for not accessing online banking. 14 responses (33%) of the non-online banking respondents were concerned about the security of online banking whereas 10 responses (24%) indicated that they were not interested in using online banking. In addition, 4 responses (10%) revealed that they did not see any real value in using online banking or having an online banking account; 6 responses (14%) mentioned that they did not have an online banking account.

Table 4.3.1 Reasons given by non-online banking respondents

Reasons of non-online banking respondents	Responses	
	N	**Percent**
I am not interested in online banking.	10	24
I do not know how to use online banking.	2	5
I do not know how to use Internet.	1	2
I do not know how to use computer.	1	2
I do not have an Internet connection.	1	2
I do not have an online banking account.	6	14
I am concerned about security.	14	33
I have not had time to open an account.	1	2
I do not see any real value in using online banking or having an online banking account.	4	10
It is too new. I would like to see how it works, and then I may open an account.	1	2
Other, please specify....	1	2
Rounding error	0	2
Total	42	100

Note: As small numbers of respondents are involved in this section, percentages have been rounded to appropriate whole numbers.

People who had used online banking services were also given the opportunity in the questionnaire to select multiple reasons for doing so. In contrast to the non-users, of 181 online banking respondents 36.1% indicated that they used online banking services because of their rapid operations. 28.7% of the respondents pointed out that they could avoid waiting in a queue in the bank branch, likewise 22.9% revealed that the time saved by not commuting to the bank was important. Surprisingly, only 0.6% (2 responses) felt that online banking offered better security and only 5.5% said they believed that using online banking was more convenient in terms of 24/7 access. 3.4% did not offer any reason for their adoption of online banking. In this survey, fast service, reduction of the time spent waiting or commuting may be seen as parts of the convenience. When the percentages for these three factors are combined, the total result for this study is 87.7% of the valid responses. On the other hand, there was no indication that respondents were interested because of the security of use of online banking, possibly because there is no official evidence to support a belief that using online banking is more secure than using traditional services.

Figure 4.3.2 illustrates the monthly frequency with which the respondents accessed online banking services. The largest group of respondents, 28.7%, accessed their online banking 3-5 times monthly. On the other hand, 7.2% of the respondents accessed their accounts more than 20 times per month. ACNielsen's research (2007) found that more than two-thirds of Australian Internet users accessed their online banking once a week or more. More specifically, 52% of Australians used Internet banking at least once a week whereas 16% accessed daily. Only 2.4% of the respondents did not answer this question and the other 11.5% was the group in which the respondents did not use online banking. It appears that the average Australian users accessed their online banking as frequently as once per week.

In terms of the place in which they accessed the online banking systems, a large number of the respondents, 62.6%, accessed online banking from their homes. This percentage was much higher than the 18% who carried out their online banking from their workplace, whilst only 7.2% accessed online banking from academic institutions. Respondents who were related to the schools, universities, or colleges, such as students, professors, and school administrators would access their online banking from their institutions. 20 respondents (7.5%) accessed their online banking from their mobile phone or palm top. Furthermore, those respondents accessing online banking from Internet cafés and public libraries had the lowest percentages at 1.5% and 1.1% respectively. These results are similar to the ABS (2010b) statistics recorded in 2008-2009 when 72% of the Australian households had home internet access increased from 16% to 72%. However, no statistics were found for 2010. Therefore, based on the available statistics, people have more opportunity to access the Internet from home, which may reflect an increase of online banking from homes.

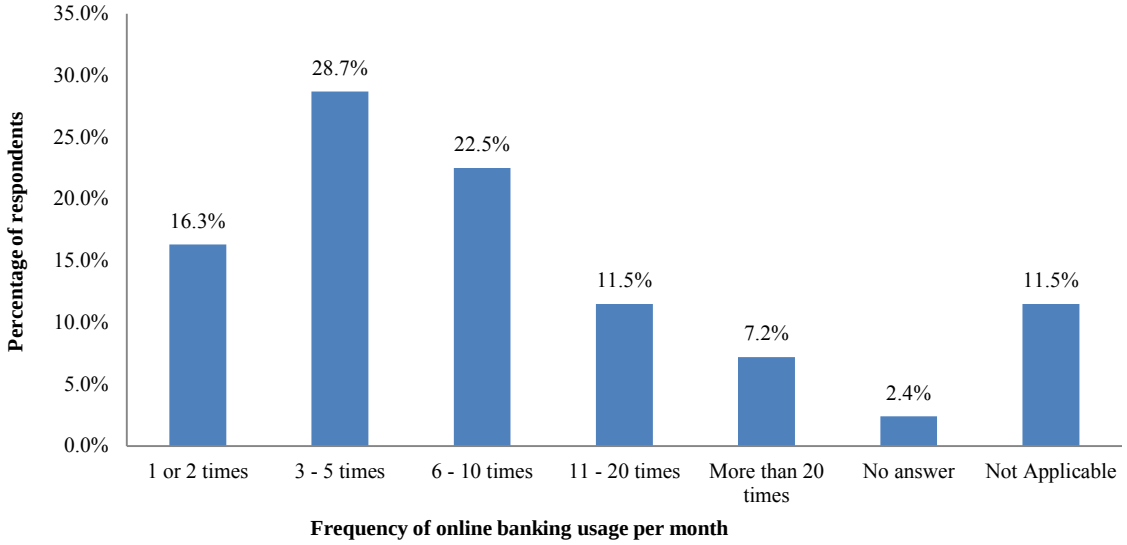


Figure 4.3.2 Monthly frequency of accessing online banking website

Further investigation revealed the main activities carried out by respondents when they were using online banking services. Table 4.3.2 lists these activities and identifies the breakdown of the group of respondents according to the activity which they nominated as being most important.

Table 4.3.2 Major activities carried out by respondents when online banking

		Frequency	Percent
Cases	Valid cases	181	86.6
	Missing cases	28	13.4
	Total cases	209	100.0
Responses	Money transfer	137	32.5
	Viewing balance and summary information	135	32.0
	Pay bill(s)	130	30.8
	Update personal information	16	3.8
	Other	4	.9
	Total responses	422	100.0

This shows clearly that most of the respondents did not think it was necessary to make regular updates of their personal information. Thus it can be seen that main

reasons why respondents used online banking were to transfer money, check their account balances, and pay their bills.

4.3.2 Online banking services in relation to individual banks

Table 4.3.2 Respondents' behaviours in accessing online banking services compared between two statuses: previous access and current access categorised according to bank

		Previous access			Current access		
		Frequency	**Percent**	**Percentage of cases**	**Frequency**	**Percent**	**Percentage of cases**
Cases	Valid cases	181	86.6	N/A	178	85.2	N/A
	Missing cases	28	13.4	N/A	28	13.4	N/A
Total cases		209	100.0	N/A	209	100.0	N/A
Responses	ANZ bank	73	24.5	40.3	63	25.0	35.4
	Commonwealth bank	69	23.2	38.1	54	21.4	30.3
	Bank West	40	13.4	22.1	30	11.9	16.9
	Westpac	40	13.4	22.1	35	13.9	19.7
	National bank	25	8.4	13.8	24	9.5	13.5
	Citibank	7	2.3	3.9	4	1.6	2.2
	HSBC bank	7	2.3	3.9	5	2.0	2.8
	I prefer not to answer	6	2.0	3.3	10	4.0	5.6
	Others	31	10.4	17.1	27	10.7	15.2
Total responses		298	100.0	164.6	252	100.0	141.6

Respondents were asked to detail their banking history and online banking preferences. They were asked whether they were still banking with their original bank (previous access in Table 4.3.2), whether they had changed to another bank or whether they had ceased to use online banking services. Respondents were allowed to select more than one bank. Table 4.3.2.above illustrates the comparison between the previous online banking access and the current online banking access of the respondents. In the left column, 73 respondents (24.5%) have chosen the ANZ Bank as their first choice of online banking service, while the Commonwealth Bank was the second selection with 69 respondents (23.2%). Bank West and the Westpac had the equivalent percentages of online baking accesses at 13.4% (40 respondents). The right column displays statistics of the respondents who decided to continue, discontinue, or had changed from a previous bank to another online banking service. 63 respondents (25%) of 252

respondents had chosen the ANZ Bank whereas the Commonwealth Bank, the Westpac and the Bank West had been chosen at 21.4%, 13.9% and 11.9% respectively. The results show that 80 respondents had used more than one online banking service, equivalent to 44.2%. These results are similar to a previous study carried out by Lichtenstein and Williamson (2006), who revealed that 40.6% used at least one Internet banking service.

Figure 4.3.2 shows the comparative statistics of the banks that the respondents had previously accessed and had been continuing. It can be seen that, overall, the current access, excluding the no answer provided option, had declined compared to the previous access. Focusing at first on the four most commonly used online banking services; the ANZ was the bank that the respondents still used even if it had declined by 4.9%. It was followed by the Commonwealth Bank for which the numbers dropped dramatically by 7.8%. Similarly, the Westpac and the Bank West had decreased by 2.4% and 5.2% respectively. Note that these percentages have been derived from the total case percentages as shown in table 4.4.2, due to the unequal numbers of respondents between the two periods. Reasons why the respondents decided to stop using online banking services are discussed below.

The most important reason that influenced the respondents to choose online banking with a particular bank was that 47.4% had continued by using online services offered by the bank in which they operated a traditional account. 19.7% chose a bank because of the excellent service it offered; followed by 13.7% who chose according to the security protections offered by the bank.

On the other hand, many of the respondents did not continue with their original bank when they moved to online banking services. 38.9% decided to move their online banking account to another bank. 27.8% gave reasons such as they had forgotten their username and/or password, refinanced their accounts, and/or lost their money from that particular account. Another 16.7% decided to close their account permanently without giving any reasons; while another 16.7% discontinued their account due to their

uncertainty about the security of their online banking system. Importantly, for the one case in which the respondent had lost money from his online banking account it may be assumed that either there was a low level of security provided by the victim's bank and/or his terminal was vulnerable to a phisher who gained access to the online banking system, as described in chapter 2.

4.3.3 Summary of description of respondents' experiences in using online banking

Sections 4.3.1-4.3.2 provided a description of the respondents' experiences in using their online banking services. These sections described the banks respondents accessed, their frequency of usage, their reasons to use online banking and choose a particular bank, and included the place in which they usually had access to online banking.

The overall results show that the number of online banking respondents was greater than the non-online banking respondents. The reason that influenced most to use online banking was the convenience, whereas those who were not interested in using online banking were concerned about the security of online banking itself. The core activities of the respondents in accessing online banking services were money transfer, viewing balance and summary information, and paying bills; however, the activity of updating personal information was not often regarded as important.

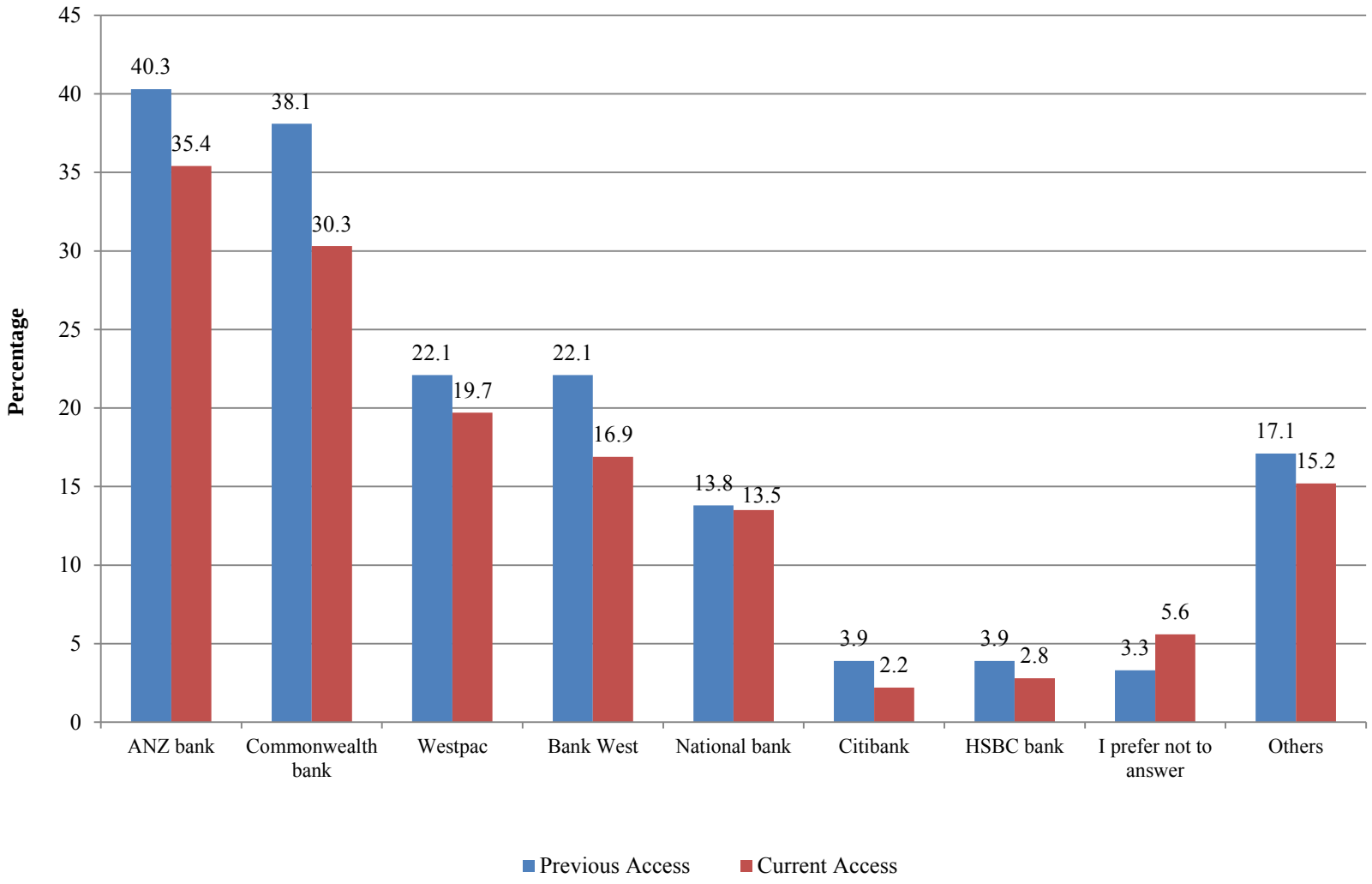


Figure 4.3.2 Respondents' behaviours in accessing online banking services compared between two statuses: previously accessed and currently accessing, categorised according to bank

Respondents usually accessed their online banking once a week from their home. Nearly half of the respondents had more than one online banking account. The reason that persuaded them to use their particular banks was that their existing traditional bank service could also offer online services. That usually occurred if there had been no incidents had led them to seek an alternative new bank. However, 16.7% had changed banks or closed their previous accounts because they felt that the online system they were using was not secure enough. People having more opportunity to access the Internet from home resulted in an increase of online banking access. Nevertheless, the perception that the security was not adequate outweighed the convenience offered by online banking, so that a significant number of people were still unwilling to utilise the services offered.

4.4 Respondents' experiences of online banking security

Section 4.4 includes the analysis of the respondents' experiences with regard to online banking security. The experiences of online banking incidents of some of the respondents are included in this and following sections.

4.4.1 General use of accessing online banking services

Statistics about the types of the Internet connections that the respondents used when accessing online banking were collected. The respondents who connected to the Internet with asymmetrical digital subscriber line (ADSL) wireless broadband had the highest frequency at 84 responses (40.2%), while ADSL wired broadband had 65 responses or 31.1%. However, 14 responses (6.7%) did not know which type of Internet connection they used even though they accessed the Internet from home. AusCert (2008) revealed from their survey that 84% have some form of wired broadband; 9% have wireless or mobile broadband and 6% still use dial-up modems. In addition, similar research disclosed by ABS (2010d) released types of Internet connection from all the ISPs operating in Australia at 30 June 2010. At that time 92% of the Internet connections were non dial-up, and 44% of the total Internet connections were digital subscriber lines (DSL) which continued to be the major technology. In an extension to its definition, ABS (2010c) described DSL as:

> It is a family of technologies that provides digital data transmission over the local telephone network. This suite of technologies, now referred to as xDSL, includes Asymmetrical Digital Subscriber Line (ADSL, ADSL2, ADSL2+) and Symmetrical Digital Subscriber Line (SDSL), etc. DSL is excluded from ABS counts where it is not used for internet connectivity (e.g. leased lines).

An Australian Communications and Media Authority (ACMA) (2011) survey concluded that "financial considerations appear to be the strongest driver in consumer selection of an internet service provider (ISP) for a home internet service… Other factors identified in the survey were:

Table 4.4.1. Reasons for choice of ISP

Reason	Percentage
Price	45
Service speed	25
Download limits	16
Bundling and package deals	13

(Source: Australian Communications and Media Authority, 2011)

Perhaps the development of newer technologies has also had an effect on the consumer uptake of Internet connections, but the ACMA data does not include an examination of this possibility.

Further detail was gathered about the technologies with which the respondents accessed their online banking. Different types of operating systems (OS) were installed on the computers that they most often used to access online banking. 30.8% had installed Windows XP for their OS, followed by Windows Vista, and Windows 7 at 28.1% and 21.9% respectively. On the other hand, the respondents who installed Macintosh OS comprised 6.7 % of the total, while only 2.2% installed open source operating systems such as Linux. 2.7% were not sure of the operating system used in their device while only .4% (1 person) said that he used a banking sim card to access his online banking service. 20 people said that they used mobile palmtop devices to access

their online banking services. It is possible that the 6 of those who could not identify their OS were using mobile operating systems such as Windows Mobile, Android or iOS platforms.

These findings parallel the W3Schools (2011) finding that the most popular operating system in 2010 was the Windows platform. In particular, Windows XP was still the highest OS platform installation, even if its use continuously decreased from January 2010 at 59.4% to December 2010 at 47.2%. Windows 7, on the other hand, increased continuously from January 2010 at 11.3% to December 2010 at 29.1%. StatCounter (2011) also revealed that Windows XP had the highest OS usage at approximately 48% and declined to 35% from January 2010 to December 2010. However, Windows 7 had increased dramatically from approximately 11% to 29% from the January to December in 2010. Nevertheless, Linux remained steady at the bottom of the list at approximately 1%. Internet connection types, operating systems installed, and their impacts on the respondents' views toward online banking will be discussed further in chapter 5.

4.4.2 Security protections installed on respondents' computers

This section of the questionnaire focused on the use of security protection that was installed on respondents' usual online banking access devices. It is possible that some people installed more than one type of security protection.

Table 4.4.2 Types of security protection installed on respondents' computers

		Frequency	Percent
Cases	Valid cases	174	83.3
	Missing cases	35	16.7
	Total cases	209	100.0
Responses	Yes, I have installed anti-virus software.	124	38.9
	Yes, I have installed firewall application.	76	23.8
	Yes, I have installed a popup window blocking tool.	43	13.5
	Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	42	13.2
	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	14	4.4
	I am not sure whether I have security protection or not (go to question C5).	7	2.2
	No, I do not use computer security software protection (go to question C5).	9	2.8
	Other, please specify	4	1.3
	Total responses	319	100.0

Table 4.4.2 illustrates types of security protection installed on the respondents' computers. As can be seen from Table 4.2.2, respondents were able to nominate more than one type of security in this section of the questionnaire. 174 respondents made a total of 319 responses. 38.9% of respondents installed anti-virus software as a main security protection. The second most common protection that respondents installed in their computers was a firewall, at 23.8%. Only 13.5% and 13.2% of the respondents installed anti-malware and pop-up blockers, respectively. 4.4% said that they had security protection, but they were unsure what types of security had been installed. Finally, 2.2% declared that they were not sure whether they had security protection on their computer or not. Most respondents relied on anti-virus applications to secure their computers whereas 48 respondents chose to install only the anti-virus without any extra applications. Thus it can be seen that most respondents relied on a single anti-virus protection to protect their computer system and secure their personal information. On one hand, it can be viewed as a positive result that most respondents were concerned about computer attacks; on the other hand, relying only on one type of software

protection is less effective in securing computer and personal information. Further discussion about this impact is in chapter 5. Moreover, the investigation of respondents' frequency in updating security software also showed that most relied on their automatic security update at 36.5% of total responses, followed by daily update and weekly update which were 15.6% and 12.6% respectively.

Upon the investigation, out of the 83.7% valid cases there were 58.9% who defined online banking statement as a website that resides on the bank's server in the form of the bank's home page. 7.2% (15 respondents) answered that online banking service is software provided by bank that operated and was resident on a PC to connect to the bank. On the contrary, 16.7% were not sure of the definition of online banking. According to Dixit and Datta (2010) Internet banking or online banking on a basic level can be referred to the mean of "setting up of a web page by a bank to give information about its products and services". It also involves provision of facilities such as accessing accounts, transferring funds, and buying financial products or services online so that the consumer can use the Internet to access their bank account and to undertake transactions (Dixit & Datta, 2010). When asked, a majority of respondents understood the basic concept of online banking system. Further discussion about knowledge in online banking and the installation of security protection will be included in chapter 5 to report the respondents' knowledge of online banking security systems and the software used to protect them from phishing attacks.

Figure 4.4.3 illustrates the types of online banking authentication provided by the banks when the respondents accessed their online banking accounts. Most respondents were required to use a login and password authentication; this equated to 61.2%. Login and password with mobile (SMS) verification code was dramatically less frequent, although it remained the second highest percentage at 18.2%. Login and password with token device was reported by 7.9%. Interestingly, logging in with the code that was attached on the credit card, EFTPOS or on a paper assigned by the bank and authenticating with other uncategorised online banking authentications (e.g.,

password via online keyboard with mobile verification codes, and use ID and PIN entered via mouse which cannot be typed), had the same lowest percentages at 1.4%.

However, the number of the respondents who had accessed their online banking account with biometric security was only 1.90%. Biometric security seems to be the newest type of authentication security that banks have started to implement to secure their customers' personal identity. In Australia, the National Australia Bank (NAB) (Gedda, 2009) had launched a voice biometric identification and verification function aimed at delivering enhanced customer experience and security.

The initial use of online banking authentication method as login + password was the most popular used, even if many banks were trying to develop and introduce better security authentication for their customers. Further investigation evaluated the numbers of passwords that the respondents exploited when accessing their online banking. It found that 8-character of the password was the length that most respondents selected when authenticating their account with the frequency used of 48 responses (27.6%) whereas 10-character password was used to authenticate with the frequency of 30 responses (17.2%). Interestingly, the 2 character password had a higher number of uses than 4 character password for 22 (12.6%). Finally, there were 19 responses (10.9%) who had password lengths more than 10-16 characters.

4.4.3 Respondents' security protection provided when accessing online banking services

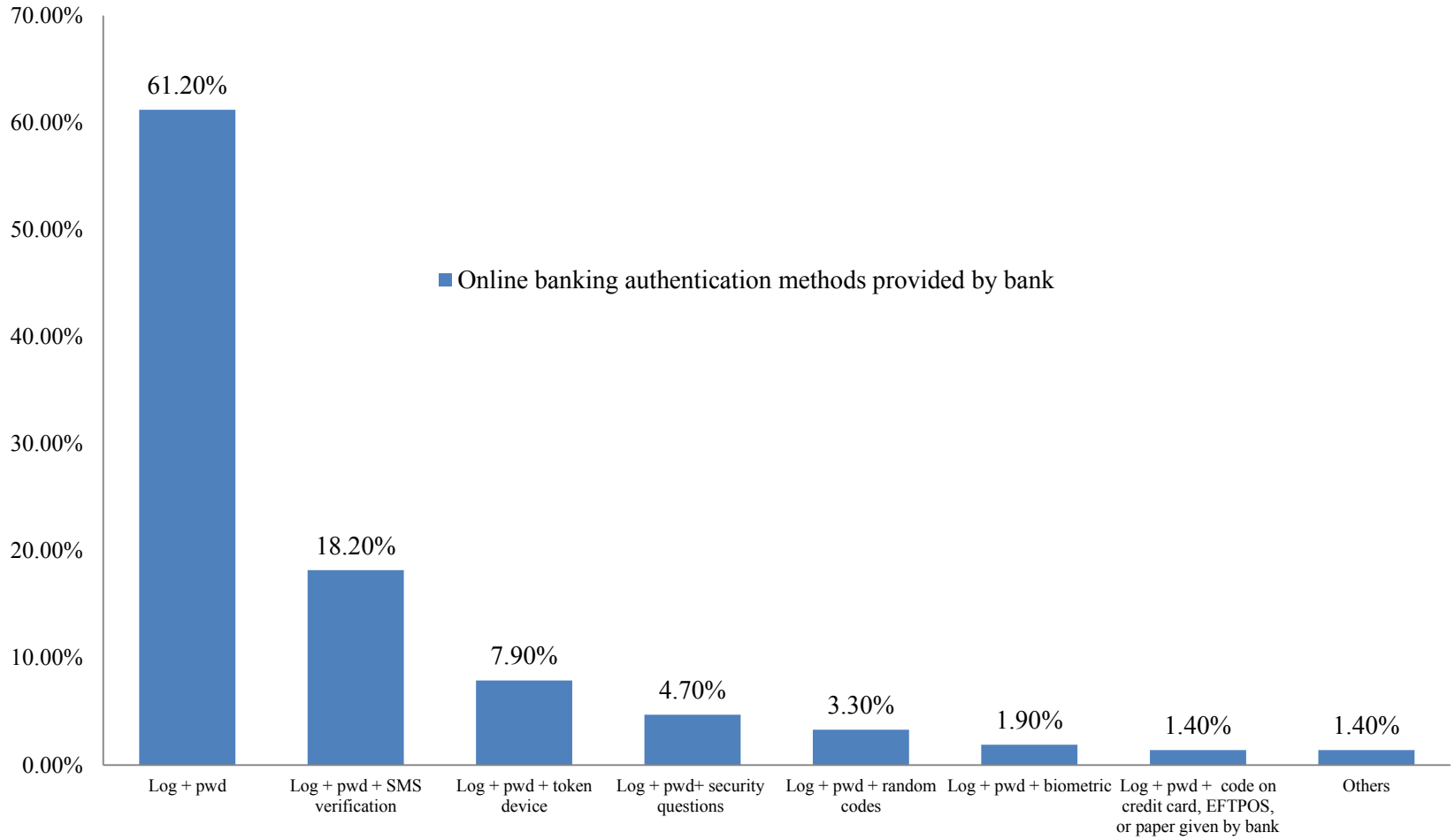


Figure 4.4.3 Types of security authentication provided for online banking

4.4.4 Respondents' experiences of inaccessible online banking services

Table 4.4.4 Experience of inaccessible online banking services

		Have been locked out		Allowed to re-access	
		Frequency	**Percent**	**Frequency**	**Percent**
Responses	Yes	64	30.6	34	16.3
	No	112	53.6	30	14.4
	Total	176	84.2	64	30.6
Missing	No answer	9	4.4	9	4.4
	Not applicable	24	11.5	136	65.1
	Total	33	15.8	145	69.4
Total responses		209	100	209	100

Table 4.4.4 displays the statistics related to respondents who admitted having made an error which restricted their access to their online banking accounts. More than half of the sample, 112 respondents (53.6%) had never experienced their online bank accounts becoming inaccessible. On the other hand, 64 respondents (30.6%) had experienced their accounts becoming inaccessible. Conversely, the right-hand columns show that there were 30 respondents (14.4%) who were not allowed to re-access their online banking account whilst 34 respondents (16.3%) still were allowed to re-access their account after a period of time. The survey also asked the respondents how they reported online banking incidents. Of 156 respondents to this question, 46.7% chose to call a number provided on the 'contact us' webpage, whereas 17.3% chose to inform the bank in person, and 13.1% preferred to use the e-mail provided. Other respondents indicated that they would "call bank centre", "call number on card", "contact account manager", "direct call to the bank I know, not just 'contact us' page", and "ring bank 1800 number".

Figure 4.4.5 illustrates the online financial institutions and services the respondents believed had the strongest security. Of 83.7% of valid cases, the bank was seen to have the strongest online security, with a percentage of 44% overall, or half of the valid total. However, 27.8% (58 respondents) were not sure what could be the most secure institution for online financial services. Another three reasons the respondents specified, beyond the choices included in the question, were: "I trust the companies that

use an external code on special remote", "I don't trust anyone", and "they are equally bad".

Further discussion exemplified the preferred security that the respondents trusted in their online financial institution. There were 59 people, (28.2%), who did not know what they liked about their preferred online financial institutions' security, whereas 52 people (24.6%) provided some details.

The strongest four reasons, each selected by 1.9% of the respondents, were the issue of their safe and secure feelings, the presence of password authentication mechanisms, and SMS verification. A miscellaneous group, totalling 7.7% of respondents, provided other reasons as follows:

(i) It allows the use of long passwords with both letters and numbers to authenticate,
(ii) It has HTTPs secure web protection,
(iii) It monitors customers activities, and
(iv) They have high standards.

The above reasons were some of the main points that respondents mentioned about their trust of the security measures offered by their chosen organization. If the similar group of reasons are combined, it can be seen that respondents paid more attention to the password authentication methods than to the feelings of trust or the complexities of the security authentication.

4.4.5 Respondents' levels of trust of secure online financial institutions

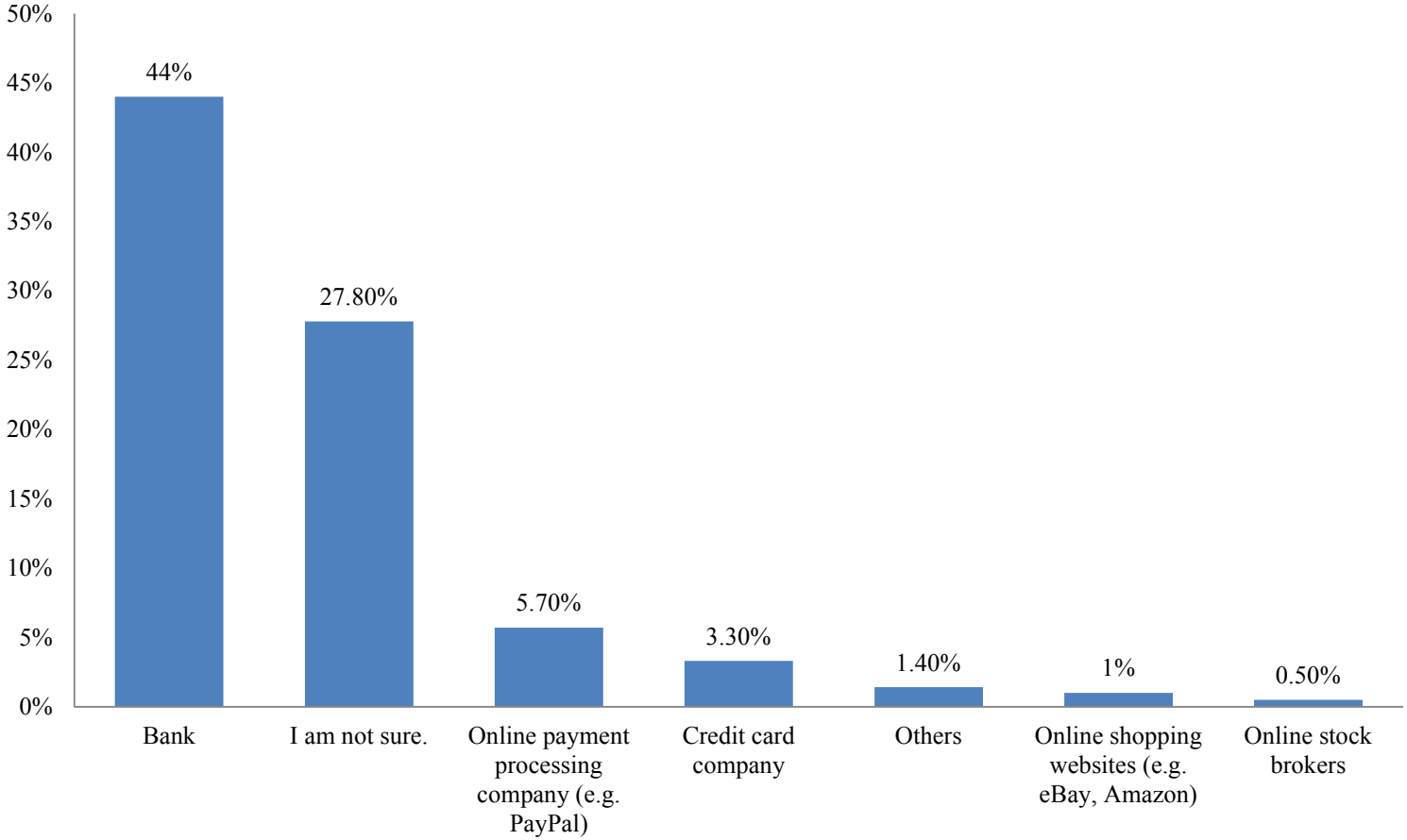


Figure 4.4.5 Levels of trust of secure online financial institution

4.4.6 Summary of respondents' experiences of online banking security

Sections 4.4.1-4.4.5 present descriptive results of respondents' experiences of online banking security in terms of the types of OS implemented in the machine they used for their online banking, the security software protection they used, the types of authentication security provided, their experiences in being locked out from the systems and how to deal with any of the problems they faced, in conjunction with their basic perceptions of online banking systems. The overall results show that most respondents had wireless Internet connections and used the Windows XP platform to access their online banking. Approximately one of every three respondents installed only anti-virus software without any extra security applications; this was the most secure option that most respondents installed. Even if most respondents had knowledge of online banking systems, they seemed to believe anti-virus software with the auto-update option was secure enough to protect their computers and personal information. Surprisingly, a basic login with username and password was the most common online banking security provided to the respondents by banks, with most respondents assigned passwords with 8 digits. Approximately half of the respondents had experienced being unable to access their own accounts; with half of those being allowed to re-access their online banking account. Finally, the majority of the respondents indicated that they believed that the banks were the strongest financial institutions in terms of the security provided.

4.5 Respondents' preferences for deployment of online banking security protection

This section discusses the respondents' perceptions and preferences in terms of the security offered by the online banking services they used. Respondents were asked whether they believed it was necessary to pay fees to ensure additional security, what kinds of passwords should be utilised and whether different kinds of authentication should be used in combination with passwords.

4.5.1 General information of online banking security system preferences

The investigator asked respondents for their reactions to the suggestion of paying mandatory fees for additional security measures such as biometric, or physical security authentication, or token devices such as a random numeric code device. 50.7% of the

valid responses disagreed with paying a mandatory fee as they believed that it should have been included in bank fees or it should have been the bank's responsibility to provide customers with security services free of charge. On the other hand, 32.5% agreed to pay a fee and specified various fee rates, as shown in Figure 4.5.1. 13.4% preferred to pay $2-$5 per month, while 8.6% of the respondents decided $1 monthly should be sufficient.

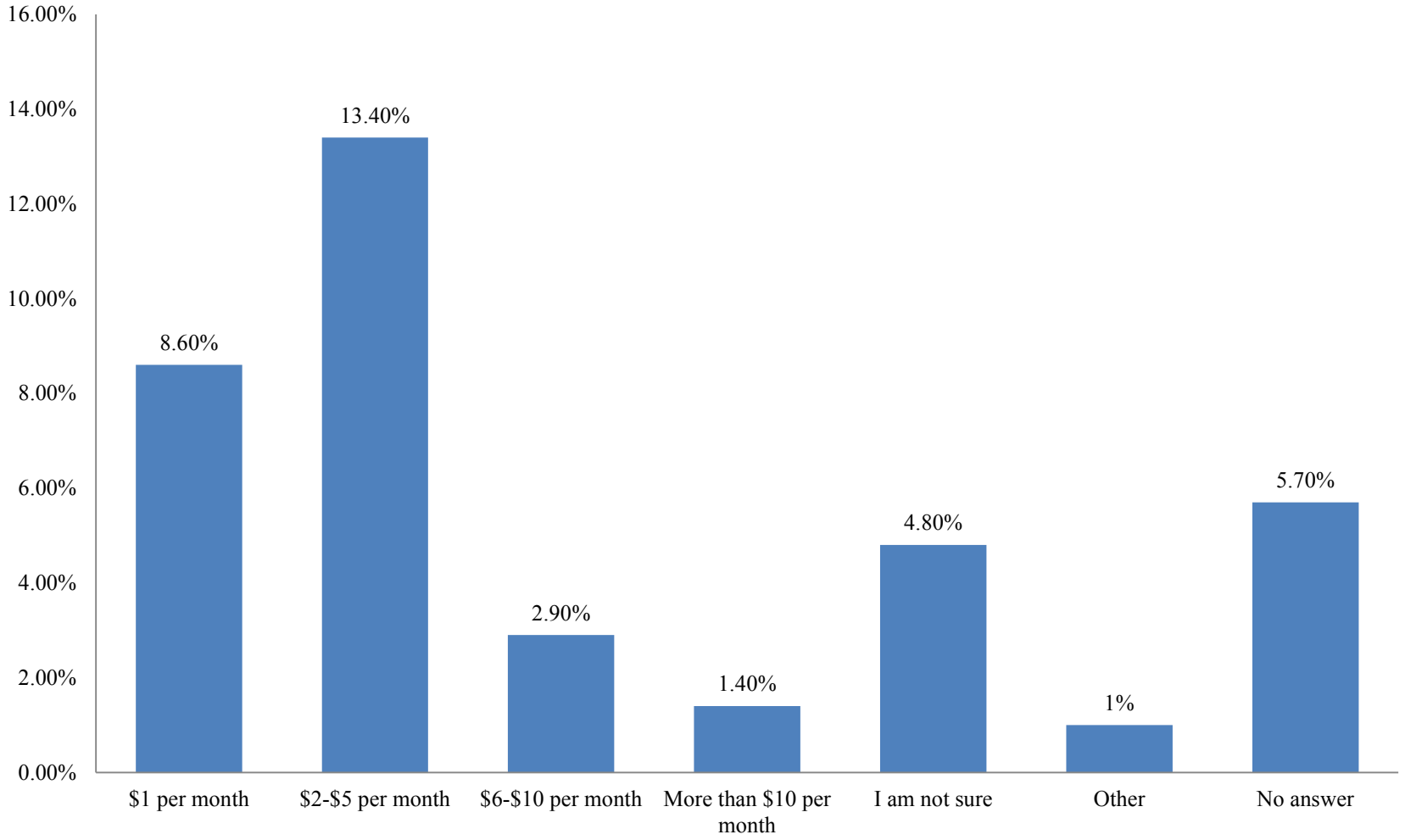


Figure 4.5.1 Suggested monthly fees for using additional security measures

4.5.2 Respondents' password preferences in online banking security

Respondents were asked how they thought they should create their passwords to secure their online banking accounts.

Table 4.5.2 Types of passwords preferred for secure online banking account

		Frequency	Percent
Cases	Valid cases	153	73.2
	Missing cases	56	26.8
	Total cases	209	100.0
Responses	Numbers	12	7.5
	Lower case alphabets (e.g. abc)	7	4.4
	Upper case alphabets (e.g., ABC)	2	1.3
	Special characters (e.g. @#%&*)	4	2.5
	Mixed of numbers and lower case alphabets	48	30.0
	Mixed of numbers and upper case alphabets	8	5.0
	Mixed of numbers and special characters	8	5.0
	Mixed of numbers, special characters, lower case and upper case alphabets	52	32.5
	I prefer not to answer	16	10.0
	Other, please specify	3	1.9
	Total responses	160	100

Table 4.5.2 summarises the types of password respondents preferred to use to secure their online banking account from attack. The preferred passwords were not only provided by the respondents, but also included the use of password generators or token devices that randomly assigned security codes. 52 responses (32.5%) selected a mix of numbers and special characters with lower case and upper case alphabets, while the mixture of numbers and lower case alphabets had 48 responses (30%). On the other hand, purely upper case alphabets were selected by only 1.3% of respondents. It can be seen that most respondents preferred to mix lower and upper case alphabets and numbers to create their passwords rather than using a weaker type of password for their online banking authentication processes.

Table 4.5.3 Minimum length of passwords preferences

Password	Frequency	Percent	Password	Frequency	Percent	Password	Frequency	Percent
10	20	9.6	4	1	.5	8-10	3	1.4
10-12	1	.5	5	3	1.4	9	6	2.9
10-15	1	.5	5-6	1	.5	Doesn't matter	1	.5
10-20	1	.5	6	28	13.4	More than 4.	1	.5
11	1	.5	6-10	1	.5	More than 5	1	.5
12	3	1.4	6-8	3	1.4	More than10.	1	.5
15	4	1.9	7	7	3.3	Unlimited	1	.5
16	2	1.0	8	61	29.2	-	-	-
Valid Total			152			72.7		
Missing	No answer		31			14.8		
	Not applicable		26			12.4		
Missing Total			57			27.3		
Overall Total			209			100.0		

The investigator then asked the 152 respondents about the minimum length of their passwords. 61 respondents, or 29.2%, verified their passwords as being 8 digits in length. 28 respondents (13.4%), selected 6 digits for the minimum length of their passwords. The next largest group, of 20 respondents (9.6%), chose 10 digits. The minimum password length that the one respondent preferred was 4 characters; another believed it was not necessary to specify how many characters formed the password, as long as there was a minimum of 10 digits. Each of these options was selected by 1 person and formed 0.5% of responses. In addition, one person indicated that it was not necessary to specify the length of passwords, because he believed that increasing the length of the password did not enhance the robustness of the password.

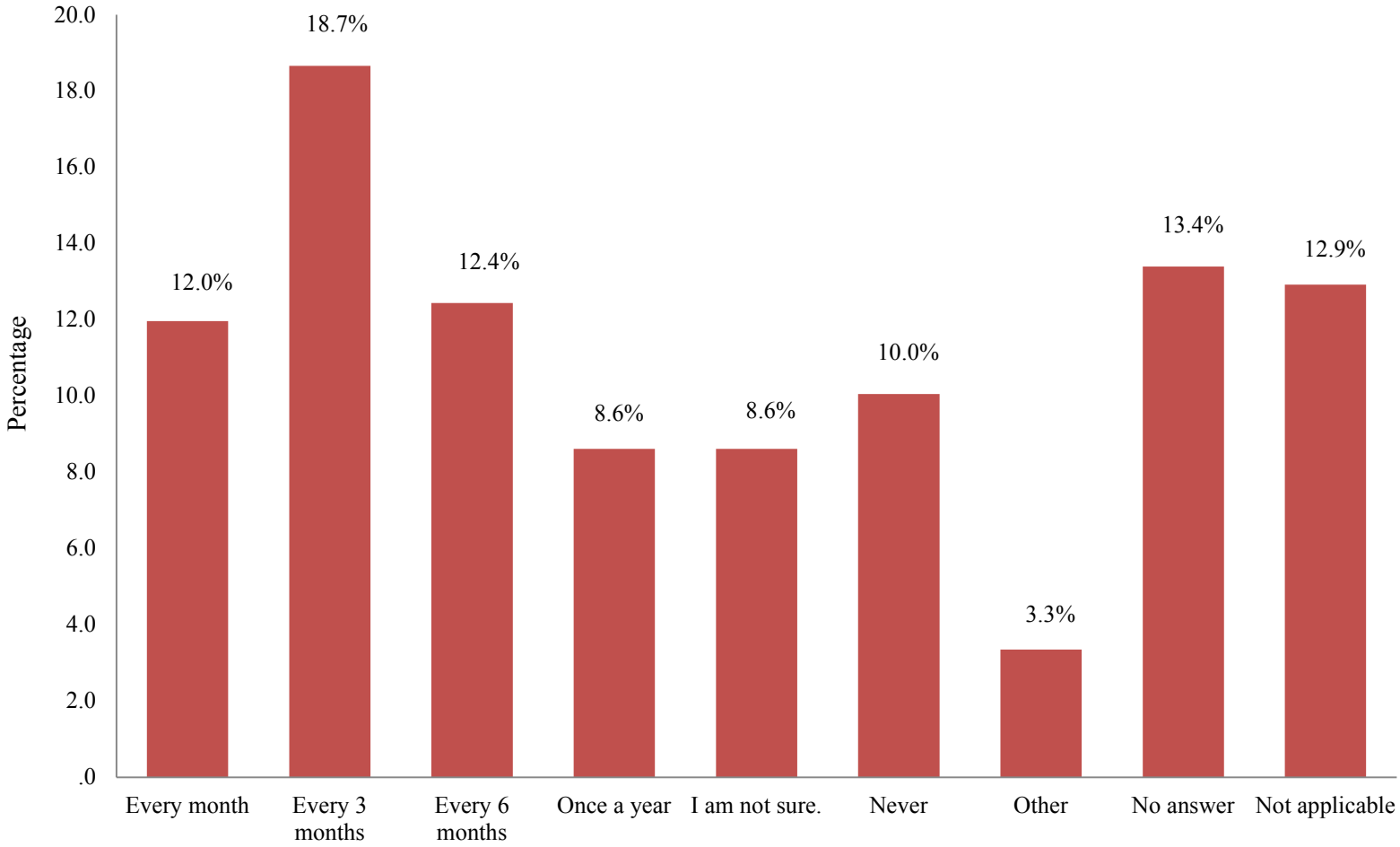


Figure 4.5.2 Frequency in changing online banking password

Furthermore, the survey also collected the respondents' opinions about the frequency of changing online banking passwords. The graph 4.5.2 shows that most respondents (18.7%) preferred to change their password every 3 months, while 12.4% preferred to change their password every 6 months, and a further 12% chose to change their password every month.

In addition to this survey, the respondents were asked their opinion toward changing their online banking passwords periodically in order to protect their account from unauthorised use. The result revealed that out of 172 responses, 132 respondents (63.2%) agreed to change their online banking password. This result was also opposed with KeCrypt's research (2010) in which 7% of the customers preferred to change their passwords. However, 40 respondents (19.1%) disagreed to change their password. The reasons that those who chose not to change their password were listed below:

(i) It is easy to forget; therefore, so they may choose to write down the new password and this could make them more vulnerable.
(ii) It is inconvenient to create a new password.
(iii) Changing the password may not solve the problem as changing the password does not counteract all types of phishing attacks.
(iv) Changing the password should depend on the customers' preferences.

The reasons above paralleled Dale's (2010) research about the problems of using multiple passwords and PINs as authentication methods. 60% had a problem with remembering and/or forgetting passwords, which eventually required the respondents to write them down (KeCrypt Systems Ltd, 2010).

4.5.3 Respondents' security authentication preferences

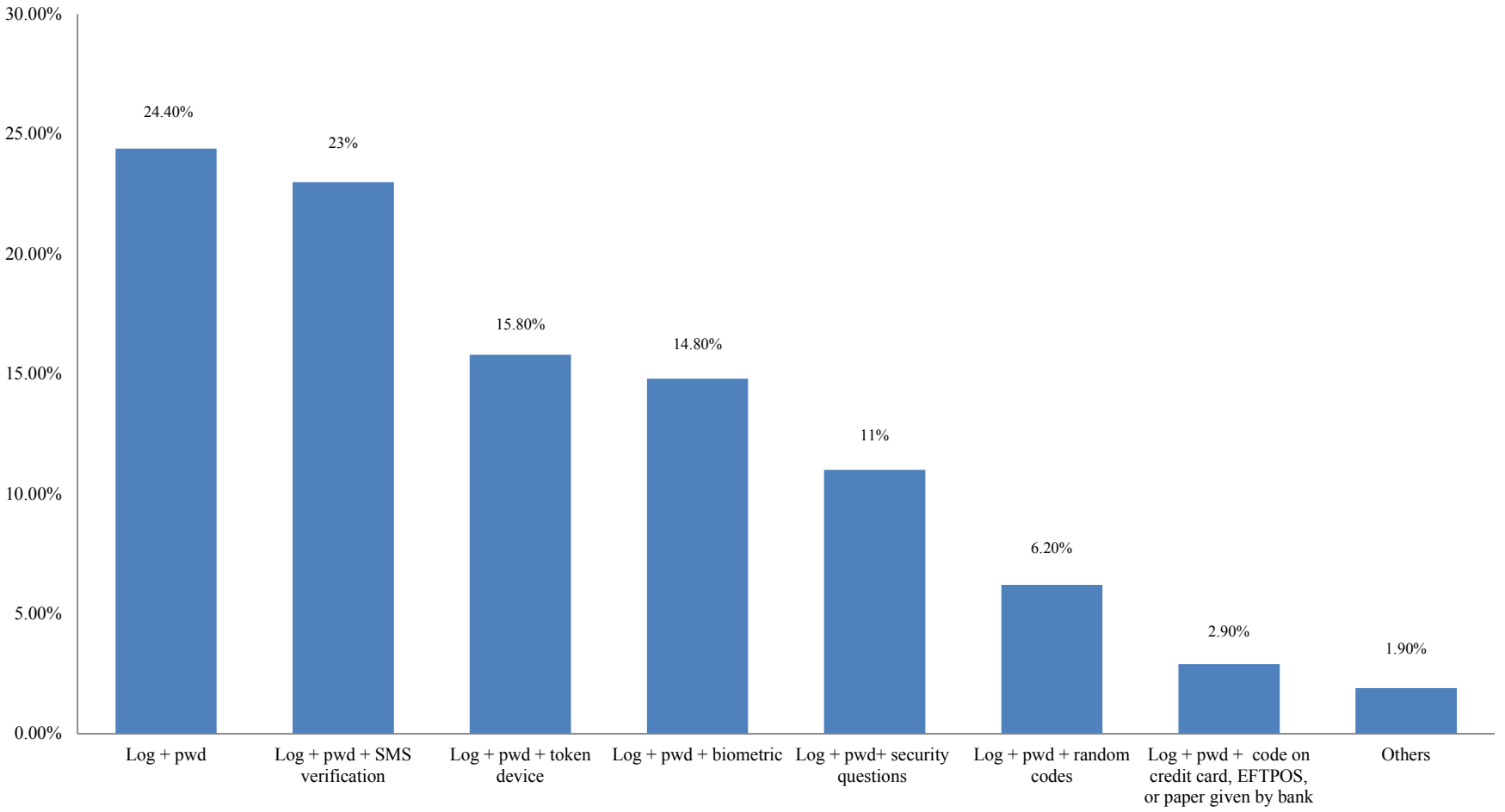


Figure 4.5.3 Preferred online banking authentication methods

It was very surprising that a simple login of username and password was the highest scoring authentication method, being chosen by 51 respondents (24.4%). This was followed by mobile (SMS) verification, which was chosen by 48 respondents (23%). Login with password and an additional token device, and verification with passwords and biometrics were the third and the fourth choices of respondents, with 33 responses (15.8%) and 31 responses (14.8%) respectively. Nevertheless, in a group of miscellaneous answers, one respondent recommended the combination of all the first seven security methods shown on Figure 4.5.3. Another believed that none of the authentication methods listed in Figure 4.5.3 was secure.

Subsequently the investigator analysed the hypothesis that there was a significant correlation between the security provided by banks (Figure 4.4.3) and the perceptions of the respondents in choosing their preferred authentication methods (Figure 4.5.3). Therefore, a goodness-of-fit of the chi-square test (X2) was used to compute the hypothesis assumption. The hypotheses for this test were written according to the formula below:

H0: The authentication security provided by bank has no influence on the respondents in choosing their authentication security preferences.

H1: The authentication security provided by banks has an influence on respondents in choosing their authentication security preferences.

The compiled results showed the chi-square result and related values as X2 (49, N = 155) = 175.306 p <.01 (p = .000), which means the X2 value was 175.306, degree of freedom (df) was 49, and the probability of chance (p-value) was 0.000. This can be interpreted to mean that the chi-square value is not greater than the critical value at level .01; therefore, the null hypothesis (H0) is rejected and H1 can be accepted. Therefore, the authentication security provided by banks does influence respondents in choosing their authentication security preferences.

4.5.4 Means and standard deviations of preferred security authentication methods

Table 4.5.4 Descriptive statistics of online banking security methods in customers' opinions

Common types of online banking security methods	N	Mean	Standard Deviation
Login+ password	140	5.44	2.277
Login+ password + static verification code attached on card	140	4.41	1.512
Login+ password + security questions	140	4.22	1.957
Login + password + challenge-response code	140	3.83	1.967
Login+ password + token device	140	3.41	1.658
Login+ password + mobile (SMS) verification code	140	3.41	1.586
Login+ password + biometric	140	3.28	2.046

Table 4.5.4 displays common types of online banking security methods that 140 respondents prioritised from what they believed it was the most secure to the least secure. Answers to this question were calculated to find the mean values and the standard deviations (SD). The higher the mean value, the lower common security methods were ranked. Types of online banking security methods have been prioritised from the highest mean and SD values to the lowest one. It appears that login + password had the highest result (M = 5.44, SD = 2.277), followed by login + password + static verification code (M = 4.41, SD = 1.512). On the other hand, login + password + biometric had the lowest value (M = 3.28, SD = 2.046). It can be seen few of the respondents believed that the simplest protection, such as Login + password, was sufficient for online banking, while the use of biometric authentication was accepted by many of the respondents as offering the necessary highest levels of security.

4.5.5 Respondents' opinions regarding the safety, trust, and confidence toward their online banking system

Table 4.5.5 Respondents' opinions in relation to the safety of using online banking

		1		2		3		4		5		6		7		8	
		f	%	f	%	f	%	f	%	f	%	f	%	f	%	f	%
Cases	Valid cases	161	77.0	162	77.5	162	77.5	158	75.6	158	75.6	156	74.6	159	76.1	158	75.6
	Missing cases	48	23.0	47	22.5	47	22.5	51	24.4	51	24.4	53	25.4	50	23.9	51	24.4
Total cases		209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0
Responses	1= Strongly not believe	5	2.4	3	1.4	1	.5	17	8.1	19	9.1	2	1.0	7	3.3	3	1.4
	2= not believe	11	5.3	20	9.6	15	7.2	34	16.3	32	15.3	10	4.8	15	7.2	6	2.9
	3= neither believe nor not believe	54	25.8	42	20.1	35	16.7	47	22.5	56	26.8	39	18.7	30	14.4	35	16.7
	4= believe	70	33.5	73	34.6	85	40.7	49	23.4	35	16.7	83	39.7	61	29.2	55	26.3
	5= strongly believe	21	10.0	24	11.5	26	12.4	11	5.3	16	7.7	22	10.5	46	22.0	59	28.2
Missing	No answer	24	11.5	23	11.0	23	11.0	27	12.9	27	12.9	29	13.9	26	12.4	27	12.9
	Not applicable	24	11.5	24	11.5	24	11.5	24	11.5	24	11.5	24	11.5	24	11.5	24	11.5
Total responses		209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0

f= Frequency, number of times score

1= Using an online banking system is financially secure.

2= I trust an online banking system to protect my personal information

3= I have confidence in the security measures that my online banking system uses.

4= Attack incidents against online banking systems have no influence in my level of confidence about online banking

5= I am able to distinguish if a financial institution's website is secure.

6= I am satisfied with the security protection of my online banking account.

7= I consider that security features are a main factor in my decision whether or not to do business with an Internet based company

8= My bank should offer security metrics to measure how secure my online banking is; this would be valuable to me.

Table 4.5.5 shows respondents' opinions about the safety of using online banking. The questions within this section of the questionnaire aimed to evaluate respondents' feelings about whether they could trust the levels of safety offered by their online banking institution. Responses were categorised by each of the statements listed above. 70 respondents (33.5%) believed that using an online banking system was financially secure. 73 respondents (34.66%) believed they could trust an online banking system to protect their personal information. 85 respondents (40.7%) believed that they could be confident about the security measures that their online banking system used. This confidence also extended to the situation where 49 respondents (23.4%) believed that attack incidents against online banking systems would not diminish their levels of confidence about online banking. However, 56 respondents (26.8%) of the group were unable to say whether they had the ability to distinguish whether a financial institution's website was secure or not. Satisfaction with the security protection of customers' online banking accounts was reported by 83 respondents (39.7%), while 61 respondents (29.2%) of the group believed that the security features offered were a major factor in respondents' decisions whether or not to do business with an Internet-based company. Eventually, 59 respondents (28.8%) suggested that they would find it valuable if their

banks had offered security metrics to measure the levels of security of their online banking.

The previous paragraph has reported the levels of agreement with statements about the trustworthiness of online banking security. Some of the statements were very similar. For example, statement 3 respondents who believed or strongly believed they could have confidence in the security measures of their online banking system totalled 53.1%. Those respondents who believed or strongly believed statement 6, that they were satisfied with the security protection of their online banking account, totalled 50.2%. Analysis of the 8th statement, that respondents would value the banks which offered security metrics for customers to measure the security of their online banking, showed that 54.5% of respondents agreed or strongly agreed. Nearly half of the respondents agreed or strongly agreed with statement 1 that using an online banking system is financially secure. 46.4% agreed or strongly agreed with statement 2, that the banks were trusted to protect their personal information. Interestingly, the number of respondents who believed that attack incidents against online banking systems would have no influence on their levels of confidence about online banking was only slightly greater at 28.7% than those would disagreed or disagreed strongly at 24.4%. The neutral responses to this statement totalled 22.5% of the group. Those respondents who were not sure if they were able to distinguish if a financial institution's website was secure totalled 26.8%, greater than those who believed that they could with only 24.4% of respondents selecting that option. Those who were sure they could not identify a secure webpage numbered 24.4% of the group.

Therefore, it can be concluded that respondents trusted the security provided for their online banking more than their own ability to diagnose any problems with their online banking. Although the group who agreed that online attacks would not prejudice their level of confidence about online banking was the largest group of responses to statement 4, the differences between the groups was not significant. There was no clear indication that attack incidents would either damage or enhance their trust of the security offered by their existing online banking.

4.5.6 Respondents' opinions regarding the multilevel and complexity of security protection toward their online banking system

Table 4.5.6 Respondents' opinion about security preferences of their online banking system

		1		**2**		**3**		**4**		**5**		**6**		**7**		**8**	
		f	%	f	%	f	%	f	%	f	%	f	%	f	%	f	%
Cases	Valid cases	159	76.1	160	76.6	159	76.1	157	75.1	160	76.6	159	76.1	157	75.1	156	74.6
	Missing cases	50	23.9	49	23.4	50	23.9	52	24.6	49	23.4	50	23.9	52	24.6	53	25.4
Total cases		209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0
Responses	1= Strongly disagree	2	1.0	11	5.3	3	1.4	6	2.9	4	1.9	6	2.9	9	4.4	7	3.3
	2= disagree	12	5.7	34	16.3	4	1.9	6	2.9	6	2.9	3	1.4	13	6.2	7	3.3
	3=neither agree or nor disagree	22	10.5	31	14.8	23	11.0	18	8.6	12	5.7	4	1.9	25	12.0	12	5.7
	4= agree	54	25.8	43	20.6	54	25.8	25	12.0	25	12.0	14	6.7	19	9.1	25	12.0
	5= strongly agree	69	33.0	41	19.6	75	35.9	102	48.8	113	54.1	132	63.2	91	43.5	105	50.2
Missing	No answer	26	12.4	25	12.0	26	12.4	28	13.4	25	12.0	26	12.4	28	13.4	29	13.9
	Not applicable	24	11.5	24	11.5	24	11.5	24	11.5	24	11.5	24	11.5	24	11.5	24	11.5
Total responses		209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0	209	100.0

f= frequency, number of times score
1= My bank should apply multi security protection, such as login and password and SMS mobile verification code and digital signature.
2= My bank should prompt me with a security question, such as ‘what is your mother's maiden name?’ every time I log on to my online banking account.
3= My bank should offer a tracking facility showing all transactions and detail about when I have logged in and out.
4= My bank should never allow more than one computer access to the same online banking account at the same time.
5= My bank should detect, deny and stop all online banking activities if there is more than one computer accessing the same online banking account at the same time.
6= My bank should log off my account automatically when I close the window.
7= My bank should log off my account automatically after I have been logged on for 45 minutes.
8= My bank should log off my account automatically if my bank webpage is not active for 15 minutes.

Table 4.5.6 shows respondents’ opinions about the security deployment of their online banking system. The questions within this section of the questionnaire aimed to evaluate respondents’ opinion about their transaction security preferences by their online banking institution. Responses were categorised by each of the statements listed above. 69 respondents (33%) strongly agreed that their bank should have applied multi security protection, such as login and password and SMS mobile verification code and digital signature. 75 respondents (35.9%) strongly agreed that their bank should have offered a tracking facility that shows all transactions and detail about when the respondents have had logged in and out. This strong attitude also extended to the situation where 102 respondents (48.8%) respondents agreed that their bank should have not allowed more than one computer to have access to the same online banking account at the same time. Also, they preferred their banks to have a monitoring system to detect, deny, and stop all online banking activities if there is more than one computer accessing the same online banking account at the same time. This percentage was 54.1% or

equalled 113 respondents. Moreover, high numbers of 132 respondents (63.2%), strongly agreed that their bank should have logged off their account automatically when they closed the windows. In addition, there was strong agreement of 105 respondents (50.2%) to the statement that their banks should log off their accounts automatically if their bank webpage was not active for 15 minutes. Lastly, when the respondents were asked if their banks should have logged off their accounts automatically after they have been logged on for 45 minutes, the numbers strongly agreeing were 91 responses (43.5%.) However, only 43 respondents (20.6%) just agreed to allow their banks to prompt them with a security question every time they logged on to their online account.

The previous paragraph has reported the levels of agreement with statements about the multiple levels and complexities of security protection. It can be seen that most respondents strongly agreed that their banks should have applied those complexities of security to their online banking systems. Only one security protection, statement 2 which was the security question, such as 'What is your mother's maiden name?', saw many respondents agree rather than strongly agree.

In addition, the table showed apparently that the majority of the respondents had positive opinions about implementing multilevel security for their online accounts. The total numbers of the respondents who agreed and strongly agreed with each statement were higher than the total number of those who disagreed and strongly disagreed or were neutral.

4.5.7 Respondents' additional opinions toward online banking system

Table 4.5.7 Respondents' opinion about using online banking or security protection for online banking

Responses	Frequency	Percent
Increasing/ improving level of online banking security	15	31.3
Convenient satisfaction	8	16.7
User education	6	12.5
Self-awareness in security	4	8.3
Ease of use	3	6.3
Refund policy satisfaction	2	4.2
Security satisfaction	1	2.1
Other, please specify	9	18.8
Total responses	48	100.0

Table 4.5.7 shows respondents' additional opinions regarding the use of online banking or security protection for online banking. It can be seen that 16.7% of respondents were satisfied that the convenience of using online banking made their life easier; however, only 2.1% were satisfied with online banking security measures. In addition, 31.3% of the respondents concerned about bank security and therefore wanted banks to increase and/or improve level of online banking security. 12.5% of the respondents suggested that it was necessary to educate users about benefits of online banking, its security, and to provide additional information about protecting users from online banking attacks. Moreover, 18.8% of the respondents mentioned their additional opinions that, even if they were using online banking, they really preferred not to use it because they were aware of the numbers of threats and attacks on online banking. These show that the security issue is the main concern for respondents in regarding to using online banking services. It can be concluded that increasing and improving online banking security by banks was the main concern that banks should focus upon ensuring that respondents have been given all information about the system and know how to protect themselves from the scammers.

4.5.8 Summary of respondents' opinions about online banking security

Sections 4.5.1-4.5.7 illustrate descriptive results of respondents' opinion in a deployment of online banking security protection in terms of types of passwords and online banking security protection, and mandatory fees for deploying security measures. It also covered the respondents' views about changing passwords durations, minimum length of secured passwords, prioritised secured password preferences, and their opinion on online banking safety and security features. The data about the respondents' opinions of authentication security and advanced security features, needed to enhance their online banking security knowledge and ensure they can protect themselves from phishing attacks, has been analysed. The overall results indicated that most respondents preferred their passwords to have a mix of numbers, special characters, and lower case and upper case alphabets with the minimum of 8 digits. The responses revealed that the respondents agreed to change their password every 3 months for their bank account security. However, types of security authentication methods were not correlated with the complexity of the password. What was interesting was that most respondents chose the simplest authentication method, such as login with username and password, for their access more than the more complex methods such as login with username, password and mobile verification (SMS). This result was associated with the next question, which asked the respondents to prioritise the common types of online banking security from strongest protection to the weakest protection. However, the outcome revealed that login and password had become the weakest type of security whereas login with username + password and token digits had become the strongest security protection. Nevertheless, most respondents still believed in the safety, trust, and confidence toward their existing online banking system and also agreed to the points that their bank should have increased or implicated more multilevel and complexity of security protection toward their online banking system with free of charge. Lastly, more of their opinions about online banking security also indicated in the same way of the results that banks should have increased and/or improved level of online banking security to protect against phishing.

4.6 Respondents' experiences in relation to online banking attacks

This section presents the analysis of the semi-structured and open-ended questionnaire reports of the respondents' experiences and their knowledge about phishing attacks and how to mitigate the risks. Due to the qualitative findings gathered, data cannot be analysed with any statistical degree of measurement. However, with a high volume of interview responses, the investigator has grouped similar viewpoints together and categorised them flexibly, based on the main keywords of the analysis. Findings are presented below in graphs or tables with their percentages and/or frequency values. Some questions included the ability to make more than one choice from the options named. The totals of frequencies and percentages may be varied according to the numbers of respondents who answered each question.

4.6.1 Interview question 1: Respondents' opinions toward any online banking threat

Table 4.6.1 Interview question 1: Knowledge about online banking threat

Responses	Frequency	Percent
Yes, I know	74	35.4
No, I do not know	25	12
Total	99	47.4

Table 4.6.1 displays the interview question that had been asked the respondents about any online banking threat that they had heard from different channels. Out of 99 interviewees, 74 respondents (35.4%) had heard of online banking threats whereas 25 respondents (12%) had never heard of any online banking threats. Respondents were asked further whether they had heard about any online banking threat and whether their information had come from media, friends or banks. ATM skimming device incidents were specifically excluded. Particular detail of what respondents knew or had heard will be discussed on the paragraph below.

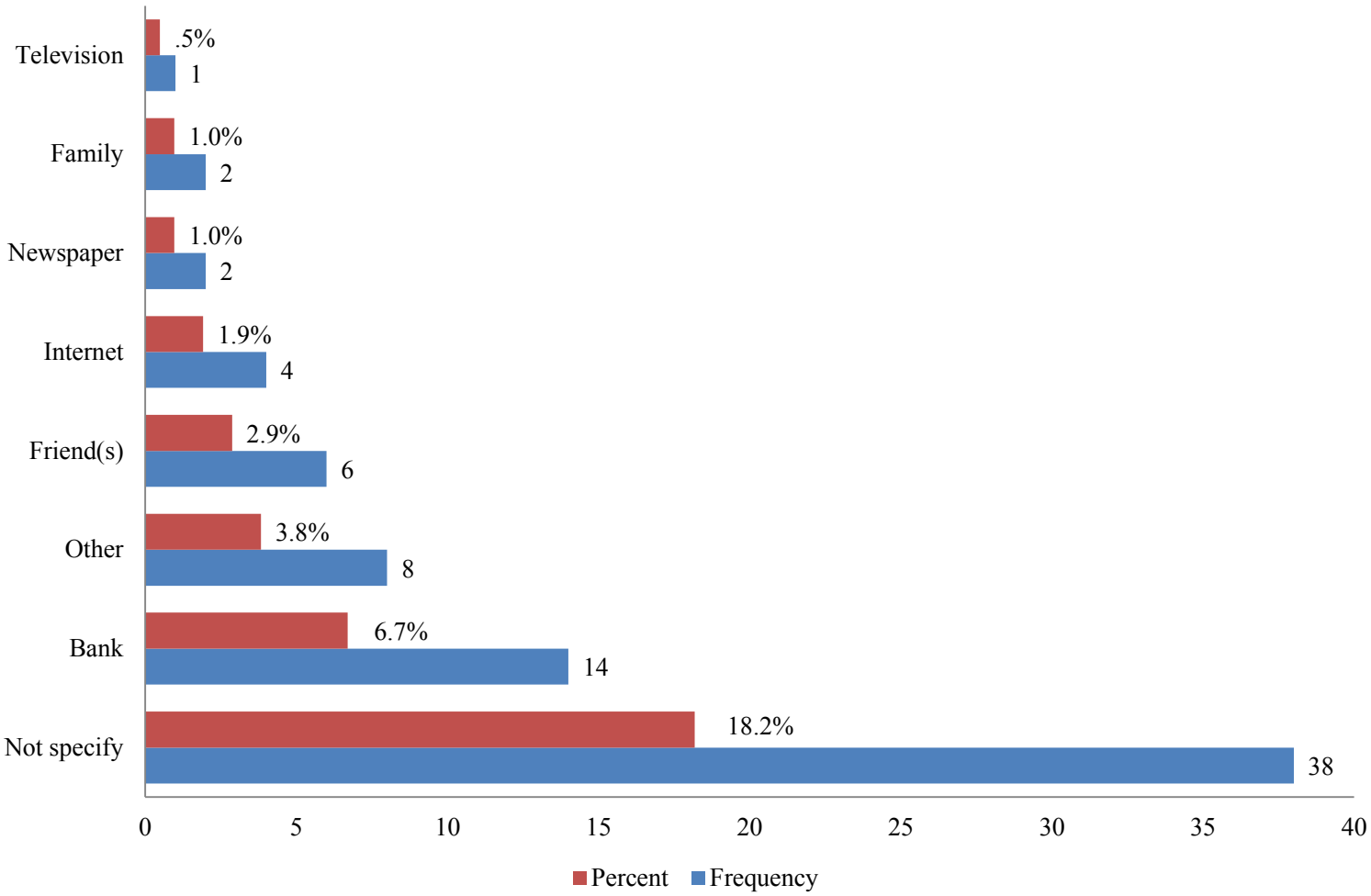


Figure 4.6.1 Channels of information obtained about any online banking threats

The graph shows that 14 respondents (6.7%) obtained information from a bank, while 6 respondents (2.9%) heard about online banking threats from friends. 8 respondents (3.8%) received information about online banking threats from other sources, such as school discussion, radio, and from published articles. It can be seen that the respondents had good connections to their banks in terms of receiving online banking security information.

Table 4.6.1.1 Main points about online banking threats that respondents knew or had heard

Responses	Frequency	Percent
Warning/ customers' awareness regarding online banking threats	10	4.8
Fraudulent e-mail pretending to be from bank and asking for bank account detail or security question.	10	4.8
Have heard from someone's experience where his/her credit card number or money has been transferred/ used/ stolen	7	3.3
Scam mail that may look like legitimate business requesting personal information (e.g., username & password)	5	2.4
Attacking users' computer system with installed malware application to manipulate, acquire or delete user's information for fraudulent purposes	5	2.4
Fraudulent website that may look like the legitimate bank, asking to click the link and provide information	2	1.0
Hacking into victim's account and transferring money to the scammer	2	1.0
Coming from Nigeria/ winning lotto/ charity that looks like a legitimate business to join or participate with them by providing some information	1	.5
Other, please specify...(uncategorised answers)	5	2.4
Other, please specify...(unrelated/ unclear answers)	4	1.9
Not specified	22	10.5
Total	73	34.9

Responses to the online banking threat question had been categorised according to the points respondents raised about their experiences which were shown in Table 4.6.1.1. 10 respondents (4.8%) received customers' awareness information about online banking threats by their bank's announcements. 9 respondents (4.4%) specified what

they knew or had heard about online banking threat that it was a fraudulent e-mail which pretended to be from a bank and asked recipients for account details or security questions. Interestingly, 7 respondents (3.3%), claimed to have heard about someone else's experience, such as their friends or families, whom their credit card number or money had been transferred, used, or stolen from the Internet. In addition, 6 respondents (2.9%) knew or had heard about online banking threats differently. The answers provided were:

(i) Yes, users information was disclosed to online & tele-sales as 'CONTACTS'.
(ii) Yes, bank security system attacks by hacker.
(iii) Identity theft - dangers of discarding bank statements etc without shredding.
(iv) I read an article that a number of years ago a computer in Asia was found to have all the customers banking details from a bank in Australia.
(v) From a friend originally from New Zealand. He said he gets phishing e-mails regularly.

It can be seen that most respondents knew, had heard, or had been informed about online banking security threats by their banks in most cases. The most frequent responses were about fraudulent e-mail pretending to be from the bank and asking customers for bank account details or security questions, and customers' awareness about online banking threat.

4.6.2 Interview question 2: Respondents' opinions about phishing

This question aimed to interview the respondents of what they knew or had heard about phishing.

Table 4.6.2 Interview question 2: Knowledge about phishing

Responses	Frequency	Percent
Yes, I know	36	17.2
Yes, I know (a little/ somewhat), but I am not so sure	30	14.4
No, I do not know	16	7.7
I am not sure	5	2.4
Other	8	3.8
Total	95	45.5

From the table above, 66 respondents (31.6%) believed that they knew or had heard about phishing whereas 16 people (7.7%) had never heard of phishing at all. Among the 66 respondents, 30 respondents (14.4%) of the entire group, knew or had heard about phishing vaguely, whereas 36 respondents (17.2%) had more confidence about their phishing knowledge. Only 5 respondents (2.4%) indicated that they were unsure if they really knew about phishing.

Table 4.6.2.1 categorises respondents' knowledge about phishing. 16% indicated that phishing was a fraudulent e-mail which pretended to be from a bank and asked recipients for bank account details or their security questions. 14.5% believed that phishing was a scammer who penetrated into victims' accounts, and stole and/or transferred money to the scammers' accounts without the victims' knowledge. 12% said that phishing was a fraudulent website that looked like a legitimate bank, and that asked a customer to click the given link to provide personal information. In contrast, 2.7% believed that phishing was malicious software which attacked users' computer systems and manipulated and/or stole users' information for fraudulent purposes. In addition, 9.3% provided different answers. Their answer pointed out roughly that phishing was a hack, a kind of illegal act, or a form of social engineering.

Table 4.6.2.1 Respondents' knowledge about phishing

Responses	Frequency	Percent
Fraudulent e-mail pretending to be from bank and asking for bank account detail or security question.	12	16.0
Scammer penetrates into victim's account and steals/ transfers money to the scammer's account	11	14.5
Fraudulent website that may look like legitimate bank, asking to click the link and provide information	9	12.0
Scam mail that may look like legitimate business requesting personal information (e.g., username & password)	6	8.0
Coming from Nigeria/ winning lotto/ charity that looks like a legitimate business to join or participate with them by providing some information	4	5.3
An illegal activity for the purpose of criminally attempting to acquire sensitive information such as usernames, passwords, and credit card numbers.	3	4.0
Malicious software attacks users' computer system and manipulate/ steal users' information for fraudulent purposes	2	2.7
Other, please specify...(uncategorised answers)	7	9.3
Other, please specify...(unrelated answers)	6	8.0
Not specify	15	20.0
total	75	100

The interesting point is that the main idea of phishing attack, in respondents' opinions, was more focused on the threat that imitated bank forms, either by e-mail or website versions, to entice customers into revealing their personal information. These combinations were 28% compared to all kinds of phishing activities.

The answers that the respondents had mentioned about phishing were: fraudulent e-mail pretending to be from the bank, penetrating into user's account to steal money, and fraudulent websites that look like legitimate bank were the main answers respondents mentioned. To ensure that their knowledge were sufficient enough in terms of the acts of phishing, the research has quoted most common acts of phishing under 3 circumstances defined by the Commonwealth of Australia (2011b) as follows:

‘Phishing’ refers to e-mails that trick people into giving out their personal and banking information; they can also be sent by SMS. These messages seem to come from legitimate businesses, normally banks or other financial institutions or telecommunications providers. The scammers are generally trying to get information like your bank account numbers, passwords and credit card numbers, which they will then use to steal your money.

Phishing e-mails often look genuine and use what look to be genuine internet addresses—in fact, they often copy an institution's logo and message format, which is very easy to do. It is also common for phishing messages to contain links to websites that are convincing fakes of real companies' home pages.

The website that the scammer’s e-mail links to will have an address (URL) that is similar to but not the same as a real bank's or financial institution’s site. For example, if the genuine site is at 'www.realbank.com.au', the scammer may use an address like 'www.realbank.com.au.log107.biz' or 'www.phoneybank.com/realbank.com.au/login'.

4.6.3 Interview question 3: Respondents’ opinions about malicious attack

The purpose of this question was to explore the respondents’ opinions about spyware, adware, and Trojans.

Table 4.6.3 Interview question 3: Discussion about malicious threats

Responses	Frequency	Percent
Yes, I know	9	4.3
No, I do not know	17	8.1
Yes, I know (a little/ somewhat), but I am not so sure	55	26.3
I am not sure	5	2.4
Other	4	1.9
Total	90	43.1

From the table above, 64 respondents (30.6%) believed that they knew or had heard about malicious software whereas 17 respondents (8.1%) did not understand this

terminology. However, among the knowledge answers, 55 respondents considered that they knew or had heard about malicious software slightly, whereas 9 respondents (4.3%) had more confidence with their knowledge. Only 5 respondents (2.4%) were unlikely to indicate the malicious definitions. Results of respondents' knowledge of each term will be displayed in a table below.

As shown in table 4.6.3, 9 respondents (4.3%) indicated their knowledge that spyware was a software attack that secretly monitored users' computer and collected/manipulated personal information, or interfered with users' computer controls. On the other hand, 5 respondents (2.4%) believed that spyware was a virus, or a program used for detecting viruses, or something that could damage users' computers. In addition, 8 respondents (3.8%) stated their belief that adware was a form of pop-up or any software package which automatically played, displayed, or downloaded advertisements to a computer. Some types of attacks were integrated with the spyware designed to interfere with users' computers or to gain personal information. In contrast, 3 respondents (1.4%) believed that adware was a kind of security protection for detecting viruses, or something that collected users' information in order to sell it to marketers. Besides, 11 respondents (5.3%) said that Trojans were harmful pieces of software that looked legitimate and allowed an attacker to gain remote access to a target computer system and perform various unwanted/unauthorised operations. On the contrary, 4 respondents (1.9%) claimed that Trojans were the most serious virus and very difficult to remove, or they were the same type of viruses or spyware applications that allowed people to detect the victim's password.

Table 4.6.3 Respondents' opinions about malicious definitions

	Spyware	Frequency	%	Adware	Frequency	%	Trojan Horses	Frequency	%
Responses	Software that secretly monitors users' computing and collect/ manipulate various types of personal information or interfere with users' computer controls.	9	4.3	A form of pop-up or any software package which automatically plays, displays, or downloads advertisements to a computer. Some may integrate with spyware purposed for interfere users' computer or gain personal information.	8	3.8	Harmful pieces of software that looks legitimate and may allow an attacker remote access to a target computer system and perform unwanted/ unauthorised various operations.	11	5.3
	Other, please specify	5	2.4	Other, please specify	3	1.4	Other, please specify	4	1.9
	I don't know			Frequency = 18			Percent = 8.6		
	Not specify			Frequency = 3			Percent = 1.4		
	I am not sure			Frequency =4			Percent = 1.9		
	Total	39	18.7	Total	36	17.2	Total	39	18.7
Missing	No opinion			Frequency = 5			Percent = 2.4		
	No answer			Frequency = 116			Percent = 55.5		
	Not applicable	49	23.4	Not applicable	52	24.6	Not applicable	49	23.4
	Total	170	81.3	Total	173	82.8	Total	170	81.3
Total responses		209	100.0	Total responses	209	100.0	Total responses	209	100.0

However, for the three different types of malicious software, the percentage of the respondents who did not know some of those definitions were 8.6%, while 1.4% did not specify what they knew or had heard, and 1.9% were not really sure how to describe what they had heard or knew about all three terms.

4.6.4 Interview question 4: Respondents' opinions on how personal information can be stolen from the Internet

The purpose of this question was to ask respondents what they knew about ways that personal information could be stolen from the Internet. Of 86 interviewees, or 41.1%, 63 respondents (30.1%) of the total group, believed that they knew how personal information could be stolen from the Internet. Conversely, 13 respondents (6.2%) believed that they knew nothing while 5 other respondents (2.4%) were unsure. Details from respondents of what they believed that they knew or have heard will be discussed below.

Table 4.6.4 Respondents' opinions about how personal information can be stolen from the Internet

Respondents' opinion about ways of personal information can be stolen from the Internet	Frequency	Percent
Malicious software attacks installed in unprotected/vulnerable computer	21	25.6%
Visiting untrustworthy/counterfeit websites which look legitimate and may have become infected with Trojans	9	11.0%
Scam mail that may look like legitimate business requesting personal information (e.g., username & password)	7	8.5%
Negligent user	3	3.7%
Visiting unsecured websites	2	2.4%
I do not know	14	17.1%
I am not sure	4	4.6%
Other, please specify...(uncategorised answers)	10	12.2%
Other, please specify...(unrelated/ unclear answers)	6	7.3%
Not specify	6	7.3%
Total responses	82	100.0%

Table 4.6.4 shows respondents' opinions about ways in which personal information can be stolen from the Internet. 21 responses (25.6%) of the total group, focused on the malicious software attacks installed in unprotected/vulnerable computers, while visiting untrustworthy/counterfeit websites which looked legitimate and could be active with Trojans had 9 responses (11%). 7 respondents (8.5%) believed that information could be stolen by a scam mail that seemed to be a legitimate business e-mail requesting personal information, such as username and password. On the other hand, 16 respondents (19.5%) indicated that personal information could be obtained from search engine caches, downloaded files which were corrupted or contained viruses, or data could be sent away using common protocols, e.g. cross site scripting and buffer overflow, and acts of identity theft.

4.6.5 Interview question 5: Using a combination of letters and numbers in passwords can protect an online banking account

This question asked respondents' opinions about the use of a combination of numbers and upper and lower case characters in their passwords to help protect them from an online banking scam.

Table 4.6.5 Interview question 5: Using a combination of passwords can help people from an online banking scam

Responses	Frequency	Percent
Yes	56	26.8
Yes, perhaps. However/ If	24	11.5
Yes, I think (a little/ somewhat), but I am not sure	2	1.0
No	10	4.8
Neither Yes nor No	7	3.3
I do not know	4	1.9
Total	103	49.3

82 respondents (38.3%) of the total group, believed a combination of characters could mitigate the risk from online banking scams. However, 2 respondents agreed generally, but were unsure about their answers, while 24 respondents (11.5%) believed that the use

of a combination of upper and lower case letters and numbers was definitely safe, but depended on the situation. On the other hand, 10 respondents (4.8%) believed that such a combination of characters was not secure at all. 4 respondent were unsure about this question, and 7 people chose neither Yes nor No. More details about respondents' opinions will be outlined below.

Even though a majority of respondents agreed to this concept, because they believed that it was a good idea and would definitely protect them from online banking scams, there were two main reasons why some resisted this idea. Firstly, there were some who answered 'yes' conditionally. The reasons they gave were:

(i) It was secure, but it was hard to remember.
(ii) It was secure, but it was ineffective if other types of scam attacks occur.
(iii) It was secure only if the password has been changed regularly.
(iv) It was secure, but it could be very complicated for the customers.
(v) It was securing, but not only relying on using alphabets recognition.
(vi) Secondly the 10 people, who disagreed that complex passwords would offer sufficient protection, offered reasons which were very similar to those given by respondents who had agreed conditionally:
(vii) It was too hard to remember.
(viii) It was not enough protection as a phisher could still gain access to the system.
(ix) It was not strong protection as a phisher could still figure it out.
(x) It was too complicated and too confusing.
(xi) It was so unuseful with this method.

While the majority of respondents agreed with the use of combination passwords, the minority seemed to be unsure whether using such passwords could secure their online banking. If passwords are too complicated to memorise, using them on their own will not be enough to protect respondents' banking accounts.

4.6.6 Interview question 6: Using date of birth or phone number as a password is insecure

This question reveals 110 respondents' opinions, for 52.6% of the total group, about whether using a password containing customers' personal details such as dates of birth or phone numbers is insecure.

Table 4.6.6 Interview question 6: Respondents' opinions about using date of birth or phone number as a password is insecure

Responses	Frequency	Percent
Yes	88	42.1
No	14	6.7
I do not know	1	0.5
Yes, perhaps. However/ If	5	2.4
Neither Yes nor No	2	1.0
Total	110	52.6

From table 4.6.6, 88 respondents (42.1%) believed that using personal information as a password is insecure. However, 5 respondents (2.4%) slightly believed it was secure but they were unsure about it. On the other hand, 14 respondents (6.7%) believed that personal information was too weak to be used as a secure password. Further discussion of this question will be mentioned in the paragraph below.

A majority of respondents agreed to this statement because they believed that any types of personal information which were used as a password were very insecure. However, 2 respondents who neither agreed nor disagreed believed differently. To begin with the first conditional agreement, this group of people agreed to answer 'yes, it was insecure; however,...' the supporting reasons for this answer are included below:

(i) It is insecure if it is accessible by the public.

(ii) It is insecure if types of personal information such as date of birth or phone number have been used in conjunction with other knowledge such as hard drive number, ISP, or Domain name.

The respondents who believed in using personal information in passwords seemed to feel secure. They thought the password would be safe as long as it was not accessible by public viewers or used in conjunction with other registered identification.

4.6.7 Interview question 7: Discussion about opinions if changing password every 3-6 months can protect their online banking account from phishing

Answers to this question revealed 105 valid respondents' opinions, from 50.2% of the total group, about whether changing their password every 3-6 months could protect their online banking account from phishing.

Table 4.6.7 Interview question 7: Respondents' opinions about changing password every 3-6 months to protect their online banking account from phishing

Responses	Frequency	Percent
Yes	35	16.7
No	33	15.8
Yes, perhaps. However/ If	26	12.4
Yes, I think (a little/ somewhat), but I am not sure	4	1.9
I do not know	5	2.4
Neither Yes nor No	2	1.0
Total	105	50.2

The above table shows that 65 respondents (31%) of the entire group, believed that changing passwords every 3-6 months could protect their online banking account from phishing. However, among these numbers, 4 respondents (1.9%) slightly believed it was a good idea, even if they still were unsure about it. 26 respondents (12.4%) in contrast preferred to believe conditionally and 35 respondents (16.7%) had more confidence in their agreements. On the other hand, 33 respondents (15.8%) disagreed with this statement. Further discussion of this statement is presented below.

A majority of respondents, who agreed to this concept, believed that it was more secure than using unvarying passwords. However, respondents who agreed conditionally proposed that:

(i) It seems to be secure, but it is very impractical for customers.

(ii) It is secure, but it is hard to remember.

(iii) It is secure, but it still can be guessed easily.

(iv) It could be secured only some sorts of attacks.

(v) It is secure as long as the user's computer is also secure.

(vi) It may help, but there should be other protection available to use as well.

(vii) It is good idea, but very confusing.

(viii) It would help, but still can be too late if password had already been taken.

(ix) It is good idea, but not convenient.

(x) Yes, it would be more secure if password had been changed more often that the statement pointed out.

(xi) Yes, it would help, but it would be better for customers to change their passwords without banks requiring that it should be done in a certain time.

On the contrary, those who disagreed indicated their reasons, which were similar to the conditional agreement reasons, that:

(i) It cannot protect as it seems. There should be other protection available to protect customers.

(ii) It is unhelpful unless it has been changed every time after log off.

(iii) It is so confusing to keep changing.

(iv) It should be the bank's responsibility to secure customer with their proper protection without asking customers to take the trouble.

(v) No it is easily to retrieve.

(vi) No, users should be aware of the danger by themselves.

It appears that, while the majority of respondents agreed to change their password periodically, the minority seemed to be unsure that using combinations of passwords could secure their online banking. They believed it was very impractical for them to memorise passwords, when other additional protections still needed to be applied.

4.6.8 Interview question 8: Respondents' experiences in receiving an e-mail from a bank and asking respondents for confidential information

The question reveals 109 valid respondents' opinions, or 52.2% of the total group, about experience in receiving an e-mail from banks and asking for confidential information.

Table 4.6.8 Interview question 8: Discussion about experience in receiving an e-mail from a banks and asking for confidential information

Responses	Frequency	Percent
No, I have not	71	34.0
Yes, I have	34	16.3
I am not sure if I have or I have not	1	.5
Other	3	1.4
Total	109	52.2

From table 4.6.8, 34 respondents (16.3%) had experience with receiving an e-mail which pretended to be from a bank whereas 71 respondents (34%) had never received one. In addition, 3 respondents (1.4%) did not specify in their answers whether they had or had not received such an e-mail. The table below illustrates respondents' reactions when they received the scam e-mails.

Table 4.6.8 illustrates reactions from respondents when they received e-mails that requested users' confidential information. It shows that 15 respondents (7.2%) deleted a scam e-mail while 7 respondents (3.3%) just ignored it. Moreover, 6 respondents (2.9%) preferred to contact their bank to verify the matter. On the other hand, those who had never received scam e-mails indicated that if they had received one, they would have contacted their bank immediately.

However, respondents who had never received the scam e-mail also said that if they had received one, they would have checked their e-mail address to see if that e-mail was reliable or not, or they would have contacted their bank immediately. 1 respondent, who was not sure if she or he had received an e-mail or not, indicated her/his belief that

encryption is the best answer for any electronic correspondence containing highly sensitive information.

Table 4.6.8.1 Discussion about reaction of receiving e-mail requesting for confidential information

Responses	Frequency	Percent
Yes. Deleted it.	15	7.2
Yes. Ignored it.	7	3.3
Yes. Contacted bank to verify.	6	2.9
Yes. But not specify the solution.	3	1.4
Yes. Deleted the e-mail & contacted the bank.	2	1.0
Yes, I just did as the bank told me.	1	.5
Yes. I have deleted most of them. Once I sent it through to the bank to let them know.	1	.5
Yes. Ignored the e-mail and contacted the bank.	1	.5
No, their letter said they would never do this. It is happens, I will check the mail address first.	1	.5
No. but my first step if I was I would contact my bank immediately.	1	.5
No. If I did, I will call my bank personally to verify before providing the information required.	1	.5
No. if it occurs, I will check whether it is reliable or not.	1	.5
Nope, and I would do it if I received a mail like that. I would directly go to the bank to confirm authenticity of that mail.	1	.5
Not sure. I cannot remember but I do think that encryption is the best answer for any electronic correspondence containing highly sensitive information.	1	.5
Uncategorised answer: Bank e-mails will not provide direct link to the login page. Uncategorised answer: Somewhere in the content of genuine e-mail from bank will advise all users to log on a fresh page.	1	.5
Uncategorised answer: If the e-mail has asked for information, it is a scam.	1	.5
Total	44	21.1

On the other hand, 3 respondents, who did not indicate whether they had received the scam e-mail or not, stated that bank e-mails would have never provided a direct link to the login webpage; in addition, if any e-mail asked for personal information, it could be assumed that it was a scam.

4.6.9 Interview question 9: Discussion about ways to determine a legitimate e-mail

The question reveals 103 respondents' opinions (49.3%) of the entire group, about how to determine whether e-mails, which appear to be from banks, are scam e-mails.

Table 4.6.9 Interview question 9: Discussion about ways to determine a legitimate e-mail

Responses	Frequency	Percent
I do know how to determine if an e-mail is a scam	87	41.6
I do not know	6	2.9
Neither know nor not know	5	2.4
I am not sure	3	1.4
I know (a little/ somewhat), but I am not sure	2	1.0
Total	103	49.3

Table 4.6.9 shows that 87 respondents (41.6%) indicated that they believed they knew how to determine a legitimate e-mail while 2 respondents (1%) believed that they may have known how to verify a little bit of the difference, and 3 respondents (1.4%) were not sure if they really knew or not. Whereas there were 6 respondents (2.9%) did not know how to determine the legitimate e-mail at all and another 5 respondents (2.4%) who did not specify whether they knew or not.

Figure 4.6.9 displays methods which respondents indicated were the ways used to verify their incoming e-mails. It can be seen that 14 respondents (14.4%) preferred to contact their bank regarding their receiving e-mail and to verify the legitimate e-mail from the bank; however, 13 respondents (13.4%) chose to believe themself by checking the correct e-mail address, whereas 7 responses (8.2%) chose to check e-mail content. The numbers of people chose to check only contact details, and chose to ignore unusual e-mail had the equivalent percentages at 7.2% or 7 responses.

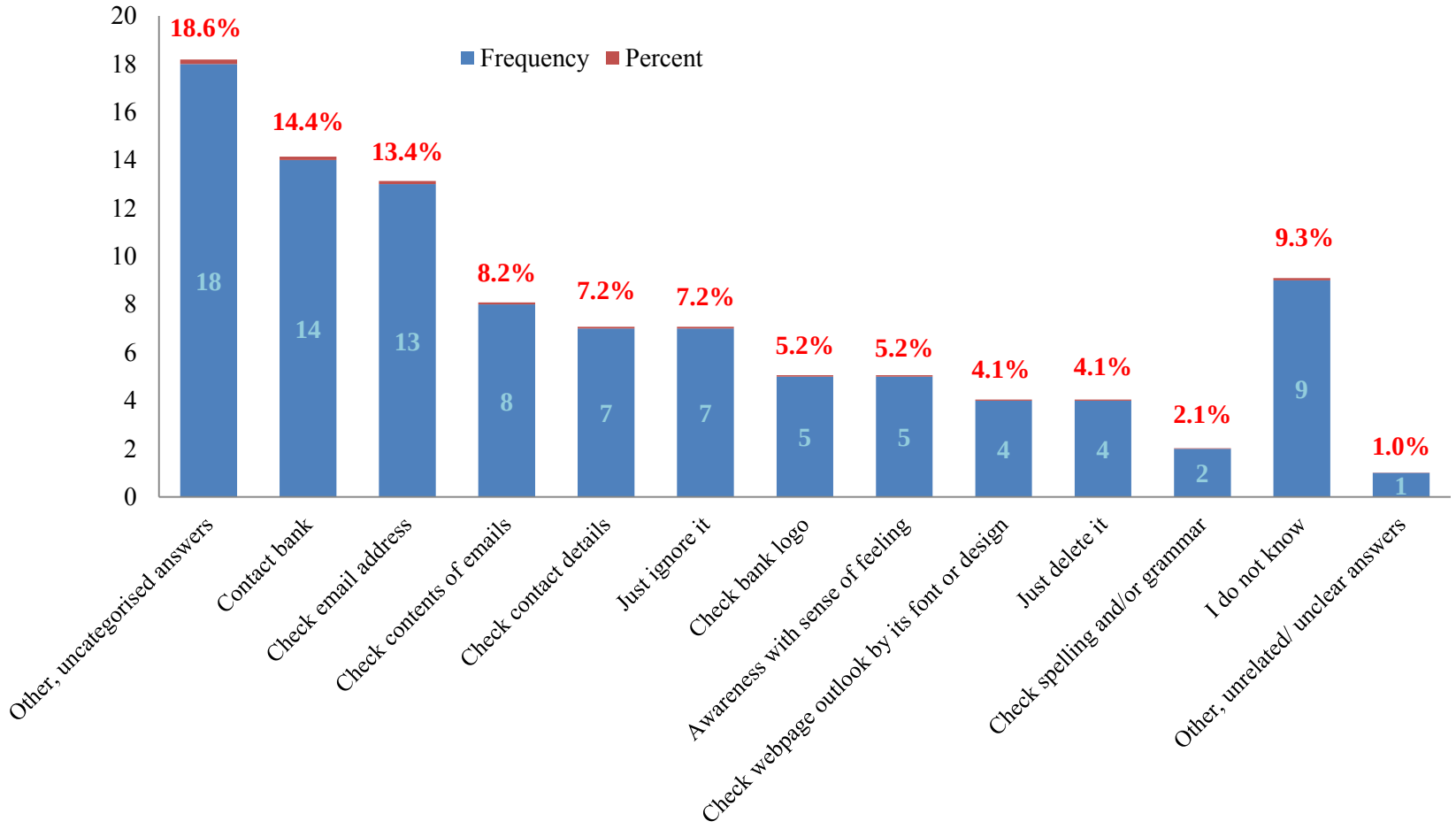


Figure 4.6.9 Respondents' determination of a legitimate e-mail

On the other hand, there were 9 respondents who indicated that they did not know how to check a legitimate e-mail; 6 respondents from the group who chose 'I do not know', and 3 respondents chose the 'I am not sure' option. In addition, there were 18 responses or 18.6% of the answers which were included in the miscellaneous group. Their answers have been illustrated below:

(i) They are not asking for my personal information. I have also introduced by bank that any e-mails need to include the address employee no. as well as their contact phone number.

(ii) Check with your ISP and the ASIC website.

(iii) Code and lock Sign.

(iv) I don't check e-mails from Internet banking.

(v) I receive my e-mails inside online banking log on as well as my personal e-mail address.

(vi) If bank only sends a statement or advertisement but no website attached, I think it is not a scam.

(vii) Just by giving a reply.

(viii) Read e-mail or compare real site.

(ix) The topic of e-mail which indicates the name of the bank and makes me know that is the e-mail from bank.

Statements above reveal some additional ways of how respondents determine a legitimate e-mail and decide whether it is a scam or not. If analysing the contents of the various methods, it can be seen that respondents chose to check the lock icon, verify with their ISP or the reliable website, to determine from the subject heading of the e-mail or did not check e-mail from the bank at all. From the overall results, it can be seen that most respondents know how to determine between a legitimate e-mail and a scam e-mail.

4.6.10 Interview question 10: Discussion about ways to distinguish a legitimate online banking website

The question illustrates 94 or 45% participated respondent's opinion regarding methods to distinguish a legitimate online banking website.

Table 4.6.10 Interview question 10: Discussion about ways to distinguish a legitimate online banking website

Responses	Frequency	Percent
I did know how to distinguish	62	29.7
I did not know	17	8.1
I am not sure	7	3.3
I knew (a little/ somewhat), but I was not sure	5	2.4
Other	3	1.4
Total	94	45.0

The result shows in the table above that 67% of the respondents knew how to verify the genuine website. 5 respondent (2.4%) of the entire group, believed that they had little knowledge of how to check the legitimate website, whereas 62 respondents (29.7%) had more confidence in identifying the legitimate website. On the other hand, 17 respondents, or 8.1%, did not know how to distinguish the website, whilst 7 respondents (3.3%) were not sure whether they really knew or not. 3 respondents (1.4%) defined other opinions. Various methods that respondents used to distinguish the legitimate website are discussed below.

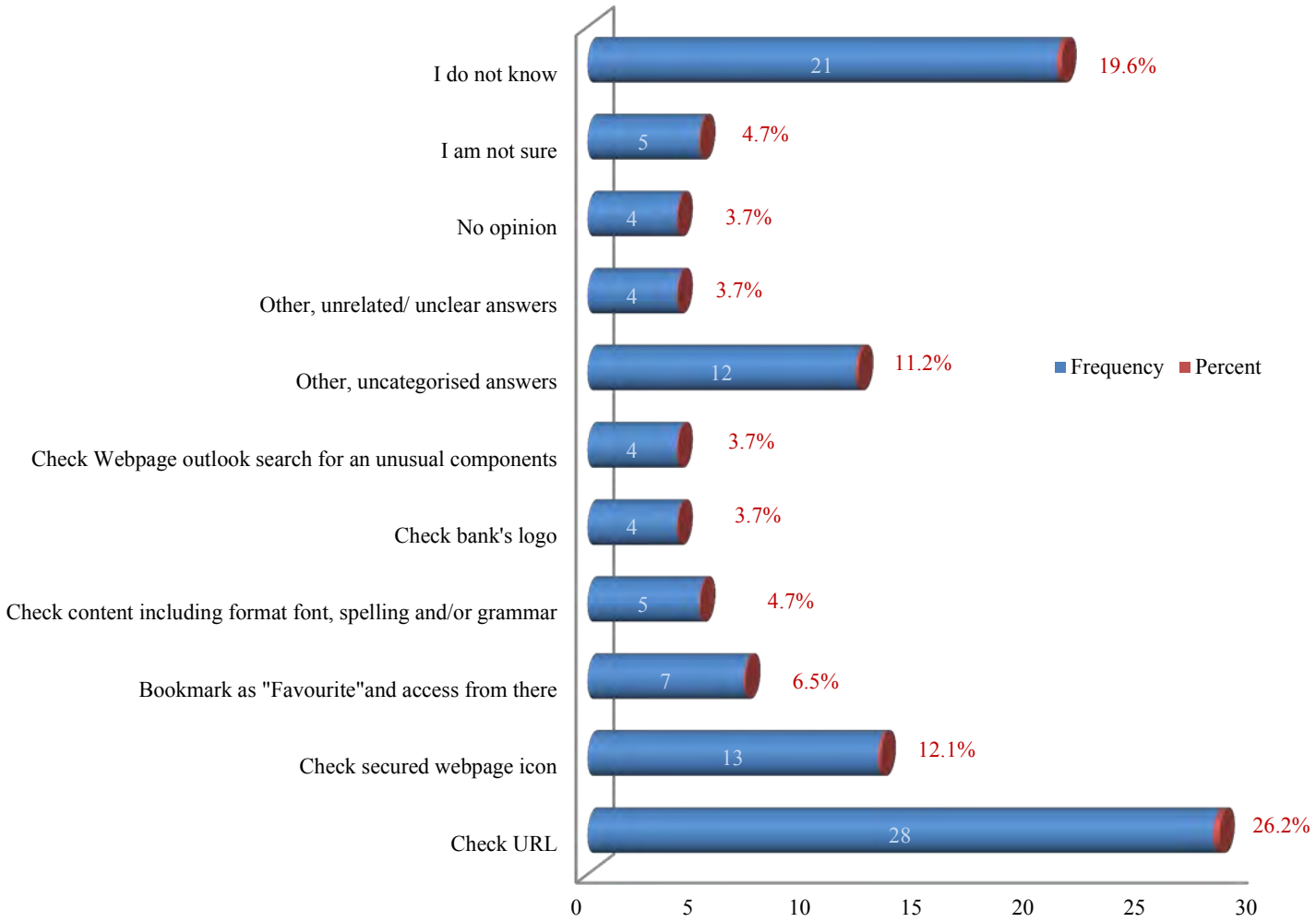


Figure 4.6.10 Respondents' distinguishing about legitimate webpage

Figure 4.6.10 displays various methods respondents used to distinguish a legitimate online banking webpage. 28 respondents (26.2%) focused on checking the correct web address, followed by 13 respondents (12.1%) who would check a secured webpage icon with its authorised coloured address bar. 7 respondents (6.5%) verified the legitimate webpage by accessing via favourite bookmark and 5 respondents (4.4%) checked for contents including font, spelling, and grammar. Alternatively, 21 respondents (19.6%) did not know how to distinguish, while other 12 respondents (11.2 %), had additional ways to inspect their legitimate webpage as listed below:

(i) By using the information given to me by the bank i.e. Netbank etc.
(ii) Never go through a link attached to an e-mail.
(iii) Just go to the government web site to check.
(iv) The online banking webpage can only be connected to from the official bank website. Takes a long time to go through security protocols.
(v) Sometimes the bank tells you. But one way to know is also that the sequence of process differs from the usual way I have been doing or accustom to.

According to the Australian Department of Broadband, Communication and the Digital Economy (n.d.) there are indicators which tell if a website is secure:

(i) The banks digital certificate is present and valid.
(ii) The web address includes https:// instead of http://
(iii) A locked padlock or key appears in the browser window.

From the overall results, it can be seen that even though most respondents believed they had knowledge of distinguishing the legitimate website whether it was from a bank or delivered by a phisher, only 12.1% of 67% of the respondents had knowledge that were in line with the government recommendations. The most common method that they used to verify the legitimate webpage was checking the web address.

4.6.11 Interview question 11: Respondents' experiences of phishing attacks.

Victimisation rates for identity fraud, across Australia and its territories, have increased from 2007 to 2011 as shown in figure 4.6.11.1. Specifically, the number of victims of identity fraud increased among the states within four years, from 56,100 victims (3.5%) in 2007 to 95,500 victims (5.3%) in 2010-11.

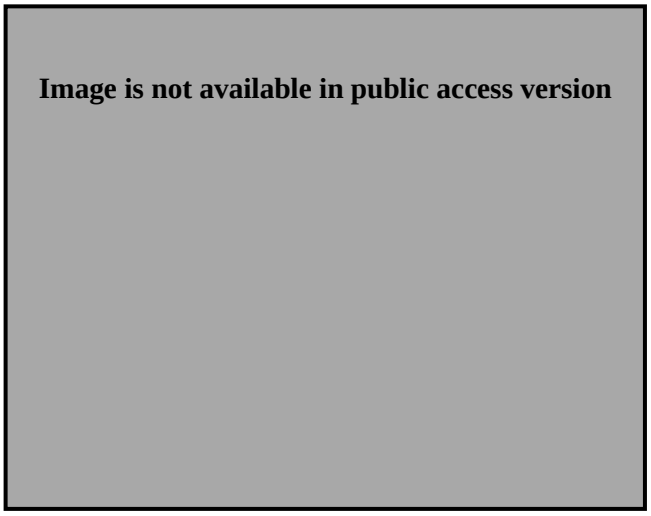


Figure 4.6.11.1 Identity fraud victimisation rates by state/territory, 2007 and 2010-11 (Australian Bureau of Statistics, 2012)

In this survey, 5 females had experience in phishing attack whereas 4 were found in males. The data found was similar to the ABS result where females in Western Australia were more likely to be victims of identity fraud (56,200 victims) than males (39,400) (Australian Bureau of Statistics, 2012).

Table 4.6.11 below distinguishes between those respondents who had experience of an online banking attack and those who had not.

Table 4.6.11 Interview question 11: Respondents' experiences in phishing attacks

Responses	Frequency	Percent
No, I have not	84	40.2
Yes, I have	9	4.3
I am not sure if I have or I have not	5	2.4
Total	98	46.9

The result shows that only nine respondents (4.3%) had experience of an online banking attack. Another five respondents (2.4%) were unsure whether they had been targeted by a phishing attack and thought they would have needed to check with their bank. A majority of the respondents, 84 people (40.2%) believed they had never been attacked by a phisher. However, those who had experienced provided more detailed information, as given below.

Table 4.6.11.1 shows respondents' experiences regarding phishing attacks. It found that only one respondent had knowledge of his sister's account being attacked and her credit card had been used by an unauthorised person. Respondents for the remaining 8 cases were found and notified by their bank that someone was trying to access their account and to withdraw their money to spend without their permission.

Table 4.6.11.1 Respondents' experiences of phishing attacks

Responses' opinions	Frequency	Percent
Credit card yes, bank alerted us & cancelled transaction & used new card.	1	.5
I had only one of my account hacked and a phishing site was installed. Westpac called me and I changed my password and deleted the phishing directories.	1	.5
Yes, because I have lost my money for $3,000 from online banking.	1	.5
Yes, I noticed a small transaction appearing on my credit card once a month. I called the bank and had my card replaced.	1	.5
Yes, my NAB had been hacked when I booked the air ticket. The hacker came from Greece.	1	.5
Yes, the bank's fraud division told me that someone from New York was using my Visa for shopping.	1	.5
Yes. I have only been contacted once because someone was trying to use my credit card in another province. The bank suspected it was fraud, they contacted me and I assured them the purchaser was not me. I then immediately cancelled the credit card and received a new one.	1	.5
Yes. I periodically view my banking details. I once noticed that only 1 cent or 2 cents had been deducted from my account. I immediately contacted my bank.	1	.5
No, not mine. But twice with my sister's account had been attacked. We went to the bank and explained that we have not used credit card. It used by unauthorised person and bank investigated.	1	.5
Total	9	4.3

4.6.12 Interview question 12: Respondents' financial impacts from phishing attacks

11 respondents to this question (5.3%) revealed they had experienced online banking attacks which had had a financial impact. The question focused on whether the attacker was successful in obtaining anything from their accounts.

Table 4.6.12 Interview question 12: Discussion whether the attack was successful in obtaining anything from respondents' accounts

Responses	Frequency	Percent
Yes, it was	6	2.9
No, it was not	3	1.4
I am not sure if it was or it was not	2	1.0
Total	11	5.3

The result shows 6 respondents (2.9%) who acknowledged that their accounts had been attacked successfully, whereas 3 respondents (1.9%) had not lost anything from their accounts, although they were aware that they had been attacked. In addition, 2 respondents were not sure if the phishing attack was successful or not. Their situations are outlined below:

(i) I didn't see anything on the statements but they had apparently made secure purchases.

(ii) Obviously, they had deducted $2-$3 each time for about 2 months – all ended up around $40.

(iii) Yes, because I have lost my money for $3,000 from online banking.

(iv) Yes, he used her credit card twice.

(v) Yes, the hacker took $5,000.

(vi) Yes. 1 cent or 2 cents had been deducted from my account.

The answers above show various successful phishing activities which may be categorised into three attack methods: a small amount of money has been deducted regularly, credit has been used for unauthorized purchases, and larger sums of money has been taken out of the bank.

4.6.13 Interview question 13: Discussion of attempts to use personal information for other fraudulent purposes

10 respondents answered the question about whether they thought an attacker was successful in attempting to use their personal information for other fraudulent purposes. Examples given were that the personal information could be used for claims for medical care, a job, or government benefits, for renting accommodation, or giving misleading information to the police if criminals were charged with crimes or traffic violations.

Table 4.6.13 Interview question 13: Attempts by phishers to use personal information for other fraudulent purposes

Responses	Frequency	Percent
I am not sure if it was or it was not	4	1.9
Yes, it was	3	1.4
No, it was not	3	1.4
Total	10	4.8

3 respondents (1.4%) disclosed that they had suffered from the use of information obtained by phishers. One person whose personal information had been obtained had had her family called by the phisher who was hoping to get money:
I was contacted on Saturday at 6.00pm from a 'bank' and asked about personal details. I discontinued the phone call and contacted my bank in the next working day.

In this case, the respondent believed that her online banking had never been attacked by a phisher. However, she stated that her information was obtained by someone via the Internet and used her information to call up her family and ask for further personal details.

In addition, in a second case, the credit card of the respondent had been used somewhere the authorised owner had never visited.

(i) Yes, credit card details was claimed to use in a place where I have never been to.

Lastly, although having been the subject of a phishing attack, another victim was in doubt if his situation was caused by the phishing attack or not. His license plates were subsequently stolen from his car, which may have been because the thieves had found his address during the phishing attack.

(ii) Not via banking; however, did have license plates stolen from my car which was then be used on another car without the police checking their own details. It was claimed to be my car which meant they felt I was liable for the costs.

4.6.14 Interview question 14: Discussion about vulnerabilities of online banking.

This question aimed to obtain respondents' opinions about the vulnerabilities associated with online banking that could lead to a phishing attack.

Table 4.6.14 Interview question 14: Respondents' opinions about the vulnerabilities of online banking.

Responses	Frequency	Percent
User ignorance	41	41.4
Bank security	12	12.1
Unsecure user's computer	8	8.2
Password	7	7.1
Unsecure website	3	3.0
Unsecure e-mail/ phishing e-mail	2	2.0
Other(s), please specify	6	5.8
No opinion	8	8.2
I do not know	7	7.1
I am not sure	5	5.1
Total responses	99	100.0

Table 4.6.14 illustrates the 99 respondents' views about the vulnerabilities of online banking. User ignorance was thought to be the most vulnerable aspect of online banking attacks, with a percentage of 42.3%, followed by bank security at 12.1%. 5.8% offered additional details, which are included below:

(i) Banking policies including user right to get access to the information.
(ii) Government policies to deal with system penetrator.
(iii) Minor responsibilities go to cyber operators too.
(iv) There was an incident regarding this matter.
(v) Some responsibilities to ISPs. If only ISPs have strong firewall or other security measures, it could be remarkably reduced.
(vi) By requesting details using offer that may appear too good to be true.
(vii) Getting the person's personal information.
(viii) Good copy version which is similar to others.
(ix) Not enough security.
(x) Too complex to remember, in action.

The above statements display respondents' opinions toward vulnerabilities that could lead to successful online banking attacks. Some respondents were concerned about too simple or too complex levels of security protection. Some also focused on the need for information and policies from responsible people or organisations to increase so that users of online banking could become more aware of ways of dealing with security vulnerabilities.

4.6.15 Interview question 15: What respondents would do to protect themselves or solve problems caused by phishers

The question reveals respondents' opinions about various ways to protect themselves from online banking attacks or solve the problems resulting from phishing attacks.

Table 4.6.15 Interview question 15: Discussion about methods that respondents used, or would use, to protect themselves or to solve the problems caused phishers.

Responses	Frequency	Percent
What I did/would do was (is)	60	28.7
I don't know	2	1.0
Other	2	1.0
Total	64	30.6

It can be seen that only 2 respondents (1%) did not know how to prevent or solve the problems caused by online banking attacks at all, whereas 60 respondents (28.7%) believed they knew how to work against the attack. Below are respondents' opinions about ways to counteract online banking scams and or phishers.

Figure 4.6.15 above shows methods in which respondents chose to mitigate risk and protect themselves from online banking attack. 31 responses (39.7%) chose to believe in self-awareness in security, for example, to check for any suspicious activities on their online banking account and their computer device. Besides, the result in Figure 4.6.15 illustrates that 13 respondents (16.7%) contacted their bank and informed it about any suspicious activity in their online banking account or an e-mail which pretended to be from the bank and asked for confidential information.

Interestingly, installing software protection, detection or monitoring software was chosen by only 8 respondents (10.3%). The method was followed by changing passwords periodically with the percentage of 9.2%. Other methods that respondents used, or would use, are listed below:

(i) Changed to a bank which has better online security.

(ii) Delete any e-mails from banks. If I need information I phone them or login to my online banking facility.

(iii) Do not use online banking.

(iv) I delete or ignore all phishing.

(v) Keep my security program up to date.

(vi) I did not do anything.

Most banking phishing (that I know of) is by fake mails from bank with links to phishing sites. I don't use links from bank e-mails.

Rang the people and got their details i.e. full name, employee numbers, and requested that they take the suspicious matter up with their supervisors. Then I requested a follow up and call from their supervisor as well as a letter of apology.

The statements above display all the uncategorised solutions that respondents chose to react to a phishing attack. Interestingly, 3 responses (1.4%) believed that they did not do anything regarding the phishing protection. Other responses were provided, based on their respondents' perceptions, which included deleting any e-mails from banks and waiting to be contacted in person, stopping using online banking, deleting or ignoring all phishing attacks, to keep updating security applications, maintaining a complex password and changing to better online banking security.

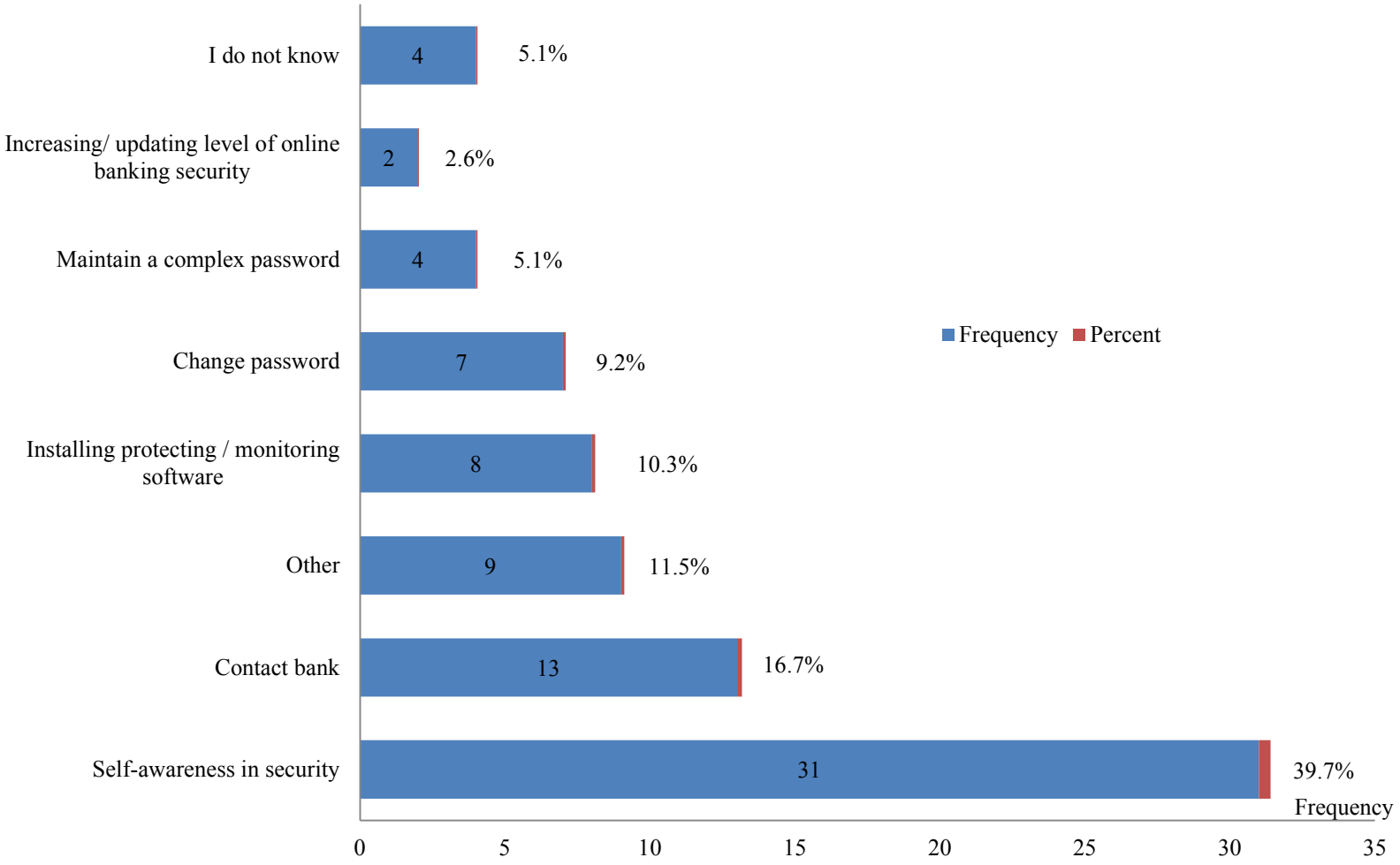


Figure 4.6.15 Method respondents used, or would use, to protect themselves from phishing attacks

4.6.16 Interview question 16: Installing an anti-malware application is enough to protect the user's computer from being attacked.

The table below illustrates respondents' reactions to the suggestion that installing an anti-malware application provides enough security to prevent users' computers from being attacked.

Table 4.6.16 Interview question 16: Respondents' opinions about installing an anti-malware application.

Responses	Frequency	Percent
No	39	18.6
Yes	30	14.4
Yes, perhaps. However/ If	19	9.1
Yes, I think (a little/ somewhat), but I am not sure	1	0.5
I do not know	3	1.4
Other	2	1.0
Total	94	45.0

The results show that 39 respondents (18.6%) did not believe that installing an anti-malware application provided enough security, whereas 50 respondents (24%) believed it would provide sufficient security. However, among those who believed in anti-malware security installation, 19 respondents (9.1%) indicated that their agreements were conditional and only 1 respondent believed slightly but was not entirely confident that it would provide adequate protection. On the other hand, 30 respondents (14.4%) were confident that it would be absolutely secure. Additionally, those who did not believe in using a single security protection stated that viruses were updating all the time and that the anti-malware software might not always work. Also, some people believed that these types of software could be used to steal users' information without their knowledge. On the other hand, the respondents who believed conditionally specified that effective security depended on appropriate anti-malware applications being installed to protect against particular malware attacks. Other respondents indicated that an anti-malware application would only work well if it was updated regularly. In summary, most respondents believed they could trust that a single anti-malware application was secure enough to protect them from online banking attacks.

4.6.17 Interview question 17: How do respondents secure themselves against phishing e-mails, phishing web pages and other phishing activities that they could encounter in their daily lives?

91 respondents (43.5%) of the group interviewed, described methods they used to protect themselves from phishing activities.

Table 4.6.17 Interview question 17: How respondents secure themselves from phishing e-mails, phishing web pages and other phishing activities that occur in their daily lives

Responses	Frequency	Percent
What I did/would do was (is)	86	41.1
I don't know	4	1.9
I am not sure	1	.5
Total	91	43.5

86 respondents (41.1%) gave their opinions in answer to this question, whereas 4 respondents (1.9%) did not know about the protection methods, and only 1 respondent was unsure if he or she really knew how to deal with the problems. Further details about respondents' opinions are shown in the table below.

Table 4.6.17 indicates that 64 respondents (57.7%) focused on increasing their own security-awareness while 15 respondents (13.5%) indicated that installing anti-malicious software would be sufficient protection. It can be seen from the table of responses that most participants believed that their improved self-awareness about security was the best countermeasure to guard them against fraudulent activities.

Table 4.6.17.1 Respondents' opinions about countermeasures that could secure them against various kinds of online banking attacks

Responses	Frequency	Percent
Self-awareness in security	64	57.7
Installing anti-malicious software	15	13.5
Other, please specify	13	11.7
Limiting online activities	3	2.7
User education	2	1.8
Increasing/ updating level of online banking security	1	0.9
Security satisfaction	1	0.9
I do not know	10	9.0
No opinion	2	1.8
Total responses	65	100.0

4.6.18 Interview question 18: Current or future situations in online scamming

The following table presents respondents' feedback about current phishing, online banking security, or the future of online banking attacks.

Table 4.6.18 Interview question 18: Comments or additional opinions about the current or future situations of online scamming

Responses	Frequency	Percent
What I did/would do/ suggest was (is)	44	21.1
I don't know	3	1.4
I am not sure at all	1	.5
Total	48	23.0

The table show that 44 respondents (21.1%) provided additional comments which are listed below.

Table 4.6.18.1 Respondent's suggestions in online banking security

Responses	Frequency	Percent
Increasing/ improving level of online banking security	18	8.6
User education	10	4.8
Self-awareness about banking security	6	2.9
Security satisfaction	3	1.4
Refund policy satisfaction	2	1.0
Other, please specify	5	2.4
Total responses	44	21.1
User education	10	4.8

From the table above, it can be seen that 8.6% of the respondents were concerned about increasing and/or improving the levels of online banking security by the banks. 4.8% suggested that educating users was desirable and that the necessary education could be provided by banks. 2.9% believed that users of online banking should become more vigilant and have better awareness of security measures used in online banking. However, only 1.4% was satisfied with current online banking security. Thus it can be concluded that the main improvement that respondents expected from their banks was increased and/or improved online banking security.

4.6.19 Summary of interviewees' experience and knowledge of online banking attacks

Sections 4.6.1-4.6.18 examined interviewees' experiences and knowledge of online banking attacks. Respondents' perceptions of their own knowledge about phishing attacks and various other aspects of online banking security have been analysed. The interviewer posed questions which also focused on experiences of online banking attacks to determine how respondents identified the particular attacks and how the problems were solved. Overall, most respondents had heard about online banking threats from bank announcements and they knew about phishing. However, most of them had only low levels of knowledge about the terminology associated with malicious software. In particular, most were not aware of the differences between spyware, adware, and Trojans. Furthermore, most respondents were more likely to agree that the use of a password combination, in which were included numbers, and upper and lower

case characters, was sufficient to guard them against an online banking attack. They also believed that using personal details, such as date of birth or phone number, as passwords was insecure. Interestingly, a majority of the respondents agreed that changing password every 3-6 months could protect their accounts from phishing attacks. Nevertheless, respondents who believed strongly that it was necessary to change passwords regularly were only slightly more numerous than those who agreed but felt that it was not easy to memorise new passwords all the time.

Interviewees were asked about their ability to determine whether an e-mail was legitimate or not. Most of the respondents believed they knew how to determine whether an e-mail was legitimate by checking the e-mail address of the sender. In addition, many reported that they had been informed by the banks that the banks would never send e-mails asking for personal information. Some had received an e-mail that asked for their confidential information and they immediately deleted because they knew that it was a scam. Most respondents also knew how to distinguish a legitimate bank webpage by checking for the securely locked sign with highlighted colour as well as checking the full URL. However, the number of respondents who knew how to determine if a website was securely locked was much smaller than those who could identify a legitimate e-mail.

Upon investigation, very few respondents had experience of phishing attacks. Among this group, the case was more that their money had been deducted or used for purchasing goods without their knowledge. However, they were unsure if their personal information had been used for the commission of further crimes. Interviewees were also asked about the vulnerabilities which made successful phishing attacks possible. Most answers indicated that user ignorance was a significant factor and that the best ways to protect themselves or solve problems caused by phishing attacks were by installing anti-malware applications and by reporting to the bank immediately.

Additionally, interviewees were asked to provide their opinions about whether installing anti-malware application was enough to secure their computers from being

attacked or not. Most respondents disagreed, because they believed that a new attack was always likely to be one step ahead of existing anti-malware applications and because only a single application would not necessarily be enough to secure their computers.

Finally, the last two questions asked the respondents' opinions about ways to secure themselves against phishing e-mails, phishing web pages, and other phishing activities that they could encounter in their daily life. The answers conveyed their opinions that, if the attack was one in which the user was the weakest point, protection should begin with increased self-awareness about accessing and/or using online banking security, such as being alerted to any new attacks or keeping up-to-date with details of online attacks. They also suggested that banks should have increased or improved online banking security systems, which were more robust and complex in order to secure their customers against being attacked, while ensuring that online banking functions remained easy to use by all levels of users.

4.7 Cross-tabulations results

Cross-tabulations are computed to evaluate the correlations between qualitative and/or quantitative variables. This following section presents data about experiences, levels of knowledge, and opinions of clients about online banking access security, phishing and related online banking threats. Data has been categorised into two major groups of online and non-online banking respondents. Each group has been classified into respondents who have phishing and non-phishing attack experiences. Experiences reported in this survey include phishing e-mails that pretended to be from their bank and asked for personal information, and phishing website which had led the respondents into disclosing personal information or losing money.

The total number of cross-tabulations in each column or row could be different from the total number of a single variable. Respondents were allowed to answer more than one choice in some questions and they could also drop the questions that they

wished not to answer. This investigation only analysed the most significant values that had been supplied by the respondents.

The frequency of respondents in each group reacted upon the respondents' answers and their perceptions in qualitative aspects rather than comparing and contrasting the answers in terms of quantitative attributes. The correlative data contributes more deeply of additional research results to evaluate better understanding of the study and research purposes. The critical points will be used to discuss in the next chapters for appropriate assumptions and recommendations arise from this study. However, when data did not make any values to the questions, an N/A (not applicable) indication will be displayed in the table.

Table 4.7.1 displays the respondents' level of knowledge about phishing and online banking threats through experienced and non-experienced phishing attacks. Non-online banking users were allowed to participate in this activity. Even though they had not experienced online banking attacks, they may have received phishing e-mails pretending to be from their banks and asking for their personal credentials. In addition, knowledge of online banking threats was not only restricted to online banking users. The overall result shows that majority of respondents in all groups had heard about all kinds of online banking threats. These people could explain what they knew or had heard and how the threats could attack online banking users and steal personal information from the Internet. In terms of knowledge, most respondents had more confidence when explaining about a phishing attack. This includes non-online banking respondents. Online banking respondents who had received phishing e-mail had slightly less confidence in identifying what phishing was. On the contrary, those non-phishing attack experiences on the two left columns of Table 4.7.1 were seen to have more confidence in their knowledge of phishing attack when compared within their own groups. In the case of malware knowledge, although a majority of the respondents in all groups could tell what malware was, in fact they had less confidence in explaining what they knew about the threats. Moreover, less people could differentiate between spyware,

adware, and Trojan attacks while most respondents, within their groups, said they did not know or had heard these terms before.

Table 4.7.2 illustrates respondents' knowledge about determining general forms of phishing methods and the vulnerabilities associated with phishing attacks. The questions also covered the ways of mitigating phishing and ways to protect themselves from phishing attacks. Solving the risk was not limited to respondents who had experienced phishing; people who had not been attacked could also answer this question and say what they would do if the incident had happened to them. Most online banking respondents identified phishing e-mails by checking e-mail addresses, checking contact details and contacting their banks. The significant number within the group which had not experienced a phishing attack did not know how to check whether bank e-mails were legitimate. On the other hand, non-online banking respondents chose to contact their banks to confirm e-mail status. Further discussion found that, most respondents who had fallen to phishing decided to delete suspicious e-mails straight away. The groups of non-phishing experienced respondents even they followed similar methods, would go further, call up their bank and report the incident after deleting the e-mail.

In the case of distinguishing phishing bank websites, the number of respondents who did not know how to check legitimate websites was higher than those who did not know how to check e-mails. Those who believed that they knew how to check tended to rely on the name of the URL and the secure web icon which is a padlock located on the address bar. Most respondents who were confident of their knowledge about phishing said that users who neglected to develop their knowledge, or were unaware of the explosion in the numbers of phishing attacks, were the most vulnerable to phishing. Conversely, all groups of respondents still strongly insisted that trusting themselves when dealing with phishing attacks was their first choice before asking for assistance from banks. They felt that being aware of fraudulent e-mail contacts and counterfeit webpages was sufficient to protect themselves. They felt the use of common sense when sharing information was the best practice.

Table 4.7.1 Cross-tabulation of level of knowledge about phishing and online banking threat associations

	Online banking				**Non-online banking**		
	Non-phishing attack experienced		**Phishing attack experienced**		**Phishing attack experienced via e-mail**		**No attack bank experienced**
	phishing e-mail	**phishing online banking account**	**phishing e-mail**	**phishing online banking account**	**Had received phishing e-mail**	**Never received phishing e-mail**	**knowledge of threats**
Online banking threats	Yes (41/60)	Yes (53/72)	Yes (25/27)	Yes (6/7)	Yes (1/1)	Yes (4/5)	Yes (4/5)
Phishing	Yes, strongly (22) Yes, slightly (15)	Yes, strongly (29) Yes, slightly (23)	Yes, slightly (12) Yes, strongly (11)	Yes, strongly (3) Yes, slightly (2)	Yes, strongly (1) Yes, slightly (1)	Yes, slightly (2) Yes, strongly (1)	Yes, slightly (3)
Total	56	71	28	7	2	4	5
Malware knowledge	Yes, slightly (34) Yes, strongly (5)	Yes, slightly (41) Yes, strongly (8)	Yes, slightly (16) Yes, strongly (4)	Yes, slightly (6)	I do not know (1)	Yes, slightly (3)	Yes, slightly (2)
Total	54	67	26	7	1	4	5
Malware: Spyware	Yes (5/22)	Yes (8/28)	Yes (4/13)	Yes (1/3)	Yes (1/1)	Yes (1/1)	I don't know (2/2)
Malware: Adware	Yes (3/19)	Yes (6/25)	Yes (5/13)	Yes (1/3)	Yes (1/1)	Yes (1/1)	I don't know (2/2)
Malware: Trojan	Yes (6/22)	Yes (9/29)	Yes (5/14)	Yes (0/3)	Yes (1/1)	Yes (1/1)	I don't know (2/2)
Personal info can be stolen from the Internet	Yes (40/51)	Yes (46/64)	Yes (16/24)	Yes (5/6)	Yes (1/2)	Yes (3/4)	Yes (4/5)

Table 4.7.2 Cross-tabulation of respondents' perceptions about risk determinations, mitigations, and protections

	Online banking				**Non-online banking**		
	Non-phishing attack experienced		**Phishing attack experienced**		**Phishing attack experienced via e-mail**		**No attack bank experienced**
	phishing e-mail	**phishing online banking account**	**phishing e-mail**	**phishing online banking account**	**Had received phishing e-mail**	**Never received phishing e-mail**	**knowledge of threats**
Determine phishing e-mails	E-mail address (9) I do not know (7) E-mails contents (5) Contact details (5) Contact bank (5)	E-mail address (12) I do not know (7) Contact details (7) Contact bank (7)	E-mail address (3) Contact details (3) Contact bank (3)	E-mails contents (1) Contact bank (1) I do not know (1)	Contact bank (3)	Contact bank (3)	Contact bank (3)
Ways to handles phishing e-mails	Varied solutions (6)*	Just deleted it (11)	Just deleted it (13)	Just deleted it (2)	Varied solutions (4)*	N/A	Varied solutions (3)*
Distinguish legitimate bank websites	URL (19) I do not know (12) Secure web icon (9)	URL (23) I do not know (14) Secure web icon (12)	URL (8) I do not know (6) Secure web icon (3)	URL (1) Bookmark (1) I do not know (1)	Secure web icon (1)	URL (1)	URL (1) Secure web icon (1)
Ways to mitigate or solve the phishing attacked	Self-awareness practice (20) Contact bank (9)	Self-awareness practice (23) Contact bank (9) Installing protection/detection software (8)	Self-awareness practice (8) Contact bank (3)	Self-awareness practice (3) Contact bank (3)	Self-awareness practice (1) Contact bank (1)	N/A	Self-awareness practice (1) Contact bank (1)
Most vulnerable point to phishing attack	User (27)	User (29)	User (9)	User (4)	Password (1)	User (2)	User (2)
Installing a single security protection is sufficient to against phishing attacks	Yes, definitely (22) Yes, if…update/ right software (10) No, definitely (20) No, if…not update/ right software (10)	Yes, definitely (27) Yes, if…update/right software (17) No, definitely (24)	Yes, definitely (6) Yes, if…update/right software (9) No, definitely (11)	No, definitely (4)	No, definitely (1)	No, definitely (3)	No, definitely (4)
Self-protection from phishing activities	Self-awareness (37)	Self-awareness (51) Installing protection/detection software (13)	Self-awareness (22)	Self-awareness (3)	Self-awareness (3)	Self-awareness (2) I do not know (2)	Self-awareness (2) I do not know (2)

However, smaller groups still believed that contacting their bank to solve any phishing incidents was their best solution. The group of online banking users without experience of-phishing focused on the installation of monitoring software to detect unusual activities occurring on their computers. The self-trusting answer was revealed once again by these respondents, that the best way to protect themselves from any unforeseen threats was for them to be observant or self-aware. They believed that there was no way users can be secure from phishing if they did not protect themselves, have the alertness and learn to understand and deal with any suspicious online banking activities themselves.

The respondents were also asked their opinions about installing a single security application to protect themselves against phishing attacks. It can be seen clearly that many respondents believed that installing only an anti-virus or anti-malware software was effective. The number of respondents who disagreed was much smaller than those who agreed. However, some respondents believed that they would be secure on the condition that their software was up-to-date or if they chose the right software to kill viruses or Trojans. The data shows that respondents who had phishing attack experience strongly disagreed about relying on a single security protection. In fact, there is no single security application which has the ability to protect everything and remain effective all the time (GFI Software, n.d.). Multiple appropriate security measures must be put in place to work against phishing effectively.

Table 4.7.3 shows the comparison between those who had experienced a phishing attack and those who had not, categorised by respondents' background. Female respondents who were in the 35-39 age group, who lived in the inner zone and had an average annual income of approximately $50,001-$100,000 were the victims of online banking attacks. These people had at least a bachelor degree and worked as technicians, trade workers or professionals. Moreover, respondents who had received phishing e-mails, in all the groups analysed were most often older females. They lived further out from the city, had considerably higher annual incomes, graduated with at least a bachelor degree and worked as professionals. It can be seen clearly that the younger generation, particularly male students who earned less than $20,000 per annum and perhaps were aiming to complete bachelor degrees, and did not live too far from the city were the group safest from any phishing attack activities.

Table 4.7.4 shows the comparison of the phishing attacks experienced, categorised by previously accessed banks and currently accessed banks. This cross-tabulation presented the list of the banks from which respondents had experience in online banking attack. The above and below rolls were comparing the numbers of respondents who had used online banking service and the current access use by them. Table 4.6.11 shows that 9 respondents had had online phishing through their bank account. However, there are 10 banks were listed by them which could be the case that one respondents had more than one online banking account. Further discussion found that the respondents, who previously had accessed to Bank West, decided not to continue with this bank any longer while other experienced respondents still continued their online service with their previous bank. Other results found that the numbers of current access banks by non-phishing bank attacked customers had been declined in most banks except the National Bank.

Table 4.7.5 illustrates cross-tabulation of respondents who had accessed online banking and their security authentication provided by their banks. The results found that there were few different points found between respondents who had phishing e-mail and phishing bank website experienced and the groups of who had either or both types of attacks. It found that most experienced respondents had been locked out from their banks due to the multiple incorrect password input. These respondents also accessed their bank with ADSL wired broadband connection and used the computer that installed Windows XP operating system. Whilst more non-phishing experienced respondents had never been locked out from their bank. They connected their Internet with wireless connection through the computer that installed Windows Vista operating system.

Table 4.7.3 Comparison of the phishing and non-phishing attack experienced categorised by respondents' background

	Online banking				**Non-online banking**		
	Non-phishing attack experienced		**Phishing attack experienced**		**Phishing attack experienced via e-mail**		**No attack bank experienced**
	phishing e-mail	**phishing online banking account**	**phishing e-mail**	**phishing online banking account**	**Had received phishing e-mail**	**Never received phishing e-mail**	**knowledge of threats**
Gender	Male (36) Female (30)	Male (40) Female (38)	Female (17) Male (13)	Female (5) Male (4)	Female (4) Male (0)	Male (4) Female (1)	Female (4) Male (2)
Age	25-29 (22)	25-29 (25)	Above 50 (10)	35-39 (3)	45-49 (2)	Above 50 (3)	45-49 (2) Above 50 (2)
Annual income	< 20,000 (25)	< 20,000 (26)	50,001-100,000 (10)	50,001-100,000 (3)	30,001-50,000 (1) 50,001-100,000 (1)	50,001-100,000 (2)	30,001-50,000 (1) 50,001-100,000 (1)
Occupation	Student (23) Professionals (15)	Student (25) Professionals (23)	Professionals (11) Student (6)	Technicians and trade workers (3) Professionals (2)	Professionals (1) Home duties (1) Retired (1)	Technicians and trade workers (2) Retired (2)	Retired (2)
Education	Master degree (24) * Bachelor degree (23)	Bachelor degree (31)	Bachelor degree (14)	Bachelor degree (3)	Bachelor (3)	High School (2)	Bachelor degree (3)
Postcode	6061 (5) Zone 2	6027 (5) Zone 3	6051 (4) Zone 1	6000 (1) zone 1 6003 (1) zone 1 6018 (1) zone 1 6103 (1) zone 1 6104 (1) zone 1 6150 (1) zone 2 6065 (1) zone 3 6112 (1) zone 4	6018 (1) zone 2 6025 (1) zone 3 6027 (1) zone 3 6053 (1) outside zone 4	6060 (1) zone 1 6151 (1) zone 1 6018 (1) zone 2 6062 (1) zone 2 6027 (1) zone 3	N/A

Table 4.7.4 Comparison of the phishing attacks experienced, categorised by previously accessed banks and currently access banks

			Lists of the most common online banking previously accessed by respondents									Total
			Commonwealth Bank	Bank West	Westpac	ANZ	National Bank	Citibank	HSBC	I prefer not to answer	Other	
Experience in online banking attack by a phisher?	Yes, I have	Count	2	2	1	4	2	1	0	0	2	10
	No, I have not	Count	31	13	14	31	5	4	5	4	12	76
Total		Count	33	15	15	35	7	5	5	4	14	86

			Lists of the most common online banking for a current accessed by respondents									Total
			Commonwealth Bank	Bank West	Westpac	ANZ	National Bank	Citibank	HSBC	I prefer not to answer	Other	
Experience in online banking attack by a phisher?	Yes, I have	Count	2	1	1	4	2	1	0	0	2	10
	No, I have not	Count	25	8	13	26	5	2	3	6	9	74
Total		Count	27	9	14	30	7	3	3	6	11	84

Table 4.7.5 Cross-tabulation of respondents who had accessed online banking and their security authentication provided

	Online banking			
	Non-phishing attack experienced		**Phishing attack experienced**	
	phishing e-mail	**phishing online banking account**	**phishing e-mail**	**phishing online banking account**
Frequency of online banking access	3-5 times (23)	3-5 times (23) 6-10 times (20) 1-2 times (18)	6-10 times (9) 3-5 times (8)	3-5 times (4)
Type of online banking authentication provided by bank	Login + password (48) Login + password + SMS verification (17)	Login + password (53) Login + password + SMS verification (21)	Login + password (20) Login + password + SMS verification (4)	Login + password (8) Login + password + token device (2)
Length of passwords used when accessed online banking	10 characters (16) 8 characters (13)	8 characters (19) 10 characters (18)	8 characters (10) 10 characters (5)	8 characters (3) 10 characters (3)
Have ever been locked out from back	No (47) Yes (17)	No (50) Yes (25)	Yes (15) No (13)	Yes (3) No (6)
Allowed to re-log in after a while	No (9) Yes (9)	No (13) Yes (12)	No (8) Yes (7)	Yes (1) No (3)
Ways to report login error	Call number provided on 'contact us' page (38) Direct informed by walking to the branch office (23)	Call number provided on 'contact us' page (47) Direct informed by walking to the branch office (24)	Call number provided on 'contact us' page (19) Report via e-mail provided (6)	Call number provided on 'contact us' page (4) Direct informed by walking to the branch office (2)
Usual place where computer were used to access online banking	My house (60)	My house (71)	My house (27)	My house (7)
Type of Internet connection	ADSL wireless broadband (35) ADSL wired broadband (23)	ADSL wireless broadband (36) ADSL wired broadband (30)	ADSL wired broadband (14) ADSL wireless broadband (7)	ADSL wired broadband (4) ADSL wireless broadband (2)
Type of operating system	Windows Vista (27) Windows XP (24) Windows 7 (16)	Windows Vista (34) Windows XP (28) Windows 7 (17)	Windows XP (13) Windows Vista (11) Windows 7 (7)	Windows XP (4) Windows Vista (2) Windows 7 (2)
Type of security protection/detection / monitoring	Anti-virus (50) Firewall (24) Pop-up blocking (16) Anti-malware (13)	Anti-virus (60) Firewall (33) Pop-up blocking (21) Anti-malware (20)	Anti-virus (21) Firewall (16) Anti-malware (11) Pop-up blocking (10)	Anti-virus (5) Firewall (4) Pop-up blocking (3) Anti-malware (2)
Frequency of security update	Auto-update (21) Once a day (9) Once a week (7)	Auto-update (31) Once a day (8) Once a week (8)	Auto-update (15) Once a day (4) Once a week (2)	Auto-update (2) Once a day (2) Once a month (2)

Table 4.7.6 Cross-tabulation of phishing e-mail experienced and phishing bank website experience

Have you ever used online banking			Experience in online banking attack by a phisher?			Total
			Yes, I have	No, I have not	I am not sure if I have or I have not	
Yes	Have ever received e-mail from bank that asked for confidential information?	Yes, I have	4	23	1	28
		No, I have not	4	55	3	62
		Other, please specify	0	0	1	1
	Total		8	78	5	91
No	Have ever received e-mail from bank that asked for confidential information?	Yes, I have	N/A	2	N/A	2
		No, I have not	N/A	3	N/A	3
		I am not sure if I have or I have not	N/A	1	N/A	1
	Total			6		6

Table 4.7.6 illustrates cross-tabulation of respondents who fell in phishing bank website and their experience in receiving any phishing e-mails that pretended to send from their banks and asked for personal identity. The data shows that four respondents who had online banking attack experience had received phishing e-mail that came from their bank and asked for their confidential information. On the other hand, four respondents had never received any phishing e-mail from their bank that asked them to provide personal information. However, two non-online banking users claimed that even though they did not have online banking service but they had received e-mail from their bank and asked for their personal information.

4.7.7 Summary of interviewees' experience and knowledge of online banking attacks

Sections 4.7 examined cross-tabulations of the interviewees' experiences of online banking services and their knowledge of phishing. The results covered respondents' preferences for secure passwords, based on their knowledge and their preferred solutions when they were confronted with unwanted risks, together with ways to protect themselves from attacks. Most respondents knew what phishing and online banking threats were and how the threats were carried out. They believed that the users form the weakest point in a phishing attack because they may be ignorant of bank warning information or lack alertness when they encounter suspicious activities towards

their computers, e-mails, webpages, or bank accounts. These possible victims were sometimes in danger of social engineering attacks in which their information may be disclosed unintentionally when their security protection is weak. Nevertheless, trusting themselves to have a thorough awareness of how to deal with online and offline personal information sharing or money transfers was the best self-practiced. Neither did they acknowledge that they would be at risk if they relied on a single security tool to defend themselves against phishing.

4.8 Summary

This chapter has analysed and discussed respondents' answers to questionnaire and interview questions. Relationships between variables have been cross-tabulated and results of those analyses presented. An in-depth analysis of the risks faced by respondents' and their vulnerabilities, identified from this survey, will be discussed in the next chapter.

CHAPTER 5 DISCUSSION AND IMPLICATIONS

5.1 Introduction

As previously stated in chapter 1, the primary objective of the study was to identify how online banking users perceived threats, such as phishing and malware, via online banking channels. This objective also covered the experience in any circumstances of online banking attacks and how they dealt with the problems. Another aspect of this objective was to identify users' knowledge of online banking security. Clearly, this objective has been achieved, as reflected by the findings revealed in chapter 4. The respondents' understanding of phishing and online threats were elicited. To answer the research questions in chapter 1, the following are the research questions:

5.2 What are the factors which lead people to use online banking?

Technology of online banking services benefit bank customers to take controls of their own accounts more flexibly. This survey found that convenience was a main reason that led most respondents decided to use online banking. Many studies identified convenience as the most important factor in the use of online banking services (Lichtenstein & Williamson, 2006 citing from ACNielsen, 2005; Pew, 2003; Ramsay and Smith, 1999; Thornton and White, 2001; Social Research Centre, 2008). Previous studies mentioned that respondents' behaviours in the adoption of online banking services depended on the elements of experience, utility and time saving (Lichtenstein & Williamson, 2006). In fact, choices that the respondents chose in this research: fast service computer operation, reduction of the time spent waiting in queue or commuting to bank may be seen as parts of the convenience. In details, the investigator discovered that the convenience of having fast service computer operation was the key. When computer technology becomes more accessible to people, the chance of having other facilities will then be more easily established. ACNielsen survey (2007) explored that bank loyalty in Australia was risen up to 44% or close to half of the respondents who were 'very loyal' to their bank. The ACNielsen survey supported finding in this study that most respondents were satisfied enough to continue their online banking services with the banks which had offered them traditional services. In particular, the ANZ Bank

and the Commonwealth Bank, because of the levels of trust engendered by their traditional services, became the first and second most popular banks with which most respondents had chosen to sign up for online services. This may have been influenced the respondents to continue their existing bank rather than seeking for the best online banking security or an excellent service reputation of the bank to start using a different banking service.

The convenience had brought the respondents accessed more frequent to online banking in approximately of once a week. Recent statistics found slightly different that the Australians engaged in online banking and finance more frequently than once a day and following with accessing just once a day in December 2010 (Commonwealth of Australia, 2011a). However, this data represented the country rather than a single state region. Besides, services such as BPAY, money transfer, home loans application, and credit redemption are some of the common online services that many banks offer to their customers. This research found that money transfers, balance summary viewing, and bill payments were the most common activities that the respondents chose to perform when they accessed their online banking services accordingly. The result was similar to a report of the Australian Government, Department of Broadband, Communications and the Digital Economy (2008), which included the top ten online activities by Internet users in June 2006. 60% of the home broadband Internet users aged 14 and over performed account balance checking, 54% accessed their online account to transfer funds, and 25% paid bills. Similarly, Nielson's survey (2006) also revealed the most common online transactions activities which included viewing account balances, viewing recent transactions, and paying bills. In addition, the same activities were also presented in the list of top online activities for home dial-up Internet users (Australia. Dept of Broadband, Communications and the Digital Economy, 2008).

On the other side, several respondents discontinued their previous banks. Few respondents had changed banks because they did not feel entirely secure with their previous banks, while another respondent's account had been attacked. Thus it could be proposed that, in the online banking industries, users continued with a system primarily

because their satisfaction had caused them to believe that the banks were trustworthy. In addition to the results found in this study some respondents did not want to join online banking because they concerned about security of the bank. The high percentage of the concern about online security among non-users may confirm the findings of Yeow, Yuen, and Tong (2008 quoted from Sathye, 1999), who stated that customers were generally more concerned with the security of online banking services compared with traditional banking services. While the use of online banking has increased, the proportion of internet users aware of online banking risks associated has remained unchanged since 2005 (at 22%) although there was new awareness of the threat posed by identity theft (Social Research Centre, 2008, p. 6). Lichtenstein and Williamson (2006); however, implied that a lack of prior experience using the Internet may have inhibited their respondents from utilising online banking services. The study could be indicated that customers lacked awareness of the security of the online banking services. They needed to be educated to ensure that they recognised that fundamental security, such as information privacy, or authentication authority, was in place and be concerned in choices of online banking factor. Banks should also establish a non-online banking customer-centric infrastructure and encourage them using innovative technology (Voutsas & Heinrich, 2011). It is important to show the key benefit of online banking and demonstrate bank's security infrastructure to enhance customers' trust. They needed to base their choice of an online banking system on more specific information than purely a sense of trust.

5.3 What are users' opinions of online banking systems?

According to this study, respondents knew the fundamentals of how online banking systems operated and believed that banks were the firms that they could trust more strongly than other types of financial institutions that were available on the Internet. Respondents stated that they had trusted the banks' reputation as well as the security protection. Their reasons for trusting their banks were because of high standards of security and banks' images and reputations. Further, good relationships between the banking firms and the customers were reflected in loyalty and prolonged commitment to bank products and had influenced them to continue using services such as Internet

banking. A similar study also found that increased customer loyalty was reflected to the positive long-term financial performance (Alrubaiee & Al-Nazer, 2010).

Supportively, most respondents positively believed and satisfied with their online banking services regarding the safety of financial status, trust in data protection, and confidence in security measures against cyber-attacks. However, one lowest level of their confidence was that many respondents had difficulty in distinguish a bank secure website. Therefore, they strongly agreed if their bank would offer security metrics measuring how secure their online banking was while they were accessing their banks. According to a summary of security checklist presented by Subsorn & Limwiriyakul (2011) there was no bank that provided an interactive 'direct' security metrics measuring system. In fact, most banks that available in Australian had not provided live check anti-virus protection, intrusion detection system and no information about them. The only security protection that most banks (except Westpac, Adelaide, Macquarie, and Members Equity banks) have had in place was firewall protection. In addition, respondents' opinions about countermeasures and suggestions pointed to increasing or improving level of online banking security and providing user education. They believed that caution and knowledge about security protection and threats were important; nonetheless, the respondents still required their banks to ensure their safety.

The security measures statements were provided to the respondents and asked them to deliver their security preferences of level of agreement. It found that major respondents agreed strongly about establishing or improving their online security system by their banks. The security they strongly preferred consisted of:

(i) Multi security protection, such as login and password and SMS mobile verification code and digital signature.

(ii) My bank should offer a tracking facility showing all transactions and detail about when I have logged in and out.

(iii) My bank should never allow more than one computer access to the same online banking account at the same time.

(iv) My bank should detect, deny and stop all online banking activities if there is more than one computer accessing the same online banking account at the same time.
(v) My bank should log off my account automatically when I close the window.
(vi) My bank should log off my account automatically after I have been logged on for 45 minutes.
(vii) My bank should log off my account automatically if my bank webpage is not active for 15 minutes.

According to the summary of the proposed Internet banking security checklist wrote by Subsorn & Limwiriyakul (2011), many banks available in Australia have complied with the session validation and tracking facility systems. However, additional research found that none of the bank provided clear information according to the above seven statements. It could be assumed that banks may not see these security measures important or much sufficient. Unless, banks posted unclear of exiting security used which may have misled bank customers into perceiving that their banks did not have such security measures when they actually had implemented. Alternatively, banks had employed encryption and digital certificate technologies to enhance level of security mechanism with additional of 24/7 bank enquiries services. One important criterion about online banking system is an authentication system. Below section is respondents' opinion about their online banking authentication preferences.

5.3.1 What are users' opinions about the available online banking authentication systems?

All data indicated that the respondents had believed the stronger and the more complex the authentication was; the more they felt their banks were secure against phishing. They had prioritised biometric protection as the strongest protection and the normal login with username and password as the weakest one. These research findings were supportive with the KeCrypt (2010), a biometrics security company, that 50% of those surveyed preferred biometric security to any other methods, such as smart cards plus passwords or PINs (20%), and multiple passwords or PINs (30%). In addition, of

those preferring biometric authentication, 63% saw it as being more secure and 27% found it more convenient than having to remember passwords and PINs (KeCrypt Systems Ltd, 2010).

Interestingly, most respondents were willing to pay mandatory fees, if banks asked for it for more robust security for their online banking, such as the implementation of biometric authentication methods. Therefore, most respondents believed that as long as any system could protect them from being attacked, fees between $2 and $5 would be acceptable. In fact, most of the banks did not imposed any additional fees or charges relating to security measures and authentication mechanisms and in many cases there was a reduction of general fees and charges (Australia. Department of Communications, Information Technology and the Arts, 2008). The main reasons for the enhanced level of trust from the respondents were the robust security protection offered by the banks, along with the provision that customers could create or were provided long and strong passwords.

Furthermore, much of the work on security focuses on creating strong passwords such as mixtures of uppercase and lowercase letters, numbers and special characters. Such combinations were preferred by most respondents. In addition, some respondents believed that maintaining such complex passwords was their solution in protecting them in phishing attacks, but some argued that if a phisher knew how to retrieve passwords from victims, any type of password would still be vulnerable and easy to obtain. That is, some users mentioned that if a phisher can steal their password, it really does not matter how long or complex they make the password. This could also reflect to respondents' preferences about the knowledge-based authentication clearly when many respondents neither agreed nor disagreed about bank should employ security question and password authentication every time when they accessed to their online banking. Rabkin (2008) assisted that "… the user is assumed to be unable to remember arbitrary strings — otherwise they would have been able to remember their password". In addition to this respondents' agreement, if the result was satisfied and had been employed by bank, the customers would have failed into spear-phishing attack. It could bypass most knowledge

based authentication systems and processes based on external data from public data aggregators and the credit bureaus (Litan, 2010). Cormac Herley, a principal researcher at Microsoft Research said that "keeping a keylogger off your machine is about a trillion times more important than the strength of any one of your passwords," (Stross, 2010). He also claimed that antivirus software could detect and block many kinds of keyloggers, but there is no guarantee that it gets everything (Stross, 2010).

Many respondents demonstrated self-efficacy (Milne, Labrecque, & Cromer, 2009) and preferred to take steps to secure their bank account. They used strong passwords and agreed with avoiding creating passwords containing date of birth, phone numbers, and residential and work addresses. They believed that such poor passwords may have consequent their online banking accounts more vulnerable. They agreed that it was necessary to change their passwords periodically, every three months if suggested by the banks, as they had believed that their security would have been improved. Nonetheless, some protested that it was difficult to keep changing passwords regularly as they were hard to remember and would not prevent them from being attacked. Some respondents said that they had to write down their passwords on a paper to remind themselves. This annoying password reminding could result in people creating guessable passwords which could open themselves up to hacking or facing a password paradox attack (Greenfield, 2011; Sines, 2011). The average person is limited to such a maximum complexity of the passwords they are willing to memorise (Schneier, 2006) and they tend to use their passwords in the same pattern. This belief has been supported by Hunt (2011) in human password generating that "password are inspired by words of personal significance or other memorable patterns." It could be assumed that the passwords which have been created from numbers, symbols, (reverse) phrases, or selected from a dictionary are possible to relate to the person's background such as name or place. Even though the phisher may take longer to crack the complicated password, they eventually will obtain it (Ingmar, 2011; Naughton, 2011).

What respondents believed and had opinions about may not be told in what they really performed into securing their online transaction. Below paragraphs illustrate the actions of the respondents when they accessed their online account.

5.4 Are users of online banking taking adequate steps to secure their online transactions?

Respondents' behaviours and their activities regarding online banking were evaluated to examine respondents' knowledge about their computers, peripheral devices, and the security applications that had been installed. Because of the high responses indicated about home internet access, most respondents had knowledge about the operating systems, types of Internet connection, and security applications used in their usual device that was used to access their online banking service. In particular to the security installation, approximately one out of every three respondents knew what type of security had been installed on their computers. Most of them acknowledged that the computer would not have been secured at all if only a single anti-malware application had been installed. They understood that one anti-malware application may only be effective against a particular threat. In addition, they believed that their computers and personal information would not be secure against attack if adequate anti-malware was not installed along with proper and regular security upgrading. Practically, however, only anti-virus software had been installed in most respondents' computers. Extra security applications, apart from the auto-update option, were lacking. Even though they acknowledged their devices and the limitation of an anti-malware protection that had been used to access their banks, they failed to employ multiple protection to secure their information privacy and computer assets.

In addition to the phishing website attack, the results revealed that the nine respondents, who had been attacked, had installed only a single anti-malware protection. Four people had installed only a firewall application, three people had installed anti-virus software, while one was unsure which security application had been installed, and another one did not use any security protection. All respondents' online banking authentication systems involved the simple username and password login method. Four

had believed that this type of security method was the strongest way to protect themselves from phishing, whereas the other five highlighted more complex types of authentications such as biometrics, token devices, and mobile verification methods. They acknowledged that there were risks in relying on a single anti-malware application. Many respondents may try to avoid risks, but their behaviours in relying on a single anti-virus application and auto-updating options are in themselves a danger. It can be seen that the majority of users installed an anti-virus application to safeguard themselves against unpredicted threats; meanwhile, new threats to respondents' privacy and online banking systems are on the rise and may not be apparent until it's too late.

Further, customers, particularly, who believed that they had less knowledge of the Internet, computers or security may have felt it is too challenging to keeping their machines updated with new patches or firmware updates which are released constantly. This belief could result in becoming a victim of phishing attacks (Milne, et al., 2009).

People will avoid an action if they do not believe they have the ability to complete the action and achieve their desired result. Self-efficacy is an import factor in determining a person's use of information security tools (Cox, 2012). According to AusCert (2008, p. 3) mentioned about the confidence of users in taking their own self-efficacy in security practice that 68% were 'confident' or 'very confident' in managing their own computer's security. This self-confidence was also found throughout this survey when asking respondents about ways or how to secure themselves from any cyber-attacks. They believed that if users were cautious, and alerted to any suspicious activities and trusted their security common sense. This was the first security line defense that could be used to mitigate phishing attack and also protect themselves from any phishing activities in the future. Therefore, it is essential for the banks to train or educate their customers about the potential risks from phishing by keeping the users' computer updated with multi security protections regularly. Perhaps banks may safeguard their customers through effective marketing communication so that banks could propose phishing awareness and anti-phishing education to enhance consumer

response efficacy and self-efficacy in coping and responding on threat reducing or removing (Cox, 2012).

5.5 What levels of knowledge do users of online banking have about phishing?

More than half of the interviewed respondents knew of or had heard about online banking attacks and other related threats from their banks. They said they had received warning messages from their banks while other channels of communication were less often recognised. Only one person had heard warnings from the television and two people mentioned hearing warning information on the radio. However, the results revealed that the more sophisticated were the types of attacks the less knowledge of them the respondents had. Most interviewed respondents knew of, or had heard about, online banking threats and how personal information could be stolen from the Internet. Nonetheless, their confidence was much less when they were asked about particular terms of bank threats, such as phishing, Trojans, adware, and spyware.

To begin with level of phishing knowledge, half of the respondents, who knew or had heard about phishing, had a stronger level of confidence about their knowledge of phishing. Their answers had been focused on the three main phishing activities: scammed email pretending to be from banks, money transfer scams and counterfeited bank websites. The results reveal that the respondents' knowledge of phishing was sufficient and was comparable to the government's statements. More in depth of the findings found that many of the online banking respondents who never experienced any types of phishing attacks had stronger confidential into believing that they knew what phishing was and how it performed. The gaps between who strongly had confidence and slightly had confidence were not too high. The critical points found in the groups of phishing attack experienced respondents. The level of confidence in phishing knowledge for respondents who received phishing e-mail and who had online banking attack experience were not different between who strongly believed and slightly believed. In fact, they should all have had strongly knowledge of phishing attack since they were the victims of the attack. Similar results were found in malware knowledge. The level of confidence in malware knowledge was quite low even though they all faced phishing

attack. Especially, respondents who had received phishing e-mail, had knowledge in specific terms of spyware, adware, and Trojan less than half of the total number in each group. Likewise, online banking respondents who never had any experience in phishing attacks also had low level of strongly knowledge in malicious attacks. Particularly, only a few respondents could differentiate between the three characterisations of Trojans, spyware, and adware. The majority of the respondents could only classify between one and two of those terms. Respondents were likely to be more familiar with the Trojan horse definition than that for spyware or adware.

The results of this study indicate that the general controllability perception of online banking threats is positively associated with their self-efficacy in earlier discussion. However, most respondents still lacked 'sufficient' knowledge and did not receive enough information regarding phishing and threats publicly. Therefore, user awareness and education/training are critical in maintaining current knowledge of the latest cybercrime activities and the best cybercrime prevention measures (Choo, 2011). Current security awareness training should emphasise the vulnerabilities related to the various information security threats and what should be performed or not be done in order to reduce such vulnerabilities. Given the influence of general perception to respondents' self-awareness or self-efficacy, awareness training should also interconnect the existence of bank's security counteracts and procedures to control online banking threats (Rhee, Kim, & Ryu, 2009).

5.5.1 Do bank customers believe that banks are taking adequate steps to prevent phishing attacks?

To begin with the authentication systems provided, it can be seen that methods can be categorised into two main groups of a single authentication system and a two-factor authentication system. Most respondents had been provided with a single authentication system which comprised a username (login) and password. This authentication method was offered by banks more than two-factor authentication methods, such as login with password and SMS mobile verification, which was higher than the token devices, biometric authentication systems, grid card, or login and

password with a secret question. These two-factor authentication were basically an optional that banks had offered to their customers and not many bank employed them (Subsorn & Limwiriyakul, 2011). The multiple modes in the more sophisticated devices added layers of complexity for customers; nevertheless, there was no indication that they had any knowledge about their potential use because they had seen little need for complex devices. Interestingly, the statistical results reflected that proved authentication security by banks to their customers was parallel to what customers preferred as mentioned in 5.4. That means the customers believed that their banks were taking adequate steps to prevent phishing attack even though another side believed that using a single mechanism was not secure enough to protect their bank account.

The contradict between security concern and actual behaviour found by Weir et al. (2009) about user perceptions of security, convenience and usability for e-banking authentication tokens that "customers see security as largely a concern of the Bank. Their preferences for authentication methods entirely followed usability and convenience concerns (p. 60)." That means the concerns for security in online banking did not override their desires for convenience and usability (Weir, et al., 2009). Respondents tended to choose something that was easy and less complexion to perform which would create a chance to get attacked by Trojans in recording data input when accessed to the bank. In regarding to this, many banks required customers to create strong and long passwords to enhance security. Banks encourage their customers to create strong and long passwords which many respondents had eight password lengths. This study shows that many respondents perceived that having only a login and password as security was ineffective. However, there were a number of people who did not realise the danger of having shorter passwords. Therefore, in addition to employing robust security and providing an education for customers about their safety, the use of mandatory policies about strong and complex passwords was essential. One technique that banks could do is to setting up an automatic strong password reset. The system may mandatory require customers to change their password every certain period of 3-6 months. The system should detect if the customer are successfully created their own password combined with lower, upper, and special characters with numeric to a

minimum of 8 password lengths. If respondents fail in either bank's policy, they could eventually be restricted their access to the online account and are required to re-activate their account in person.

In terms of log on validation failure due to a number of inadequate password input, approximately half of the respondents had experienced being unable to access their own account; with half of those being allowed to re-access their online banking account. The majority of the respondents had solved the problem by calling the bank on number provided on the 'contact us' web page rather than walking in or sending an e-mail. This method can help the respondent identify the problem immediately as soon as they had found out that their bank service had any problems. In contrast, the respondents would have failed into man-in-middle attack if the website had imitated by the phisher. It is a suggestion that banks should have a call back policy to contact their customers immediately over the phone. Alternatively, bank could send the contact number and asked them to contact to their bank immediately after three times failing of inacceptable password. Banks could further ask customers to come to the nearest branch and reset their password on the web to ensure that their account was control securely and setting up properly and authentically.

5.5.2 What could be the vulnerable point that leads online banking users into phishing attacks?

According to 4.7.2, most respondents believed that user was the vulnerable point to phishing attack. They claimed that users who had less education in security, unawareness or ignorant in any unusual of internet and computer activities could fail to the cyber-attacks. Particularly, the nine respondents who had experienced an online banking attack, only some had realised themselves that something was wrong with their accounts, while the others had been informed of the attack by their banks. Furthermore, apart from asking their banks to mitigate the risks, they remained unsure whether their information was protected and had not been used for any further criminal activities. This example could reflect to the view that if respondents were lack of regular security check and being careless on their transaction, they could fail into successful phishing attacks.

Other vulnerable points to phishing may include type of operating system, type of internet connection, authentication security method, password type and length, and type of security protection.

Florian's blog (2012) shares information from the National Vulnerability Database (NVD) of the most targeted operating system in 2011 that Microsoft operating systems were the most targeted. The targeted Microsoft versions include Microsoft Windows Server 2003, Microsoft XP, Microsoft Windows Server 2008, Microsoft Windows 7 and Microsoft Windows Vista. The followed targets were Cisco IOS, Apple Mac OS X, Google Chrome OS, and Apple Mac OS X server. Interestingly, Apple iOS and Google Android made the entry in the top 15 most vulnerable operating systems in 2011. Smart phones and tablets therefore also face strong risk of phishing attack as it was discussed on chapter 2. As the results of this survey, many respondents who used Windows platforms Windows XP, Windows Vista, and Windows7 may have faced significant risks of man-in-the-middle exposure. The attacker may use unauthorised certificate issued by Microsoft spoof content, perform phishing or man-in-the-middle attacks (Microsoft, 2012). The explosion found in the groups of respondents who had received phishing e-mail, experienced in phishing bank website, and who had not experience in any kind of attacks. In terms of internet connection, the research found that most phishing and non-phishing experienced used wired Internet connection to access their online banking accounts. Wired Internet connection could be vulnerable to denial-of-service (DOS) attack because users often turned on their machine and connect to the Internet for days (Kohli, 2008) which could render the device vulnerable to the attack. Attacker can take a chance to scan the network for available computer if any are connecting to the Internet. The attacker may attempt to deny respondents from accessing e-mail, websites, or online accounts (Thorat, Nayak, & Bokhare, 2010). Unfortunately, the question was not prepare to ask the respondents if those who used wired Internet connection disconnected or turned off their modem or disconnecting cables when they did not use the Internet. Therefore, the assumption to this possibility based from finding may indicate that the respondents who used DSL Internet connection may have been in risk of DOS attack. In fact, wireless internet connection is more vulnerable than wired

connection. The signals of most wireless networks extend beyond the walls of users' house and eventually allows anyone can make a connection to the Internet through the wireless connection (Evans, Poatsy, & Martin, 2009). Failing of adequate wireless configuration may be interfered by passive attack (attacker interpret data gathered through snooping) and active attack (attacker modify data stream or creation of false stream) (Goyal, Batra, & Singh, 2010). However, one way to identify if these respondents were possibly safe from DOS attack is investigating type of security protection. For example, if they were suspecting to be in risk of DOS attack, one possible solution to secure their computer and data is installing a firewall application because it can keeps everything out except identified traffic (DeepSearcher Inc., 2012; Thorat, et al., 2010). As type of security protection was already discussed in 5.4, the numbers of respondents who installed firewall protection was lesser than anti-virus protection. Therefore, the protection that banks could educate customers about the types of connection should include a guidance of how to be safe from attacks with different types of Internet connection. For instance, Internet cable should be pulled off when computer is shut down. Router should be turned off if it is not in used. In addition to a secure wireless connection, a wireless router should be configured to difficult-to guess a SSID (network name), turn off the SSID broadcasting to make it harder for outsider to detect your network and enable security protocols such as WPA or WEP security (Evans, et al., 2009). Importantly, multiple software protection should be installed to monitor all incoming and outgoing traffic and detect any suspicious activities in the computer.

The use of the Internet has become more important for transactions and in conjunction with the increase of privacy concerns. Users had decided to access their bank with longer password characters. As discussed partly in the previous research questions, this survey research found that many respondents had an average of eight passwords to manage; some had ten or more. Moreover, two character passwords were being used by some respondents, but even fewer respondents used as less as four characters. Further research found that the three respondents who had experienced phishing attacks were unlikely to change their passwords even if their banks had a

mandatory policy to do so, whereas others preferred to change every month (1 person), every 3 months (2 people), and every 6 months (2 people). Many respondents agreed it was necessary to change their passwords periodically, every three months if suggested by the banks. Even though the respondents had long password characters, and believed that using combinations of password characters was the strongest choice, they were still at risk of phishing attacks. Some protested that it was difficult to keep changing passwords regularly as they were hard to remember and would not prevent people from being attacked. Dale's research (2007) found that people had problem with remembering and/or forgetting their passwords which resulted in written down the passwords in a paper. Consequently, not only the respondents knew about their password, but the surrounded people would know how to access their online accounts.

A part from password protection, there is no single security application which has the ability to protect everything and remain secure all the time (GFI Software, n.d.). Many respondents may try to avoid risks, and relying on an auto-updating software protection. However, some people may find auto-updating option may be seen as a nuisance and they may turn it off without realising the high potential for harm (Milne, et al., 2009). Some big banks in Australia have increased the level of online banking security by establishing two-factor authentication for online accounts ("Banks increase security measures," 2010; Kavanagh, 2007) as well as focused on the consumer education and awareness which is one of the first line of defence to against online crime ("Banks increase security measures," 2010). The respondents who had been attacked by the phisher were at risk because they lacked concrete knowledge of how to protect their computer from external threats. Their banks may succeed to provide strong security protection but fail in approaching customers to beware of the threats. Other possible reasons that users may engage in risk by their unintentional behaviour they may be convince by phishing e-mail and in ability to identify phishing bank websites. Social engineering may adept at appealing to the user's emotions to fraudulently obtain sensitive and private information (Cox, 2012) via e-mail or pop-up windows message which will be discussed below.

5.5.3 Do users have enough knowledge to be able to distinguish a legitimate bank's e-mail and website from a fraudulent one?

Overall, the results showed that self-awareness plays an important and direct role in online protection behaviours against phishing attacks. As respondents relied on their response efficacy in self-perceived abilities of coping and desiring to handle any security issues (Cox, 2012). When the respondents felt that they were facing dangers, they believed that they had confidence, knowledge and skills in avoiding or dealing with the problems. As the results show in sections 4.6.8 to 4.6.10, most respondents were confident that they could identify legitimate e-mails that came from their banks. Similar confidence was reported in dealing with phishing websites; many respondents believed that they had the ability to distinguish legitimate bank websites. Their knowledge and confidence in coping with threats were leading them to believe that they knew how to protect themselves from any suspicious online threat.

In addition, 84% of the respondents who were interviewed in this question answered confidently about their ability in distinguishing legitimate e-mail from scam e-mail which initially seemed to be from banks. Even though many respondents indicated that checking e-mail addresses was the method they believed that they would use; nevertheless, many respondents indicated that they felt they would still need assistance by contacting their bank to verify the incoming e-mail. It was apparent that most respondents did not have sufficient information regarding bank policies about phishing e-mail informing or receiving bank information via e-mail.

In fact, no matter how caution the respondents were, if they still relied on the URL address, and e-mail content, or provided contact details, they could get trapped by the phisher. As demonstrated in chapter 2 that people can be attacked without clicking or providing anything in the e-mail as long as they just open it to read. One of the simplest ways that could avoid the respondents failing in phishing e-mails is to check full e-mail header. E-mail header allows the recipients to see where the message really originated from. This research discovered that none of the respondents mentioned about full e-mail header check. Further investigation found that no banks in available in

Australia warn or educate their customers about the benefit of full e-mail header verification. Many banks had warned their customers about bank e-mail sending policy or how to check phishing e-mail fundamentally such as e-mail content, e-mail addresses, using filter e-mail content and address. Therefore, this is another important step for all banks to insert an extra caution to educate their customers I self-verified of phishing e-mails.

On the other hand, respondents apparently knew less about verifying legitimate bank websites compared to verifying e-mails. Nevertheless, most respondents chose to check the URL to distinguish legitimate web pages, followed by checking whether the secured webpage icon was present. Distinguishing between e-mails seemed to be easier than determining whether websites were legitimate. However, there were many respondents who did not how to check e-mails and websites and a number who seemed to know how to do so, but could not explain or discuss it clearly. The number of respondents who somehow believed that they knew how to verify a website but could not explain clearly (21 people) was nearly equal to the number of respondents who were certain that they knew how to check the website by looking at the URL (28 people).

Generally, respondents understood about web legitimate check. Their knowledge was also supported by the Australian Department of Broadband, Communication and the Digital Economy (n.d.) and US-CERT, wrote by McDowell & Lytle (2010) in regarding checking the digital certificate, https:// and padlock sign was appropriate to perform. The researcher found that people who judge by checking for the URL of the legitimate website may still fall victim to the URL obfuscation if they believed that the correct domain name is the legitimate bank website they visited. As mentioned by Johnson (2008) the act of DNS cache poisoning may be done by changing or adding a rogue IP address of the bank's website by the attacker so that the user will be redirected to a wrong website instead of the original IP address. In addition, trusting in certificate depends on the level of the certificate authority that banks have been used to validate all of the information in the requests and ensure the data is secure (McDowell & Lytle, 2010).

One possible solution to protect respondents and educate them at the same time is to integrating software and interfaces that prevent users from falling for attacks while performing their online transactions or checking their e-mails. Employing blacklists and whitelists website classification is another technique to determine whether the current visiting URL is on either black or white lists. The list of prohibited website will be stored on either clients or hosted at a central server which will be blocked if the respondents fall into it (Alkhozae & Batarfi, 2011). Many commercial toolbars or web browsers have this kind of detection such as Internet Explorer 7, Nestcape Browser 8.1, and Cloudmark AntiFraud Toolbar (Afroz & Greenstadt, 2011). However, the traditional blacklisting solution may not work effectively to a zero-day attack, if the malicious tool is newer and may bypass the detecting system (Parmar, 2012). Contrary, a global white-list approach is likewise hardly possible for to cover all legitimate web sites in the entire cyber world (Cao, Han, & Le, 2008). Nevertheless, whitelist solution may be practical in building a list of trusted bank websites that users access on a regular basis (Alkhozae & Batarfi, 2011). Characteristics of a website will be scan to detect phishing rather than filtering a list. These characteristics can be the URL address, HTML source code, page feature such as the page content (Alkhozae & Batarfi, 2011), or DNS-IP mapping (Cao, et al., 2008).

To summarise the respondents' knowledge in phishing verification, they all had standard concepts of ways to verify the legitimate and counterfeit e-mails and websites. Conversely, their knowledge was lacked of latest security attack information to guide them that more complex of phishing attack has developed beyond their exiting knowledge. Non-of the bank's website provided any information that could educate their customers to be updated about latest phishing technique or demonstrate a more advance security self-practice to identify sophisticated threats. In fact, it is a customer responsibility to keep updating themselves about the new types of threats and follow news or media in association to their bank risk and safety. Bank still can educate their customers and provide more information and ensure that the self-protection guideline is up to date and remind the customers that they cannot rely on bank to be in charge 100% without customers' self-awareness.

5.6 Limitations of the study

There were some limitations with respect to the analysis and data that may have affected the results and discussion evaluation parts.

First of all, this study was limited to the investigation of the use of online banking in Western Australia. The result might not be the same if a study of a similar topic were undertaken in other regions in Australia or in other countries where the use of online banking is also accessible and practical.

Second of all, this is a pioneer study that concerns WA bank users whereas similar previous studies that were found in Australia did not focus on the knowledge and experience of phishing attacks that were discovered from the online banking respondents. Even though similar topics have been investigated in other countries, different experiences in the use of online banking and the knowledge about phishing are likely to have been reported, due to the differences of geographic, economic and cultural demands on online banking services.

Thirdly, the results of this study reveal interesting and useful information regarding the use of online banking by the WA population. Hopefully, this might be the starting point for further researchers, security developers and bank technicians to use in designing more secure online banking authentication security for the bank customers later on while ensuring that their customers are safe from using any additional devices.

Fourthly, there were some missing values in the data which were excluded from the analysis and this made the sample size for some of the time periods smaller than others. Therefore, it is possible that some values were shown to be significant in sometime periods but not in others due to the sample size (Dobbs & Maxwell, 2002).

Fifthly, phishing techniques have rapidly developed in the cyber world. This results in a number of various types of phishing techniques that are used to attack banks'

customers. This research did not cover all aspects of all phishing methods and did not include any discussion of still-developing techniques. This study; therefore, focused only on the experiences and the information provided by the respondents.

Finally, it could be difficult for respondents to "…recall information or to provide the truth about a controversial question" (Barribeau et al., n.d.). This would result in the information given to be analysed in this research not being the same if repeated with different groups.

5.7 Discussion summary

This study has attempted to understand the factors influencing respondents' in adapting to online banking and their knowledge and behaviour in the use of online service. Security concepts in association to online banking and possible threats have substantial explanatory factors regarding respondents' online banking security practice. Particularly, it involves security countermeasure used by banks and customers' security preferences, and security conscious. The research found that self-awareness and practice influences respondents' behaviours and their level of knowledge in risk determining and mitigating. The weakness in user practice and knowledge pose bigger threats to financials security than any other components. Thus, the biggest challenge online security professionals is how to transform users from the biggest vulnerability into the first line of defense by providing and educating more specific security issues to enhance their self-efficacy and adequate knowledge. The use of robust security measures is also encouraged to continuing develop and ensured that it is mandatory used to all respondents by the ease and convenience is a key approach.

CHAPTER 6 CONCLUSIONS

6.1 Summary of the study

This research examined users' behaviours in online banking authentication security and their levels of understanding and experience of phishing. The objective was to identify their online self-awareness, opinions, knowledge, experience, and attitudes regarding phishing attacks and how their knowledge could protect themselves against these attacks. This study consisted of a survey of 226 people from various groups, according to gender, careers, ages, areas of living, and salary, of the Western Australian population. This ensured that the selected samples could be represented as generalisations and could correspond with government statistical records. It was found that self-efficacy and banks' security support services have differential impacts on the levels of respondents' risks, behaviours and opinions of online banking security.

Overall, phishing education is an effective tool to lessen susceptibility to phishing attacks. Lack of strong knowledge about phishing tends to mean that bank clients are more vulnerable to the attacks. Information about phishing and online attacks or threats is often only available from the banks themselves; the communications media generally only report massive international attacks. Self-awareness and high level cognitive skills are the key factors that minimise levels of personal liability to phishing and mean that individuals have appropriate solutions to the threats. Nevertheless, the respondents who have knowledge about phishing and have strong passwords still could be fooled by the threats if they rely on a single protection method.

Moreover, most respondents tended to choose simple security authentication to be their preference as they believed it would secure them from the hazards. Interestingly, their preferences were similar to the methods that their banks had provided for them. In other words, respondents chose their authentication security preferences based on their attitudes to usability and convenience rather than on methods they perceived to be increasingly secure. Many respondents saw security as largely the concern of the bank. Consequently, the majority was not prepared to act upon what they

believed would increase security, even though they knew basically what was good for them. Only a minority was willing to carry out recommended security measures, even if they were more complex.

Banks and security practitioners could take advantage of the respondents' loyalty, trust and confidence to bridge these gaps by providing education about anti-phishing techniques. According to respondents' experience, e-mail was the most sensitive tools that most respondents had experience with and they tended to fall in phishing attacks if they relied on unaware self-efficacy as discussed in chapter 5. Instead, providing educational and training showing the acts of users that could consequent into phishing attacks, and demonstrating effective use of multiple software protections should be available in enticingly and understandably forms in various channels. Channels that may increase users' perception should include (Quagliata, 2011):

(i) Computer-based training
(ii) Policies and procedures
(iii) Newsletters
(iv) E-mail
(v) Leader-led training
(vi) Video
(vii) Posters
(viii) Brochures

However, too many educational materials may decrease participants' tendencies to click on legitimate links. This suggests that banks need to find a better solution to educate users how to distinguish phishing from non-phishing so that they avoid false positives. Obviously, e-mail seems to be the unsuccessful tool in this regard because users these days are aware phishing e-mail. Whilst, the use of mandatory policies and procedures may be more appropriate because it is forcefully the users to follow bank's processes before moving to the next step of online transaction activities such as password changes, or robust password creation.

Strategies for protecting users from phishing generally fall into three major categories: eliminating the threats, warning users about the threats, and training users not to fall for phishing. These categories of anti-phishing strategy mirror three high-level approaches to usable security by banks: building robust systems without, or requiring less, intervention on the part of users, ensuring security is intuitive and easy to use, and educating users how to perform security-critical functions. These three approaches should be complementary to each other. Findings from this research also showed that users' education should be complemented with other countermeasures such as mandatory policies for password protection. Public warning campaigns are also desirable.

Where possible, the first layer of defence should always be automated solutions to filter and increase the default security offered to bank users' computers and web applications. Many phishing emails are filtered out at email gateway services, but consumers still need to be able to recognise those malicious emails which have proceeded through the filtering mechanisms. Without this first layer of defence, even well-trained users would be inundated with phishing messages that could paralyse their decision-making and cause them to take unnecessary risks.

Given that it may be quite difficult even for security practitioners to notice a compromised browser URL bar, users' computers can be infected with malware even without any preliminary user actions. In this study, more than 65% of the respondents needed proper phishing education. Hence user education in related aspects such as strong password creation, multi anti-malware installations, along with detection software and proper software updating, would not be sufficient to alleviate the problem. It is also essential to strengthen browsers, computer operating systems, and Internet connections.

However, bank users also need to acknowledge that such systems may not be entirely accurate in detecting phishing attacks. It could be said that there is neither a single tool nor a technique that will ever be completely secure and protect against

phishing attacks accurately. At the same time as automated protection, monitoring and detection systems which have the ability to defence against more complex intrusion activities, there still remains other trust decisions and solutions that the respondents should look into in order to act upon their decisions independently. Hence, a further step of defence is to develop a corresponding approach to assist the respondents so that they can help themselves in a crisis situation with the appropriate decision support. There are two options for this approach: educate users to stay away from the suspicious activities, or build and/or implement easy-to-use software and interfaces that prevent users from falling for attacks while performing their online transactions or checking their emails. Importantly, users have to be encouraged to demand stronger authentication from the online banks themselves. Whist low-cost authentication devices with sufficient secure and authenticated functions are acceptable, more services should be offered. Banks should focus on using the Internet's unique characteristics and capabilities to make their websites more reliable and easy to access. Moreover, banks may increase the users' perceptions of security in communicating with their online banking websites by addressing three key areas. They are addressing user concerns about current phishing activities, money fraud, or computer crime, enhancing privacy invasion protection by alerting the users for any transaction activities in their accounts, and providing and allocating sufficient information or security resources for further and comprehensive self-efficacy.

It is not only the bank trying to develop the best security to protect their customers and to educate users to be aware of the current threats, and encourage them to be more vigilant about any suspicious activities that could impact upon their financial accounts. Local, state and the federal government teams are also introducing ways that customers can be protected from cybercrime especially phishing attacks by addressing information on their websites or broadcasting on the television channels. In addition to the best practice, the government could run training programs about threats, new cybercrime attacks to customers and financial business employees. This information could add the practical guidelines that enable customers and financial staff to be proactive about the latest phishing or online frauds as well as some solutions to mitigate

the threats on their online account or inside the computer. However, expecting assistance from a helper will not be the final solution if users are not training themselves to distinguish between legitimate and counterfeit online banking platforms, and other information or material that look suspicious. Importantly, they should be aware and alert for any news or advertisements about phishing, scams, or any other fraudulent activities that could harm their finances or privacy.

6.2 Future research

This section consists of recommendations for further study as suggested by the present study. In future research, a larger scale investigation could be made. It is recommended that future research uses different types of question and multiple survey methods to capture information across a wide set of phenomena. In this research, some respondents were unwilling to disclose all their information credentials due to security and privacy concerns. Future research could also explore situations to other states in Australia and then other countries.

Also, a lack of in depth quantitative work exists in this field which would yield insights into some of the results in this and other studies. It would be of interest to examine the functions of online banking security mechanisms and to testify and compare their utilities in the online banking environment to ensure the security quality and to protect users from criminal activities.

Research that continues to monitor and investigate online banking users' protective and risk behaviours is also required. People are increasing using the Internet for the transactions; hence, an investigation of the relationship between age, career, genders and other factors with the self-efficacy, capability in dealing with phishing and interest in the online environment is an important direction for future research. Additionally, research is required to examine more intensive how self-efficacy of online banking users varies over time when the new technological challenges arrive and result in their online privacy and security changes.

Finally, the results of this study reveal interesting and useful information regarding security perception towards the use of online banking by the WA population. Current threats to bank customers were discussed in the literature chapter to examine what has happened to them and why was significant. The collected data also revealed ways that customers may have fell into phishing attacks and what recommendations should be more concerned to enhance security awareness and robust protection that banks may have overlooked.

REFERENCES

Afroz, S., & Greenstadt, R. (2011). *PhishZoo: Detecting Phishing Websites By Looking at Them*. Paper presented at the Fifth IEEE International Conference on Semantic Computing (ICSC 2011), Stanford University, CA, United States.

Alkhozae, M. G., & Batarfi, O. A. (2011). Phishing Websites Detection based on Phishing Characteristics in the Webpage Source Code. *International Journal of Information and Communication Technology Research, 1*(6), 283-291.

Alrubaiee, L., & Al-Nazer, N. (2010). Investigate the Impact of Relationship Marketing Orientation on Customer Loyalty: The Customer's Perspective. *International Journal of Marketing Studies, 2*(1), 155-174.

Anti-Phishing Working Group. (2007). *Phishing Activity Trends Report for the Month of December, 2007.* Retrieved from http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf

Anti-Phishing Working Group. (2010a). *Phishing Activity Trends Report, 2nd Half / 2010*. Retrieved from http://www.antiphishing.org/reports/apwg_report_h2_2010.pdf

Anti-Phishing Working Group. (2010b). *Phishing Activity Trends Report, 2nd Quarter / 2010* (2nd Quarter ed.). Retrived from http://www.apwg.com/reports/apwg_report_q2_2010.pdf

Anti-Phishing Working Group. (n.d.). Origins of the Word "Phishing". Retrieved from http://www.antiphishing.org/word_phish.html

AppleInsider Staff. (2012). Safari vulnerability in iOS 5.1 allows URL spoofing. Retrieved from http://www.appleinsider.com/articles/12/03/22/safari_vulnerability_in_ios_51_allows_url_spoofing.html

AusCert. (2008). *Home user computer security survey 2008*. Retrieved from http://www.auscert.org.au/images/AusCERT_Home_Users_Security_Survey_2008.pdf

Australian Bankers' Association. (2011). Scam warning – bogus phone survey. Retrieved from http://www.bankers.asn.au/Media/Media-Releases/Scam-warning---bogus-phone-survey

Australian Bureau of Statistics. (2011). *Household Use of Information Technology, Australia, 2010-11*. (Cat. No. 8146.0). Retrieved from http://www.abs.gov.au

Australian Bureau of Statistics. (2012). *Personal Fraud, 2010-2011* (Cat. No. 4528.0). Retrieved from http://www.abs.gov.au

Australian Bureau Statistics. (2010a). *Feature Article: Personal Fraud*. (Cat. No. 1301.0). Retrieved from http://www.abs.gov.au

Australian Bureau Statistics. (2010b). *Home Internet*. (Cat. No. 1370.0). Australia Bureau Statistics Retrieved from http://www.abs.gov.au

Australian Bureau Statistics. (2010c). *Information and Communication Technology (ICT) and Innovation Statistics Glossary*. Retrieved from http://www.abs.gov.au

Australian Bureau Statistics. (2010d). *Internet Activity, Australia, Jun 2010*. Retrieved from http://www.abs.gov.au

Australian Bureau Statistics. (2010e). *National Regional Profile: Perth (Statistical Division) : Economy*. Retrieved from http://www.abs.gov.au.

Australian Bureau Statistics. (2010f). *Population by Age and Sex, Regions of Australia, 2009*. Retrieved from http://www.abs.gov.au

Australian Bureau Statistics. (2011a). *Household Use of Information Technology, Australia, 2010-11*. (Cat. No. 8146.0). Retrieved from http://www.abs.gov.au

Australian Bureau Statistics. (2011b). *Western Australian Statistical Indicators, 2010.* Retrieved from http://www.abs.gov.au

Australian Communications and Media Authority. (2011). *The internet service market and Australians in the online environment*. Retrieved from http://www.acma.gov.au/webwr/_assets/main/lib310665/the_internet_service_market_in_australia.pdf

Australian Government. Dept of Broadband, Communication and the Digital Economy. (2008). *Online Statistics*. (Cat. No. 57471). Canberra, Australia.

Australian Government. Dept of Broadband, Communication and the Digital Economy. (n.d.). *Banking and paying bills online*. Canberra, Australia: An Australian Government Initiative Stay Smart Online.

Ayo, C. K., & Ukpere, W. I. (2010). Design of a secure unified e-payment system in Nigeria: A case study. *African Journal of Business Management, 4*(9), 1753-1760.

Babu, P. R., Bhaskari, D. L., & Satyanarayana, C. (2010). A Comprehensive Analysis of Spoofing. *International Journal of Advanced Computer Science and Applications, 1*(6), 157-162.

Bachelor, L. (2010). Online banking fraud losses rise 14%. Retrieved from the Guardian.co.uk website: http://www.guardian.co.uk/money/2010/mar/10/online-banking-fraud-loses-rise?INTCMP=SRCH

Banks increase security measures. (2010). Retrieved from the Australian Banking and Finance website: http://www.australianbankingfinance.com/technology/banks-increase-security-measures/

Barribeau, P., Butler, B., Corney, J., Doney, M., Gault, J., Gordon, J., . . . Waggoner, T. (n.d.). *Advantages and Disadvantages of the Survey Method*. Retrieved from http://writing.colostate.edu/guides/research/survey/com2d1.cfm

Bloor, D. (1983). *Wittgenstein: a social theory of knowledge*. United States: University of Michigan.

Brinkmann, M. (2009). Top list of brands that experienced the most phishing attacks in 2009. Retrieved from the Ghacks.net website: http://www.ghacks.net/2009/12/19/top-list-of-brands-that-experienced-the-most-phishing-attacks-in-2009/

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to the HTTPS protocol. *IEEE Security and Privacy, 7*(1), 78-81.

Cao, Y., Han, W., & Le, Y. (2008). Anti-phishing based on automated individual white-list. *Proceedings of the 4th ACM workshop on Digital identity management*, Alexandria, Virginia, USA.

Center for Civic Partnerships. (2007). Quantitative and Qualitative Evaluation Methods Retrieved from

http://www.civicpartnerships.org/docs/tools_resources/Quan_Qual%20Methods%209.07.htm

Choo, K.-K. R. (2011). *Cyber threat landscape faced by financial and insurance industry*. (No. 408). Canberra, Australia: Australian Institute of Criminology.

Cole, R. (2012). Threat from new virus-infected emails which take over your PC even if you DON'T open their attachments. Retrieved from the This is Money.co.uk website: http://www.thisismoney.co.uk/sciencetech/article-2094982/Threat-new-virus-infected-emails-PC-DONT-open-attachments.html

Commonwealth Bank of Australia. (2011). *Electronic Banking*. Retrived from http://www.commbank.com.au/personal/apply-online/download-printed-forms/ElectronicBanking_ADB2426.pdf

Commonwealth of Australia. (2011a). The internet service market and Australians in the online environment *Online behaviours by frequency of internet use.* Canberra, Australia: Australian Communication and Media Authority.

Commonwealth of Australia. (2011b). Requests for your account information ('phishing' scams). Canberra, Australia: Australian Competition and Consumer Commission (Scam Watch).

Commonwealth of Australia. (2012). Requests for your account information ('phishing' scams). Canberra, Australia: Australian Competition and Consumer Commission.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(2012), 1849-1858.

Dale, J. (2007). *Businesses support biometric signatures for online banking*. Retrieved from http://whitepapers.theregister.co.uk/paper/download/200/secure-mobile-working-reg-.pdf

David B. (2012). SSL and the future of authenticity: Comodo hack and secure protocol components [Web log post]. Retrieved from http://privacy-pc.com/articles/ssl-and-the-future-of-authenticity-comodo-hack-and-secure-protocol-components.html

DeepSearcher Inc. (2012).*Threats, Attacks, Hackers & Crackers* (Chapter 18). Retrieved from

http://www.intelligentedu.com/computer_security_for_everyone/18-threats-attacks-hackers-crackers.html

Department of Communications, Information Technology and the Arts. (2008). *Banking on the Internet: A Guide to Personal Internet Banking Services* (41673). Retrieved from http://www.archive.dcita.gov.au/1999/08/banking

Dey, I. (1993). *Qualitative data analysis: A user-friendly guide for social scientists*. London: Routledge.

Dixit, N., & Datta, D. S. K. (2010). Acceptance of E-banking among Adult Customers: An Empirical Investigation in India. *Journal of Internet Banking and Commerce, 15*(2).

Dobbs, T., & Maxwell, A. (2002). *Development of a Forest Estate Management Modelling Program Management Science Honours Project 2002*. Retrieved from http://www.mang.canterbury.ac.nz/courseinfo/msci/msci480/my%20webs/limitation.htm

E-business versus e-commerce. (2012) Retrieved from the Austrlian Trade Commission website: http://www.austrade.gov.au/e-business-versus-e-commerce/default.aspx

Evans, A., Poatsy, M. A., & Martin, K. (2009). Technology In Action Poster, 5/E [Ebook version]. Retrieved from http://wps.prenhall.com/bp_evans_techinaction_5/79/20368/5214371.cw/index.html

Financial Services Information Sharing and Analysis Center (FS-ISAC), & Internet Crime Complaint Center (IC3). (2012). *Fraud Alert Involving E-mail Intrusions to Facilitate Wire Transfers Overseas*. United States: Federal Bureau of Investigation (FBI) and National White Collar Crime Center (NW3C).

Florian, C. (2012, July 30). The Most Vulnerable Operating Systems and Applications in 2011 [Web log post]. Retrieved from http://www.gfi.com/blog/the-most-vulnerable-operating-systems-and-applications-in-2011/

Fox, J., Murray, C., & Warm, A. (2003). Conducting research using web-based questionnaires: practical, methodological, and ehtical considerations. *INT.J. Social Research Methodology, 6*(2).

Fung, A. P. H., & Cheung, K. W. (2010). *HTTPSLock: Enforcing HTTPS in Unmodified Browsers with Cached Javascript.* Paper presented at the 2010 Fourth International Conference on Network and System Security.

Garson, G. D. (2008). Scales and Standard Measures. Retrieved from the Statistical Associates Publishing website: http://faculty.chass.ncsu.edu/garson/PA765/standard.htm

Gartner. (2007). *Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks*. Retrieved from http://www.gartner.com/it/page.jsp?id=565125

Gastellier-Prevost, S., Granadillo, G. G., & Laurent, M. (2011). Decisive Heuristics to Differentiate Legitimate from Phishing Sites. *Network and Information Systems Security (SAR-SSI)*, 1-9.

Gedda, R. (2009). NAB targets customer service with voice recognition. Retrieved from the ComputerWorld website: http://www.techworld.com.au/article/302004/nab_targets_customer_service_voice_recognition

GFI Software. (n.d.). *Why one virus engine is not enough*. Retrived from http://www.gfi.com/whitepapers/why-one-virus-engine-is-not-enough.pdf

Gibson, D. (2011). The Dangers of Phishing. Retrieved from the Pearson website: http://www.pearsonitcertification.com/articles/article.aspx?p=1703673

GMA Network Inc. (2012). New email scams spoof Pinterest, LinkedIn, other social networking sites. Retrieved from the GMA News website: http://www.gmanetwork.com/news/story/256247/scitech/socialmedia/new-email-scams-spoof-pinterest-linkedin-other-social-networking-sites

Goyal, P., Batra, S., & Singh, A. (2010). A Literature Review of Security Attack in Mobile Ad-hoc Networks. *International Journal of Computer Applications, 9*(2), 11-15.

Greenfield, R. (2011). The Internet Password Paradox. Retrieved from the Atlantic Wire website: http://www.theatlanticwire.com/technology/2011/08/irony-internet-passwords/41078/

Hamid, N. R. A. (2006). *An Assessment of the Internet's Potential in Enhancing Consumer Relationships* (Doctoral dissertation). Retrieved from http://wallaby.vu.edu.au/adt-VVUT/uploads/approved/adt-VVUT20060919.112900/public/03chapters4-6.pdf

Hasan, M., & Harris, E. (2009). Entrepreneurship and innovation in e-commerce. *Journal of Achievements in Materials and Manufacturing Engineering, 32*(1), 92-97.

Hasan, M., Prajapati, N., & Vohara, S. (2010). Case study on social engineering techniques for persuasion. *International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) 2*(2), 17-23.

Help Net Security. (2012). Enhanced phishing methods on the rise. Retrieved from the Help Net Security website: http://www.net-security.org/secworld.php?id=11317

Hesse-Biber, S. N. (2010). *Mixed Methods Research: Merging Theory with Practice*. New York: The Guilford Press.

Higgins, K. J. (2012). *Zeus/SpyEye 'Automatic Transfer' Module Masks Online Banking Theft: Automated attack bypasses two-factor authentication*. Retrieved from the Dark Reading website: http://www.darkreading.com/authentication/167901072/security/attacks-breaches/240002267/zeus-spyeye-automatic-transfer-module-masks-online-banking-theft.html

Hunt, T. (2011). The science of password selection [Web log post]. Retrieved from http://www.troyhunt.com/2011/07/science-of-password-selection.html

Hyde, D. (2012). Hackers crack new online banking security putting 25m people at risk. Retrieved from the This is Money.co.uk website: http://www.thisismoney.co.uk/money/saving/article-2096060/Hackers-crack-new-online-banking-security-putting-25m-people-risk.html

Ingmar. (2011). Why complex passwords may be less secure than you think [Web log post]. Retrieved from http://www.eventlogblog.com/blog/2011/08/why-complex-passwords-can-be-i.html

Internet Crime Complaint Center's (IC3). (2012). *Internet Crime Complaint Center's (IC3) Scam Alerts*. United States: Federal Bureau of Investigation (FBI) and National White Collar Crime Center (NW3C).

James, C. (2008). Cyber-crooks bank on free phishing kits. Retrieved from the SC Magazine website: http://www.securecomputing.net.au/News/110497,cybercrooks-bank-on-free-phishing-kits.aspx

Johnson, M. (2008). *A new approach to Internet banking.* Cambridge, United Kingdom: University of Cambridge, Computer Laboratory.

Juniper Networks. (2012). *2011 Mobile Threats Report*. Retrived from https://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

Kavanagh, J. (2007). Banks upgrade web security. Retrieved from the Age.com.au website: http://www.theage.com.au/news/banking/banks-upgrade-web-security/2007/02/05/1170524024585.html

KeCrypt Systems Ltd. (2010). 83% of Businesses Think Their Bank Should Offer Biometric Signature Authentication for Online Banking. Retrieved from the Security-Technology News website: http://www.security-technologynews.com/article/83-of-businesses-think-their-bank-should-offer-biometric-signature-authentication-for-online-banking.html

Keizer, G. (2011). New malware scanner finds 5 per cent of Windows PCs infected. Retrieved from the ComputerWorld website: http://www.computerworld.com.au/article/388213/new_malware_scanner_finds_5_per_cent_windows_pcs_infected/

Kessem, L. S. (2012). What makes phishing so successful? Retrieved from the InformationWeek website: http://www.informationweek.in/Security/12-05-08/What_makes_phishing_so_successful.aspx

Kitten, T. (2012). Phisher Convicted in Massive Scheme: Attacks Aimed at Chase, BofA Highlight Increasing Risks. Retrieved from the GovinfoSecurity website: http://www.govinfosecurity.com/phisher-convicted-in-massive-scheme-a-4911

Kohli, S. (2008). Exploring vulnerabilities of threats to e-commerce with popularity of search engine. *Proceeing of the 2nd National Conference*. INDIACom-2008, New Delhi.

Kolsek, M. (2011, August 06). Google Chrome HTTPS Address Bar Spoofing [Web log post]. Retrieved from http://blog.acrossecurity.com/2012/01/google-chrome-https-address-bar.html

Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. *Journal in Computer Virology, 6*(2), 105-114.

Krauss, S. E. (2005). Research Paradigms and Meaning Making: A Primer. *The Qualitative Report, 10*(4).

Kuhn, T. S. (1970). *The Structure of Scientific Revolutions* (2 ed.). Chicago, United States: The University of Chicago.

Kulkarni, M. (2009). Local Phishing Using HTML Attachments. Retrieved from the Symantec website: http://www.symantec.com/connect/blogs/local-phishing-using-html-attachments

Lanthier, E. (2002). Questionnaire. Retrieved from the Northern Virginia Community Collage website: http://www.nvcc.edu/home/elanthier/methods/questionnaire.htm

Larkin, E. (2009). Mobile-Phone Banking: Convenient and Safe? Retrieved from the PCWorld website: http://www.pcworld.com/article/171866/mobilephone_banking_convenient_and_safe.html

Lichtenstein, S., & Williamson, K. (2006). Understanding consumer adoption of Internet banking: An interpretives study in the Australian banking context. *Journal of Electronic Commerce Research, 7*(2).

Litan, A. (2010, June 17). The little known secret of knowledge based authentication and why it fails so often [Web log post]. Retrieved from http://blogs.gartner.com/avivah-litan/2010/06/17/the-little-known-secret-of-knowledge-based-authentication-and-why-it-fails-so-often/

Major, S. D. A. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective, 18*(1), 40-46.

McAfee® Labs™. (2012). *2012 Threats Predictions*. Retrived from http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf

McDowell, M., & Lytle, M. (2010). *Security Tip (ST05-010): Understanding Web Site Certificates*. United States: US-Cert.

McGlasson, L. (2010). Customer Sues Bank After Phishing Attack. Retrieved from the BankinfoSecurity website: http://www.bankinfosecurity.com/customer-sues-bank-after-phishing-attack-a-2191

Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to Malware Incident Prevention and Handling. *Recommendations of the National Institute of Standards and Technology* (SP800-83). Gaithersburg, United States: National Institute of Standards and Technology.

Mendrez, R. (2011, October 4). Phishing Scam in an HTML Attachment [Web log post]. Retrived from http://labs.m86security.com/category/phishing/

Mersdorf, S. (2009). Qualitative vs. Quantitative Research Methods [Web log post]. Retrieved from http://survey.cvent.com/blog/cvent-survey/0/0/qualitative-vs-quantitative-research-methods

Microsoft. (2011). *Domain Name System*. Retrieved from http://technet.microsoft.com/en-us/network/bb629410

Microsoft. (2012). Microsoft Security Advisory *Unauthorized Digital Certificates Could Allow Spoofing* (2718704). Retrieved from http://technet.microsoft.com/en-us/security/advisory/2718704

Microsoft Support. (2012). *Internet Explorer does not support user names and passwords in Web site addresses (HTTP or HTTPS URLs).* Retrieved from http://support.microsoft.com/kb/834489

Mills, M., Bunt, G. G. v. d., & Bruijn, J. d. (2006). Comparative Research: Persistent Problems and Promising Solutions. *International Sociological Association, 21*(5), 619-631. doi: 10.1177/0268580906067833

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward and understanding of the online consumer's risky behavior and protection practices. *The journal of consumer affairs, 43*(3), 449-473.

Mobile Users Three Times More Vulnerable to Phishing Attacks [Web log post]. (2012). Retrieved from http://www.thedatachain.com/blog/2011/1/mobile_users_three_times_more_vulnerable_to_phishing_attacks

Moscaritolo, A. (2012). Banker trade group warns of phishing uptick. Retrieved from the SCMagazine website: http://www.scmagazine.com/banker-trade-group-warns-of-phishing-uptick/article/215440/

Naughton, J. (2011). Passwords shouldn't be simple, but this is getting ridiculous. Retrieved from the Guardian website: http://www.guardian.co.uk/technology/2011/sep/25/password-security-networker-john-naughton

Neill, J. (2003). Analysis of Professional Literature Class 5: Quantitative Research Design: Sampling & Measurement. Retrieved from the Wilderdom website: http://wilderdom.com/OEcourses/PROFLIT/Class5QuantitativeResearchDesignSamplingMeasurement.htm

Nielsen Company. (2006). The retail banking evolution: Battle of the banks hots up as smaller players take on the 'big four'. Retrieved from http://au.nielsen.com/news/20060630_1.shtml

Nielsen Company. (2007). Aussie consumers choose Internet banking over ATM, phone and branch. Retrieved from http://au.acnielsen.com/news/20070426.shtml

Noor, K. B. M. (2008). Case Study: A Strategic Research Methodology. *American Journal of Applied Sciences, 5*(11), 1602-1604.

Northern Territory Government of Australia. (2012). What is eBusiness? Retrieved from the Northern Territory Government of Australia website: http://www.nt.gov.au/dbe/business/starting-business/ebusiness/Pages/ebusiness.aspx

Online Trust Alliance. (2011). *Extended validation secure socket layer (EXSSL) certificates*. Retrieved from https://otalliance.org/resources/ev/

Optus. (n.d.). 3G Coverage Perth. Retrieved from the Optus website: http://www.optus.com.au/portal/site/aboutoptus/menuitem.813c6f701cee5a14f0419f108c8ac7a0/?vgnextoid=1eb879d4bc357010VgnVCM10000029867c0aRCR

D&vgnextchannel=e85776b387797010VgnVCM10000029867c0aRCRD&vgnextfmt=default

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*.

Phifer, L. (2010). Top Ten Phishing Facts. Retrieved from the eSecurity Planet website: http://www.esecurityplanet.com/views/article.php/3875866/Top-Ten-Phishing-Facts.htm

Piscitello, D. (2011). *Web vulnerabilities survey: results and analysis (Vol. June)*. Retrieved from http://www.antiphishing.org

Prandini, M., Ramilli, M., Cerroni, W., & Callegati, F. (2010). Splitting the HTTPS Stream to Attack Secure Web Connections. *IEEE Computer and Reliability Societies, 8*(6), 80-84.

Psychology Press Ltd. (2004). *Research Methods: Data Analysis*. Retrieved from http://onlineclassroom.tv/files/posts/research_methods_chapter/document00/psych%20methods.pdf

Quagliata, K. (2011). Impact of Security Awareness Training Components on Perceived Security Effectiveness. *Information Systems Audit and Control Association (ISACA) Journal, 4*(2011), 1-6.

Queensland. Department of Education, Training and Employment Policy and Procedure. (2012). *Malware and Malicious Code Prevention*. Queensland, Australia.

Qureshi, T. M., Zafar, M. K., & Khan, M. B. (2008). Customer Acceptance of Online Banking in Developing Economies. *Journal of Internet Banking and Commerce, 13*(1).

Rabkin, A. (2008). Personal knowledge questions for fallback authentication: security questions in the era of Facebook. *Proceedings of the 4th symposium on Usable privacy and security, Pittsburgh, Pennsylvania.*

Raja, J., velmurgan, M. S., & Seetharaman, A. (2008). E-payments: Problems and Prospects. *Journal of Internet Banking and Commerce, 13*(1).

Rashid, F. Y. (2012). Phishing remains most reliable cyber fraud mechanism. Retrieved from the SCMagazine website: http://www.scmagazine.com/phishing-remains-most-reliable-cyber-fraud-mechanism/article/248998/

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(2009), 816-826.

Rickards, R. C., & Ritsert, R. (2011). Coping with the challenges of indirect sales and distribution controlling in SMEs. *International Journal of Retail & Distribution Management, 39*(12), 927-944.

Ruggiero, P., & Foote, J. (2011). *Cyber Threats to Mobile Phones*. Retrived from http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf

Sale, J. E. M., Lohfeld, L. H., & Brazil, K. (2002). Revisiting the Quantitative-Qualitative Debate: Implications for Mixed-Methods Research. *Quality & Quantity, 36*(2002), 43-53.

Salehi, M., & Alipour, M. (2010). E-Banking in Emerging Economy: Empirical Evidence of Iran. *International Journal of Economics and Finance, 2*(1), 201-209.

Schneier, B. (2006). Real-World Passwords [Web log post]. Retrieved from http://www.schneier.com/blog/archives/2006/12/realworld_passw.html

Seltzer, L. (2009). *Spoofing Server-Server Communication: How You Can Prevent It*. Retrieved from https://otalliance.org/resources/ev/SSLStrip_Whitepaper.pdf

Sharma, M. (2010). Commonwealth Bank served as training ground for global phishing attacks. Retrieved from the ComputerWorld website: http://www.computerworld.com.au/article/365585/commonwealth_bank_served_training_ground_global_phishing_attacks/

Sharpe, M. (2008). HTTPS (HTTP over SSL or HTTP Secure). Retrieved from the SearchSftwareQuality website: http://searchsoftwarequality.techtarget.com/definition/HTTPS

Sines, S. (2011). Data Security: The Password Paradox. Retrieved from the Digital Union website: http://digitalunion.osu.edu/2011/03/29/data-security-the-password-paradox/

Singer, D. D., Baradwaj, B. G., Flaherty, S., & Rugemer, F. (2012). The frequency and intensity of experience in online banking use. *Journal of Internet Banking and Commerce, 17*(1).

Singh, D. P., Sharma, P., & Kumar, A. (2012). Detection of Spoofing attacks in Wireless network and their Remedies. *International Journal of Research Review in Engineering Science and Technology, 1*(1), 1-5.

Singhal, D., & Padhmanabhan, V. (2008). A Study on Customer Perception Towards Internet Banking: Identifying Major Contributing Factors. *Journal of Nepalese Business Studies, 5*(1), 101-111.

Social Research Centre. (2008). ANZ Survey of Adult Financial Literacy in Australia. Retrieved from http://www.anz.com/Documents/AU/Aboutanz/AN_5654_Adult_Fin_Lit_Report_08_Web_Report_full.pdf

Sofaer, S. (2002). Qualitative research methods. *International Jounal for Quality in Health Care, 14*(4), 329-336.

StatCounter. (2011). Top 5 Operating Systems in Australia from Jan to Dec 10. Retrieved from http://gs.statcounter.com/#os-AU-monthly-201001-201012

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., . . . Vigna, G. (2009). Your botnet is my botnet: analysis of a botnet takeover. *Proceedings of the 16th ACM conference on Computer and communications security*, Chicago, Illinois, USA.

Stross, R. (2010). A Strong Password Isn't the Strongest Security. Retrieved from the New York Times website: http://www.nytimes.com/2010/09/05/business/05digi.html

Subsorn, P., & Limwiriyakul, S. (2011). A compatative analysis of the security of Internet banking in Australia: a customer perspective. *Proceedings of the 2nd International Cyber Resilience Conference, Perth, Western Australia.*

Symantec. (2010). *State of Phishing: A monthly Report* (#27). Retrieved from http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_01-2010.en-us.pdf

TCT Solutions. (2011). DNS cache poisoning. Retrieved from the TCT Solutions website: http://tct-solutions.com/dns-cache-poisoning/

The Association for Educational Communications and Technology. (2001). What Is Descriptive Research?. Retrived from the AECT website: http://www.aect.org/edtech/ed1/41/41-01.html

Thomas, K. (2011). HTTPS Is Under Attack Again. Retrieved from the PCWorld website: http://www.pcworld.com/businesscenter/article/224721/https_is_under_attack_again.html

Thomas, R. (2006, August 2, 2009). The Quantitative Survey Method *Lecturer Notes*. Retrieved from http://www.docstoc.com/docs/30820325/The-Quantitative-Survey-Method

Thorat, S. B., Nayak, S. K., & Bokhare, M. M. (2010). Data security: an analysis. *International Journal on Computer Science and Engineering, 2*(4), 1355-1358.

TransPerth. (2010). TransPerth Zone Map. Retrieved from the TransPerth website: http://www.transperth.wa.gov.au/Default.aspx?tabid=362&id=109

Understanding E-business. (n.d.). Retrieved from the New South Wales Government Website: http://toolkit.smallbiz.nsw.gov.au/part/15/74/316/

United Nations World Food Programme. (n.d.). *Monitoring & Evaluation Guidelines: Choosing Methods and Tools for Data Collection*. Retrieved from http://documents.wfp.org/stellent/groups/public/documents/ko/mekb_module_13.pdf

US-CERT. (2008). *Multiple DNS implementations vulnerable to cache poisoning* (Vulnerability Note VU#800113). Retrieved from http://www.kb.cert.org/vuls/id/800113

Utakrit, N. (2006). *An investigation into the use of information and communication technology (ICT) by senior educators in Thailand* (Doctoral dissertation). Retrieved from http://library.ecu.edu.au/

Utakrit, N. (2008). *An Analysis of Phishing E-mail.* Poster session presented at the Proceedings of the Ninth Postgraduate Electrical Engineering & Computer Symposium (PEECS), Perth: The University of Western Australia.

Utakrit, N. (2009). Review of browser extensions, a man-in-the browser phishing techniques targeting bank customers. *Proceedings of the 7th Australian*

Information Security Management Conference. Perth, Western Australia: Edith Cowan University.

Valli, C. (2003). *Non-Business Use of The World Wide Web - A Study of Selected Western Australian Organisations* (Doctoral dissertation). Retrieved from http://library.ecu.edu.au/

Varkevisser, C. M., Pathmanathan, I., & Brownlee, A. (2003). *Designing and Conducting Health Systems Research Projects Volume 1: Proposal Development and Fieldwork*. HA Amsterdam: KIT Publishers.

Vinod, P., Laxmi, V., & Gaur, M. S. (2009). Survey on Malware Detection Methods. *Proceedings of the Thrid Hackers' Workshop on Computer and Internet Security* (pp.74-79). Kanpur, UP, India: Indian Institute of Technology (IIT).

Voutsas, K., & Heinrich, C. (2011). *Enhancing the banking customer value proposition through technology-led innovation*. Retrieved from http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Study_Bankingtech_E_DE.pdf

W3Schools. (2011). Web Statistics and Trends: OS Platform Statistics. Retrieved from the W3Schools website: http://www.w3schools.com/browsers/browsers_os.asp

Waite, K., & Harrison, T. (2004). Online Banking InformationL What we want and what we get. *Qualitative Market Research: An International Journal, 7*(1), 67-79.

Walliman, N. (2006). *Research Strategies and Design. Social Research Methods* [Ebook version]. doi: 10.4135/9781849209939.

Wang, J.-S., Yang, F.-Y., & Paik, I. (2011). A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices. *International Journal of Computer Science and Network Security, 11*(6), 12-19.

Warrell, A. (2011). *Computer Virus Guide*. Retrieved from http://www-public.jcu.edu.au/libcomp/computing/JCUPRD_034374

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computer and Security, 28*(2009), 47-62.

Wells, J., Hutchinson, D., & Pierce, J. (2008). Enhanced security for preventing man-in-the middle attacks in authentication, data entry and transaction verification. *Proceedings of the 6th Australian Information Security Management Conference.* Perth, Western Australia: Edith Cowan University.

Why VoIP Should Get VIP Treatment in Your Small Business. (2008) . Retrieved from the LeasingIdeas.com website: http://www.leasingideas.com/blog/business-technology/why-voip-should-get-vip-treatment-in-your-small-business/

Worthen, B. (2012). Email Giants Move to Slash 'Phishing'. Retrieved from the Wall Street Journal website: http://online.wsj.com/article/SB10001424052970204652904577191360158848618.html

Wright, K. B. (2005). Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of Computer-Mediated Communication, 10*(3).

Yeow, P. H. P., Yuen, Y. Y., & Tong, D. Y. K. (2008). User acceptance of Online Banking Service in Australia. *Communications of the IBIMA, 1*.

ZeuS-Style Attacks Trump Phishing as Greatest Threat to Online Banking. (2010). Retrieved from the SecurityWeek website: http://www.securityweek.com/zeus-style-attacks-trump-phishing-greatest-threat-online-banking

Zorz, Z. (2012). DNS-changing Trojan leads to phishing banking sites. Retrieved from the Help Net Security website: http://www.net-security.org/malware_news.php?id=2129

APPENDIX A: Glossary of term

Adware	A form of pop-up or any software package which automatically plays, displays, or downloads advertisements to a computer. Some may integrate with spyware purposed for interfere users' computer or gain personal information.
Backdoor	A program that allows unauthorised users remote access to a targeted computer without requiring user identification.
Botnet	A number of infected computer that are controlled by cyber-criminals to carry out their degenerate tasks, such as sending spam mails, performing denial-of-service attacks, or stealing personal credentials (Stone-Gross et al., 2009).
Rootkit	A program that hides the presence of another application in the computer system. It is used to gain a privilege to access to a computer and become undetectable by an anti-malware and alter the standard functionality of the system in a malicious and stealthy way (Mell, et al., 2005).
Spyware	A software that silently installed in a users' computer intended to collect user's information especially username, password, bank account details. The collected data will be transferred to the fraudster or the sender without users' knowledge.
Virus	A program which is designed to self-replicate and make copies of itself to files or computer system and disk drives (Warrell, 2011). It can damage application and data files and affect computer hardware.
Trojan horse	A harmful piece of software that looks legitimate and may allow an attacker remote access to a target computer system. It can attack computer hard drives, deleting files and re-writing system files.
Worm	A standalone self-replicating program that is completely self-contained and self-propagating (Mell, et al., 2005). It is aimed to gain access to computer silently and take up memory and network bandwidth. Effects of worm can slow down Internet traffic and stop responding.

APPENDIX B: Informed consent document to offline survey participants

QUESTIONNAIRE AND INTERVIEW SURVEY

Dear Research participants

You are invited to participate in this survey of "Security Awareness in Western Australian Online Banking Users of Phishing Attacks", part of the requirement for Doctor of Information Technology degree, School of Computer and Security Science (SCSS) at Edith Cowan University, Perth, Western Australia.

The purpose of this study is to determine your awareness of security issues relating to use of online banking. This survey will take approximately 5-10 minutes to complete. Your participation in this research is completely voluntary. You may decline to answer any question you do not wish to answer. You should also be aware that you have every right to withdraw from this research process at any time. A focus group interview may be requested if the information you provided in questionnaire is of interest. If you do decide to terminate the interview, you will also be able to remove all information you have provided, if you so wish.

This research has been approved by the ECU Human Research Ethics Committee. Ensuring confidentiality and anonymity is part of the researcher's responsibility. All data provided will be used only in the aggregate without identifying any person or organisation at any time and any place. In addition, if you agree to participate in a focus group interview, it will involve voice recording and video recordings only for the purpose of accuracy of data recording. If recordings are not possible, only notes will be

taken. All data and documents will be preserved in a secure place. Other than my supervisor(s), no one will have any access to any data I collect during this research.

If you require any further information concerning this research, please contact:

Miss Nattakant Utakrit

Contact address: School of Computer and Security Science (SCSS), Faculty of Computing, Health and Science, Edith Cowan University, Mt. Lawley, Western Australia, 6050.

E-mail: nattakau@student.ecu.edu.au

Tel: +61 422 228 393

If you have any concerns or complaints about the research project and wish to talk to an independent person, you may contact the:

Research Ethics Officer

Edith Cowan University

100 Joondalup Drive, Joondalup

Western Australia, 6027

Phone: (08) 6304 2170

E-mail: research.ethics@ecu.edu.au

Informed Consent Document

Security Awareness in Western Australian Online Banking Users of Phishing Attacks

I, the participant, have read the information above and clearly understand the contents provided. I also am informed that I have a full right to withdraw from this study at any time.

I willingly agree to participate in this study.

Participant ……..... Date .....

Investigator ……..... Date.....

APPENDIX C: Informed consent document to online survey participants

ONLINE SURVEY

Dear Research participants

You are invited to participate in this online survey of "Security Awareness in Western Australian Online Banking Users of Phishing Attacks", part of the requirement for Doctor of Information Technology degree, School of Computer and Security Science (SCSS) at Edith Cowan University, Perth, Western Australia.

The purpose of this study is to determine your awareness of security issues relating to use of online banking. This survey will take approximately 15 minutes to complete. Your participation in this research is completely voluntary. You may decline to answer any question you do not wish to answer. You should also be aware that you have every right to withdraw from this research process at any time.

This research has been approved by the ECU Human Research Ethics Committee. Ensuring confidentiality and anonymity is part of the researcher's responsibility. All data provided will be used only in the aggregate without identifying any person or organisation at any time and any place. All data and documents will be preserved in a secure place. Other than my supervisor(s), no one will have any access to any data I collect during this research.

If you require any further information concerning this research, please contact:

Miss Nattakant Utakrit

Contact address: School of Computer and Security Science (SCSS), Faculty of Computing, Health and Science, Edith Cowan University, Bradford Street, Mt. Lawley, Western Australia 6050.

E-mail: nattakau@our.ecu.edu.au

Tel: +61 422 228 393

If you have any concerns or complaints about the research project and wish to talk to an independent person, you may contact the:

Research Ethics Officer

Edith Cowan University

100 Joondalup Drive, Joondalup

Western Australia, 6027

Phone: (08) 6304 2170

E-mail: research.ethics@ecu.edu.au

Informed Consent Document

Security Awareness in Western Australian Online Banking Users of Phishing Attacks

I, the participant, have read the information above and clearly understand the contents provided. I also am informed that I have a full right to withdraw from this study at any time.

I willingly agree to participate in this study.

Participant ……..... Date .....

(Click accepted to start online survey or click unaccepted to leave from the survey)

ID ☐☐☐☐

APPENDIX D: A copy of questionnaire survey

This questionnaire includes 4 parts as follows:

Part A: Your background

Part B: Your experiences in using online banking

Part C: You experience in relation to online banking security

Part D: Your preferences in a deployment of online banking security protection

---

PART A: Your background. *Please cross (X) in the box for your most appropriate answer and fill in the blanks when necessary*

A1. Gender ☐ 1.Male ☐ 2. Female

A2. Age

☐ 1. Under 20 ☐ 2. 20 – 24

☐ 3. 25 – 29 ☐ 4. 30 – 34

☐ 5. 35 – 39 ☐ 6. 40 – 44

☐ 7.45 – 49 ☐ 8. Above 50

A3. Average annual income

☐ 1. Less than $ 20,000 ☐ 2. $20,001-$ 30,000

☐ 3. $30,001-$ 50,000 ☐ 4. $50,001 - $ 100,000

☐ 5. More than $100,000 ☐ 6. I prefer not to answer

A4. Occupation Please specify……

A5. Highest or current education level

☐ 1. PhD/ Dr. ☐ 2. Master Degree

☐ 3. Bachelor Degree ☐ 4. Diploma

☐ 5. High School ☐ 6. Others, please specify ……

A6. Usual place of residence Postcode……

PART B: Your experiences in using online banking

B1. Have you ever used online banking services? (eBay, PayPal, and online shopping are not included)

☐ 1. Yes (go to question B2) ☐ 2. No (go to question B10)

B2.Why did you decide to use online banking? You may choose more than one

☐ 1. Avoid waiting in a queue ☐ 2. Faster service computer operation

☐ 3. Reduce time spent commuting ☐ 4. Uncertain

☐ 5. Other, please specify ……

B3. Which online banking websites have you accessed? You can choose more than one

☐ 1. Commonwealth bank ☐ 2. BankWest ☐ 3. Westpac

☐ 4. ANZ bank ☐ 5. National bank ☐ 6. Citibank

☐ 7. HSBC bank ☐ 8. I prefer not to answer ☐ 9. Other …..

B4. Which online banking websites <u>are you still using</u>?

☐ 1. Commonwealth bank ☐ 2. BankWest ☐ 3. Westpac

☐ 4. ANZ bank ☐ 5. National bank ☐ 6. Citibank

☐ 7. HSBC bank ☐ 8. I prefer not to answer ☐ 9. Other ……

B5. From question B4, if you <u>have stopped</u> using some internet banking sites, why did you stop using online banking accounts?

……

……

B6. How often do (did) you use an online banking website each month?

☐ 1. None ☐ 2. 1 or 2 times ☐ 3. 3-5 times

☐ 4. 6-10 times ☐ 5. 11-20 times ☐ 6. More than 20

B7. What is (was) your main purpose for using online banking? You may choose more than one

☐ 1. Update personal information ☐ 2. Money transfer ☐ 3. Pay bill

☐ 4. Viewing balance and summary information ☐ 5. Other, please specify ……

B8. What is (was) the most important reason that you chose a particular bank as your major Internet bank? You may choose more than one

☐ 1. I have (had) a traditional bank account with the same bank

☐ 2. The brand name of the bank

☐ 3. The excellent service offered by this bank

☐ 4. The security protection offered by bank for online banking

☐ 5. Other, please specify……

B9. Where do (did) you usually access an online banking website? You may choose more than one

☐ 1. My house ☐ 2. School/ university/ college ☐ 3. My friend's house

☐ 4. Internet café ☐ 5. Public library ☐ 6. My workplace

☐ 7. I access online banking via mobile phone / palmtop

☐ 8. Other, please specify …….

B10. From question 1, why have you never used online banking? You may choose more than one option.

☐ 1. I am not interested in online banking.

☐ 2. I do not know how to use online banking.

☐ 3. I do not know how to use Internet.

☐ 4. I do not know how to use computer.

☐ 5. I have never heard of online banking.

☐ 6. I do not have an Internet connection.

☐ 7. I do not have an online banking account.

☐ 8. I do not have a computer. (Continued on the next page ----->)

☐ 9. I am concerned about security.

☐ 10. I have not had time to open an account.

☐ 11. I do not see any real value in using online banking or having an online banking account.

☐ 12. It is too new. I would like to see how it works, and then I may open an account.

☐ 13. It is not available through my bank.

☐ 14. Other, please specify ……

<u>Note.</u> If you have never used an online banking and finished answer question B10, this is end of your questionnaire. Thank you for your participation. Alternatively, if you have used an online banking and finished answer above questions, please continue to the following pages.

PART C: You experience in relation to online banking security

C1. What type of Internet connection do you use when accessing online banking? You may choose more than one

☐ 1. Analog (Dial-up modem) ☐ 2. ADSL wired broadband

☐ 3. Coaxial Cable ☐ 4. ADSL wireless broadband

☐ 5. ISDN broadband

☐ 6. I am not sure what type of internet connection I use

☐ 7. Other, please specify ……

C2.What type of operating system is installed on your computer? You may choose more than one

☐ 1. Windows 98 ☐ 2.Windows 2000 ☐ 3. Windows XP

☐ 4. Windows Vista ☐ 5. Windows 7 ☐ 6. Windows Mobile

☐ 7. Linux ☐ 8. Macintosh ☐ 9. MS-DOS

☐ 10. I am not sure what operating system I use

☐ 11. Other, please specify ……

C3. Do you have security protection on your computer? What type of security protection do you deploy on your computer (i.e. the computer with which you most often access online banking websites)? You may choose more than 1.

☐ 1. Yes, I have installed firewall application (e.g., Zone Alarm, Webroot, and Norton).

☐ 2. Yes, I have installed anti-virus software (e.g., Norton, AVG, Mcafee, and NOD32).

☐ 3. Yes, I have installed anti-spyware/ adware/ Trojan/backdoor (e.g., SpyBot, Spy Sweeper, and Spyware Doctor).

☐ 4. Yes, I have installed popup windows blocker (e.g., Super Ad Blocker,Pop-Up Stopper Anti-Spyware, and Pop-Up Sentry).

☐ 5. Yes, I have installed security protection, but I am not sure what type of security protection I have installed in my computer. (Continued on the next page)

☐ 6. I am not sure whether I have security protection or not (go to question C5).

☐ 7. No, I do not use computer security software protection (go to question C5).

☐ 8. Other, please specify ……

C4. How often do you update your security protection?

☐ 1. Once a day	☐ 2. Once a week	☐ 3. Once a month
☐ 4. Twice a day	☐ 5. Twice a week	☐ 6. Twice a month
☐ 7. Every 2 weeks	☐ 8. Every 3 months	☐ 9. Every 4-6 months
☐ 10. I do not need to update	☐ 11. Auto update	☐ 12. I am not sure

☐ 13. Other, please specify ……

C5. Which of the following statements best explains your online banking situation?

☐ 1. Your bank provides you with an application software program that operates on your PC. Then you dial into the bank via modem, download data, and operate the program that is resident on your PC.

☐ 2. You use a Web browser, but the actual banking software resides on the bank's server in the form of bank's home page.

☐ 3. I am not sure

☐ 4. Others, please specify ……

C6. Which security authentication are you provided when accessing an online banking website? You may choose more than one if you have more than one online banking account

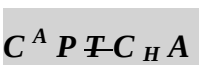
☐ 1. Login + password

☐ 2. Login+ password+ biometric

☐ 3. Login+ password+ token device

☐ 4. Login + password + mobile (SMS) verification code

☐ 5. Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank

☐ 6. Login + password + challenge-response (random verification) code (e.g.,  or ) (Continued on the next page)

☐ 7. Login + password + security questions (e.g., what is your mother's maiden name?)

☐ 8. Others, please specify ……

C7. How many characters (letters or numbers) are there in your online banking password?

☐ 1. 4 ☐ 2. 6 ☐ 3. 8

☐ 4. 10 ☐ 5. Other, please specify…….

☐ 6. I prefer not to answer

C8. Have you ever been locked out from your online account due to providing incorrect passwords multiple times?

☐ 1. Yes (go to question C9) ☐ 2. No (go to question C10)

C9. From question 8, when you have been locked out from your online banking account, did the online banking system allow you to log in again after sometime?

☐ 1. Yes ☐ 2. No

C10. If you have (had) a problem with accessing your online banking, how would you report your problem? You may choose more than one.

☐ 1. Report via e-mail provided

☐ 2. Report via the report form on web page

☐ 3. Call number provided on 'contact us' page

☐ 4. Report to police

☐ 5. Direct inform by walk in to the branch office

☐ 6. I am not sure

☐ 7. I do not report

☐ 8. Other, please specify ……

C11. Which type of financial institution do you believe has the <u>strongest</u> online security?

☐ 1. Banks ☐ 2. Credit Card Company

☐ 3. Online Stock Brokers ☐ 4. Online Auction websites

☐ 5. I am not sure

☐ 6. Online Payment Processing Company (e.g., PayPal)

☐ 7. Online Shopping Websites (e.g., Ebay, Amazon)

☐ 8. Others, please specify ……

C12. From question C11, What do you like about their security?

……

……

……

☐ I do not know

PART D: Your preferences in a deployment of online banking security protection

D1. If your bank asks you to pay mandatory fees for the use of additional security measures such as biometric (physical security authentication) or token devices, are you willing to pay for this service?

Biometrics is used as a form of identity access control in which refers to methods for uniquely recognizing humans based upon intrinsic physical or behavioral traits such as such as retina scan, fingerprint scan, and voice recognition.

Security Token is a random numeric code device; known as digital token, that is used to identify one's identity electronically as in the case of a customer is who they claim to be trying to access their bank account. 

☐ 1. Yes (go to question D2) ☐ 2. No (go to question D3)

D2. How much are you willing to pay for using biometric or token devices?

☐ 1. $1 per month ☐ 2. $2-$5 per month ☐ 3. $6-$10 per month

☐ 4. More than $10 per month ☐ 5. I am not sure ☐ 6. Other…….

D3. Which type of password would you prefer to secure your online banking account from online banking scam?

☐ 1. Numbers ☐ 2. Lower case alphabets (e.g., abc)

☐ 3. Upper case alphabets (e.g., ABC) ☐ 4. Special characters (e.g., @#%&*)

☐ 5. Mixed of numbers and lower case alphabets

☐ 6. Mixed of numbers and upper case alphabets

☐ 7. Mixed of numbers and special characters

☐ 8. Mixed of numbers, special characters, lower case and upper case alphabets

☐ 9. I prefer not to answer

☐ 10. Others, please specify ……

D4. Which security options give you a feeling of security about your online experience? You may please choose more than one.

☐ 1. Login + password

☐ 2. Login+ password+ biometric such as retina scan, fingerprint scan, and voice recognition

☐ 3. Login+ password+ token device

☐ 4. Login + password + mobile (SMS) verification code

☐ 5. Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank

☐ 6. Login + password + challenge-response (random verification) code (e.g.,  or )

☐ 7. Login + password + security questions (e.g., what is your mother's maiden name?)

☐ 8. Others, please specify ……

D5. If your bank asks you to change your online banking password periodically in order to protect your account from unauthorized use, would you agree to make the change?

☐ 1. Yes, I would agree.

☐ 2. No, I would not agree. Please specify your reason ……

D6. How often would you prefer to change your online banking password?

☐ 1. Every month ☐ 2. Every 3 months ☐ 3. Every 6 months

☐ 4. Once a year ☐ 5. I am not sure ☐ 6. Never

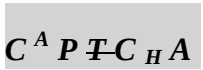
☐ 7. Other, please specify ……

D7. In your opinion what minimum length of passwords should be in your online banking system? **Please specify the number**

……

(Next page >)

D8. These are the most common online banking security protection methods. Please prioritise your online banking security methods from the maximum protection to the minimum protection in your opinion by indicating number 1, 2, 3...to 7.

1: the maximum protection7: the minimum protection	For example	Your ranks
1. Login + password	7	
2. Login+ password+ biometric	3	
3. Login+ password+ token device	1	
4. Login + password + mobile (SMS) verification code	6	
5. Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank	5	
6. Login + password + challenge-response (random verification) code (e.g.,  or )	4	
7. Login + password + security questions (e.g. what is your mother's maiden name?)	2	

ID ☐☐☐☐

<u>Question D9 – D10</u> please rate (x) on the scale where you think it is appropriate.

5 = strongly believe 4 = believe 3= neither believe nor do not believe

2 = do not believe 1 = strongly do not believe

D9. Your opinion in relation to the safety of using online banking?	**5**	**4**	**3**	**2**	**1**
1. Using an online banking system is financially secure.					
2. I trust an online banking system to protect my personal information					
3. I have confidence in the security measures that my online banking system uses.					
4. Attack incidents against online banking systems have no influence in my level of confidence about online banking					
5. I am able to distinguish if a financial institution's website is secure.					
6. I am satisfied with the security protection of my online banking account.					
7. I consider that security features are a main factor in my decision whether or not to do business with an Internet based company					
8. My bank should offer security metrics to measure how secure my online banking is that would be valuable to me.					

5 = I strongly agree 4 = I agree 3= neither agree nor disagree

2 = disagree 1 = I strongly disagree

D10. Your opinion about security of your online banking system.	**5**	**4**	**3**	**2**	**1**
1. My bank should apply multi security protection, such as login and password and SMS mobile verification code and digital signature.					
2. My bank should prompt me with a security question, such as 'what is your mother's maiden name?' every time I log on to my online banking account.					
3. My bank should offer a tracking facility showing all transactions and detail about when I have logged in and out.					
4. My bank should never allow more than one computer access to the same online banking account at the same time.					
5. My bank should detect, deny & stop all online banking activities if there is more than one computer accessing the same online banking account at the same time.					
6. My bank should log off my account automatically when I close the window.					
7. My bank should log off my account automatically after I have been logged on for 45 minutes.					
8. My bank should log off my account automatically if my bank webpage is not active for 15 minutes.					

D11. Do you have any comments about using online banking or security protection for online banking?

……

……

ID

APPENDIX E: A copy of interview/open-ended questionnaire

This semi-instructional form attempts to gain direct information from respondents in online scam threat experience. **Please provide your information/ opinion as much as possible.**

1. Have you ever heard of any online banking threat from media, your friend or your bank? Please tell us about that (ATM skimming device is not included).

2. What do you know about "phishing" (online banking scam)?

3. What do you know about spyware/adware/ Trojans?

4. Do you know anything about how your personal information can be stolen from the Internet?

5. What is your opinion about using a combination of numbers and both upper and lower case characters can help you from an online banking scam?

6. Do you think that a password using your personal detail such as date of birth or phone number is insecure?

7. Could you tell me your opinion with the sentence “changing password every 3-6 months can protect your online banking account from phishing”?

8. Have you ever received an e-mail from a bank that asked you to provide your confidential information? What did you do?

9. How do you determine that e-mails that appear to be from the banks are not e-mail scam?

10. How do you distinguish your online banking webpage whether it is a legitimate webpage or a counterfeit webpage?

11. Have your online banking account ever been attacked by a scammer? What did you do?

12. From the question above, was the attacker successful in obtaining anything from your account?

13. Was the attacker successful in the use of or attempt to use your personal information for some other fraudulent purpose such as medical care, a job, or government benefits, renting accommodation, giving your information to the police when they were charged with a crime or traffic violation, or something else?

14. In your opinion what are the vulnerable points that make the phishing successful in online banking attacks?

15. What did you do to protect yourself or solve the problem?

16. Do you think that installing either anti-virus or anti-spyware/Trojan is enough to secure your computer from being attacked? If not, please clarify your reason.

17. Please tell us about how to secure yourself from phishing e-mails, phishing webpages and any other phishing activities that could occur in your daily life?

18. Do you have any comment or anything that you would like to tell us or banks about phishing, online banking security, or the future of online banking attacks?

End of Questionnaire

Thank you for your participation

APPENDIX F: Online Survey Poster

APPENDIX G: Focus Group/ Seminar Poster

APPENDIX H: Data of respondents' background

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
1	Male	20 - 24	I prefer not to answer	Student	Student	Bachelor Degree	6027
2	Male	Above 50	I prefer not to answer	Retired	Retired	High School	6151
3	Female	45 - 49	30,001-50,000	Library Assistant	Clerical and administrative Workers	Diploma	6007
4	Male	40 - 44	> 100,000	Information Architect	Professionals	Bachelor Degree	6151
5	Female	40 - 44	No answer	Home keeper	Home Duties	Bachelor Degree	6014
6	Female	40 - 44	< 20,000	Home Executive	Professionals	Diploma	6010
7	Female	35 -39	I prefer not to answer	Importer	Technicians and Trades Workers	Bachelor Degree	6018
8	Female	45 - 49	I prefer not to answer	House Wife	Home Duties	Bachelor Degree	6018
9	Female	45 - 49	50,001-100,000	Business Owner	Professionals	High School	6014
10	Female	25 -29	20,001-30,000	Sales Assistant	Sales Workers	High School	6066
11	Female	25 -29	30,001-50,000	Sales Assistant	Sales Workers	High School	6155
12	Female	45 - 49	< 20,000	Home duties	Home Duties	Bachelor Degree	6014
13	Male	30 - 34	< 20,000	Tutor	Miscellaneous	Master Degree	6060
14	Female	Above 50	I prefer not to answer	IT Consultant	Professionals	High School	6006
15	Male	25 -29	< 20,000	Student	Student	Bachelor Degree	6107
16	Male	40 - 44	50,001-100,000	Teacher	Professionals	Bachelor Degree	6027
17	Female	25 -29	20,001-30,000	Customer Service	Clerical and administrative Workers	Master Degree	6104
18	Male	25 -29	< 20,000	Student	Student	Master Degree	6051
19	Female	25 -29	< 20,000	Student	Student	Bachelor Degree	6027
20	Male	30 - 34	30,001-50,000	Student	Student	Bachelor Degree	6061
21	Female	20 - 24	I prefer not to answer	Student	Student	Master Degree	6059

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
22	Male	20 - 24	I prefer not to answer	Small Office Home Office	Miscellaneous	Master Degree	6052
23	Male	25 -29	< 20,000	Student	Student	Master Degree	6062
24	Male	30 - 34	50,001-100,000	Swedish	Miscellaneous	Bachelor Degree	6027
25	Male	25 -29	I prefer not to answer	Student	Student	Master Degree	6059
26	Female	25 -29	I prefer not to answer	Student	Student	Bachelor Degree	6016
27	Female	25 -29	I prefer not to answer	Student	Student	Other, please specify	6014
28	Female	30 - 34	< 20,000	Student	Student	Diploma	6061
29	Male	Above 50	50,001-100,000	Manager	Managers	Master Degree	6006
30	Male	Above 50	20,001-30,000	Retired	Retired	High School	6009
31	Male	20 - 24	I prefer not to answer	Student	Student	High School	6060
32	Male	20 - 24	< 20,000	Student	Student	Master Degree	6021
33	Female	25 -29	< 20,000	Student	Student	Bachelor Degree	6163
34	Male	30 - 34	I prefer not to answer	Student	Student	Bachelor Degree	6060
35	Male	35 -39	50,001-100,000	ESL Teacher	Professionals	Bachelor Degree	6147
36	Male	20 - 24	< 20,000	Student	Student	Diploma	6062
37	Male	25 -29	50,001-100,000	IT engineer	Professionals	Diploma	6008
38	Male	20 - 24	< 20,000	No answer	No answer	Bachelor Degree	No answer
39	Male	20 - 24	50,001-100,000	Student	Student	High School	6014
40	Female	35 -39	> 100,000	Home Business Owner	Professionals	Diploma	6107
41	Female	20 - 24	< 20,000	Student	Student	High School	No answer
42	Female	20 - 24	20,001-30,000	Student	Student	Bachelor Degree	6021
43	Female	20 - 24	I prefer not to answer	Walker for Salmart	Community and Personal Service Workers	Bachelor Degree	6020

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
44	Male	Under 20	< 20,000	Service Cashier	Sales Workers	High School	6169
45	Female	20 - 24	< 20,000	Student	Student	Bachelor Degree	6157
46	Female	20 - 24	30,001-50,000	Library Technician	Technicians and Trades Workers	Bachelor Degree	6103
47	Female	Under 20	< 20,000	Student	Student	High School	6028
48	Female	Above 50	50,001-100,000	University Lecturer	Professionals	Master Degree	6055
49	Male	20 - 24	20,001-30,000	Student	Student	Master Degree	6060
50	Female	35 -39	< 20,000	No answer	No answer	Master Degree	6027
51	Male	45 - 49	I prefer not to answer	Instructional Designer	Professionals	Diploma	6151
52	Female	20 - 24	< 20,000	Student	Student	Master Degree	6059
53	Male	45 - 49	> 100,000	High School Vice Principal	Professionals	Master Degree	No answer
54	Female	25 -29	50,001-100,000	Project Administrator	Clerical and administrative Workers	High School	6153
55	Male	25 -29	< 20,000	Senior Pre-Sale Network Engine	Technicians and Trades Workers	Master Degree	No answer
56	Female	Above 50	50,001-100,000	Director	Professionals	Master Degree	6052
57	Male	45 - 49	50,001-100,000	Designer	Professionals	PhD/Dr.	6163
58	Female	25 -29	< 20,000	Student	Student	Master Degree	6061
59	Female	Above 50	30,001-50,000	Medical Secretary	Clerical and administrative Workers	High School	6026
60	Female	Above 50	30,001-50,000	Receptionist	Clerical and administrative Workers	Bachelor Degree	6025
61	Female	Above 50	50,001-100,000	Instructional Designer	Professionals	Diploma	No answer
62	Female	Above 50	50,001-100,000	Administrator	Clerical and administrative Workers	High School	6006
63	Male	Above 50	> 100,000	Group Manager	Managers	Bachelor Degree	6006
64	Female	30 - 34	< 20,000	Shop Worker	Technicians and Trades Workers	Bachelor Degree	6018
65	Male	30 - 34	30,001-50,000	Programmer	Professionals	Master Degree	No answer

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
66	Male	25 -29	< 20,000	Student	Student	Master Degree	6018
67	Male	25 -29	50,001-100,000	Software Security Engineer	Professionals	Bachelor Degree	No answer
68	Male	25 -29	50,001-100,000	Web Developer	Professionals	Diploma	6062
69	Female	Above 50	50,001-100,000	Academic	Professionals	PhD/Dr.	6003
70	Female	Above 50	I prefer not to answer	Student	Student	Bachelor Degree	6065
71	Female	45 - 49	I prefer not to answer	System and Business Consultant	Professionals	Bachelor Degree	6151
72	Female	Above 50	50,001-100,000	Teacher	Professionals	Master Degree	6012
73	Male	Above 50	> 100,000	Educator, Manager	Managers	Bachelor Degree	6101
74	Female	45 - 49	> 100,000	Recruitment	Professionals	Bachelor Degree	6151
75	Female	25 -29	< 20,000	Student	Student	Diploma	6060
76	Female	30 - 34	< 20,000	Student	Student	Master Degree	6003
77	Male	25 -29	< 20,000	Student	Student	Master Degree	6009
78	Female	Above 50	I prefer not to answer	Library Technician	Technicians and Trades Workers	Bachelor Degree	6066
79	Male	35 -39	50,001-100,000	Library Manager	Managers	Master Degree	6027
80	Female	25 -29	50,001-100,000	Engineer	Professionals	Bachelor Degree	6009
81	Male	25 -29	50,001-100,000	Draftsman	Machinery Operators and Drivers	Bachelor Degree	6008
82	Female	25 -29	50,001-100,000	Engineer	Professionals	Bachelor Degree	6065
83	Female	20 - 24	30,001-50,000	Mortgage Specialist	Professionals	Bachelor Degree	6103
84	Male	35 -39	50,001-100,000	Manager	Managers	High School	6000
85	Male	Above 50	50,001-100,000	No answer	No answer	Diploma	No answer
86	Male	Above 50	50,001-100,000	Retired Bookkeeper	Retired	Bachelor Degree	6155
87	Female	Under 20	No answer	Student	Student	High School	6014
88	Female	40 - 44	> 100,000	Lawyer	Professionals	Bachelor Degree	6014
89	Male	Above 50	50,001-100,000	Retired	Labourers	Diploma	6018

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
90	Female	40 - 44	I prefer not to answer	No answer	No answer	High School	6062
91	Male	Under 20	< 20,000	Shop assistant	Sales Workers	High School	6018
92	Female	No answer	I prefer not to answer	Retired	Retired	High School	6065
93	Female	Above 50	50,001-100,000	Economist-Finance	Professionals	Bachelor Degree	6027
94	Male	45 - 49	30,001-50,000	Food technologist	Technicians and Trades Workers	Master Degree	6027
95	No answer	Above 50	50,001-100,000	Butcher	Labourers	High School	6030
96	Male	No answer	No answer	No answer	No answer	No answer	No answer
97	Male	Above 50	30,001-50,000	Retired	Retired	High School	6065
98	Female	45 - 49	30,001-50,000	Student	Student	Bachelor Degree	6027
99	Male	30 - 34	50,001-100,000	Bricklayer	Labourers	High School	6020
100	Female	Above 50	30,001-50,000	Library Office	Clerical and administrative Workers	High School	6503
101	Male	Above 50	20,001-30,000	Retired	Retired	Diploma	6065
102	Female	Above 50	No answer	Retired	Retired	Bachelor Degree	6027
103	Female	Above 50	I prefer not to answer	Marketing Manager	Managers	High School	6023
104	Female	25 -29	50,001-100,000	OHS Advisor	Professionals	No answer	6065
105	Female	25 -29	50,001-100,000	Journalist	Professionals	Bachelor Degree	6020
106	Female	Above 50	50,001-100,000	No answer	No answer	Bachelor Degree	6069
107	Female	45 - 49	50,001-100,000	No answer	No answer	Diploma	6025
108	Male	Under 20	< 20,000	Student	Student	High School	6014
109	Female	45 - 49	50,001-100,000	Pharmacy Assistant	Clerical and administrative Workers	Diploma	6014
110	Male	45 - 49	30,001-50,000	Chef	Technicians and Trades Workers	Bachelor Degree	6051
111	Male	Above 50	< 20,000	Retired Mechanic	Retired	Diploma	6062
112	Male	Above 50	I prefer not to answer	Accountant	Professionals	Bachelor Degree	No answer

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
113	Male	40 - 44	50,001-100,000	Accountant	Professionals	Diploma	6011
114	Female	30 - 34	> 100,000	Lawyer	Professionals	Bachelor Degree	6022
115	Male	20 - 24	20,001-30,000	Bartender	Labourers	Diploma	6018
116	Male	Above 50	50,001-100,000	Building Construction	Professionals	Bachelor Degree	6010
117	Male	Above 50	30,001-50,000	No answer	No answer	High School	No answer
118	Male	20 - 24	< 20,000	Student	Student	Bachelor Degree	6010
119	Male	45 - 49	> 100,000	Company Director	Professionals	Bachelor Degree	6014
120	Male	Above 50	50,001-100,000	Social Worker	Community and Personal Service Workers	Bachelor Degree	6022
121	Female	Above 50	50,001-100,000	No answer	No answer	Bachelor Degree	6018
122	Male	45 - 49	> 100,000	No answer	No answer	Bachelor Degree	6014
123	Female	45 - 49	30,001-50,000	Journalist	Professionals	Bachelor Degree	6014
124	Female	40 - 44	No answer	Housewife	Home Duties	High School	6014
125	Female	30 - 34	< 20,000	IT research and development	Professionals	Master Degree	No answer
126	Female	Above 50	50,001-100,000	No answer	No answer	Diploma	6019
127	Female	35 -39	50,001-100,000	Business Owner	Professionals	High School	6030
128	Female	30 - 34	30,001-50,000	Teacher	Professionals	Bachelor Degree	6503
129	Male	Above 50	50,001-100,000	Financial Planner	Professionals	Diploma	6024
130	Female	Above 50	50,001-100,000	Women Gym Manager	Managers	High School	6024
131	Female	Above 50	< 20,000	Home duties	Home Duties	High School	6020
132	Female	40 - 44	I prefer not to answer	No answer	No answer	High School	No answer
133	Male	Above 50	50,001-100,000	Accountant	Professionals	Bachelor Degree	6023
134	Female	30 - 34	30,001-50,000	Graphic Designer	Professionals	Bachelor Degree	6151
135	Male	30 - 34	< 20,000	Student	Retired	Master Degree	6003
136	Female	30 - 34	I prefer not to answer	Student	Retired	Master Degree	6003

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
137	Male	40 - 44	I prefer not to answer	Business Owner	Professionals	Bachelor Degree	6018
138	Female	Above 50	I prefer not to answer	No answer	No answer	Master Degree	6014
139	Female	40 - 44	50,001-100,000	Health Professional	Professionals	Bachelor Degree	6156
140	Male	No answer	No answer	No answer	No answer	No answer	No answer
141	Male	Above 50	50,001-100,000	Consultant	Professionals	Master Degree	6014
142	Male	45 - 49	20,001-30,000	Painter	Labourers	High School	6027
143	Female	Above 50	20,001-30,000	Florist Sale Assistant	Sales Workers	High School	6059
144	Female	30 - 34	20,001-30,000	Student	Student	PhD/Dr.	6064
145	Male	Above 50	50,001-100,000	No answer	No answer	Bachelor Degree	6018
146	Male	Above 50	50,001-100,000	Heavy vehicle driver	Machinery Operators and Drivers	High School	6062
147	Male	Above 50	50,001-100,000	Truck Driver	Machinery Operators and Drivers	High School	6025
148	Female	Above 50	I prefer not to answer	No answer	No answer	High School	No answer
149	Female	25 -29	50,001-100,000	Engineer	Professionals	Bachelor Degree	No answer
150	Female	Above 50	30,001-50,000	Cleaner	Labourers	High School	6169
151	Female	40 - 44	30,001-50,000	Deli Assistant	Sales Workers	High School	6063
152	Female	40 - 44	30,001-50,000	Travel Agent	Technicians and Trades Workers	High School	6027
153	Female	30 - 34	30,001-50,000	No answer	No answer	Other, please specify	6064
154	Male	Above 50	20,001-30,000	Small Business Owner	Technicians and Trades Workers	High School	6064
155	Female	Above 50	30,001-50,000	Retail Sales	Sales Workers	High School	6163
156	Male	45 - 49	50,001-100,000	CEO	Professionals	High School	6062
157	Male	25 -29	50,001-100,000	Concreter	Labourers	High School	6064
158	Female	Above 50	20,001-30,000	No answer	No answer	High School	6430
159	Male	35 -39	50,001-100,000	No answer	No answer	High School	6060

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
160	Male	Above 50	50,001-100,000	Consultant	Professionals	PhD/Dr.	6919
161	Male	45 - 49	50,001-100,000	Administration	Clerical and administrative Workers	Diploma	6064
162	Male	Above 50	I prefer not to answer	Disability Pensions	Miscellaneous	High School	6063
163	Female	35 -39	30,001-50,000	Function Manager	Managers	High School	6066
164	Male	40 - 44	< 20,000	No answer	No answer	Bachelor Degree	6066
165	Female	40 - 44	50,001-100,000	Electrician	Technicians and Trades Workers	Other, please specify	6060
166	Male	Above 50	30,001-50,000	No answer	No answer	Diploma	6064
167	Male	35 -39	30,001-50,000	Baker	Technicians and Trades Workers	High School	6061
168	Female	40 - 44	30,001-50,000	Dry Cleaner	Labourers	Diploma	6108
169	Male	20 - 24	< 20,000	Student	Student	High School	6014
170	Male	30 - 34	50,001-100,000	Part Interpreter	Miscellaneous	Master Degree	6019
171	Male	Above 50	50,001-100,000	Health Worker	Community and Personal Service Workers	Diploma	6018
172	Male	Above 50	50,001-100,000	No answer	No answer	High School	6015
173	Female	30 - 34	30,001-50,000	Carer	Community and Personal Service Workers	Diploma	6016
174	Male	Above 50	30,001-50,000	Wool Classer	Machinery Operators and Drivers	Other, please specify	6014
175	Male	40 - 44	50,001-100,000	Civil/ Structure Engineer	Professionals	Bachelor Degree	6062
176	Female	Above 50	< 20,000	Medical Secretary	Clerical and administrative Workers	High School	6026
177	Male	Above 50	50,001-100,000	A/C Tech	Technicians and Trades Workers	High School	6018
178	Male	35 -39	50,001-100,000	Computer Technician	Technicians and Trades Workers	Bachelor Degree	6112
179	Female	Under 20	I prefer not to answer	Student	Student	High School	6014
180	Male	25 -29	20,001-30,000	Hotline technician	Technicians and Trades Workers	Diploma	6059
181	Male	25 -29	20,001-30,000	IT Executive	Professionals	Master Degree	No answer

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
182	Male	25 -29	30,001-50,000	No answer	No answer	Bachelor Degree	No answer
183	Male	30 - 34	30,001-50,000	Business	Miscellaneous	Bachelor Degree	6100
184	Male	30 - 34	30,001-50,000	IT Technician	Technicians and Trades Workers	Diploma	No answer
185	Female	20 - 24	< 20,000	Student	Student	Bachelor Degree	6018
186	Female	20 - 24	< 20,000	Student	Student	Master Degree	6051
187	Male	30 - 34	20,001-30,000	Hospitality	Technicians and Trades Workers	Master Degree	6062
188	Female	40 - 44	< 20,000	Student	Student	Master Degree	6007
189	Male	30 - 34	30,001-50,000	Helpdesk Support	Technicians and Trades Workers	Master Degree	6000
190	Male	40 - 44	< 20,000	Tai Chi Instructor	Miscellaneous	Other, please specify	6018
191	Male	45 - 49	20,001-30,000	Student	Student	Bachelor Degree	6066
192	Female	30 - 34	I prefer not to answer	Student	Student	Master Degree	6014
193	Male	20 - 24	< 20,000	Student	Student	Bachelor Degree	6152
194	Male	20 - 24	I prefer not to answer	No answer	No answer	Master Degree	6127
195	Male	Under 20	< 20,000	No answer	No answer	Diploma	6014
196	Male	25 -29	< 20,000	Engineer	Professionals	Master Degree	6107
197	Male	25 -29	< 20,000	Student	Retired	Master Degree	6009
198	Male	25 -29	< 20,000	Technician	Technicians and Trades Workers	Bachelor Degree	No answer
199	Male	20 - 24	< 20,000	Student	Student	Master Degree	6107
200	Male	25 -29	I prefer not to answer	Student	Student	Master Degree	6052
201	Female	20 - 24	30,001-50,000	Customer Service	Community and Personal Service Workers	Bachelor Degree	6051
202	Male	20 - 24	< 20,000	Customer Service	Community and Personal Service Workers	Bachelor Degree	6051
203	Male	20 - 24	< 20,000	Student	Student	Master Degree	6051

No.	Gender	Age	Income	Actual Occupation	Occupation Types	Education	Postcode
204	Male	20 - 24	< 20,000	Student	Student	Master Degree	6010
205	Female	25 -29	20,001-30,000	Food and beverage attendant	Technicians and Trades Workers	Master Degree	No answer
206	Female	30 - 34	30,001-50,000	No answer	No answer	PhD/Dr.	6150
207	Male	Above 50	50,001-100,000	Lecturer	Professionals	PhD/Dr.	6065
208	Female	20 - 24	< 20,000	Shop Assistant	Sales Workers	Bachelor Degree	6061
209	Male	30 - 34	I prefer not to answer	No answer	No answer	Bachelor Degree	6061

APPENDIX I: Data of respondents' experiences in using online banking

Part 1: Respondents' online banking information

Respondent's ID	B1	B2	B3	B4	B5
1	No	Not applicable	Not applicable	Not applicable	Not applicable
2	No	Not applicable	Not applicable	Not applicable	Not applicable
3	No	Not applicable	Not applicable	Not applicable	Not applicable
4	Yes	Faster service computer operation	Commonwealth bank Bank West National bank Citibank St. George	Citibank St. George	Changed bank(CBS,NBA); insecure bank site (Bank West)
5	Yes	Faster service computer operation Convenience	Westpac	Westpac	Not applicable
6	Yes	Faster service computer operation	Commonwealth bank National bank	National bank	Changing from Commonwealth Bank to NB.
7	Yes	Avoid waiting in a queue 24 hours service.	Westpac	Westpac	Not applicable
8	No	Not applicable	Not applicable	Not applicable	Not applicable
9	Yes	Faster service computer operation Reduce time spent commuting To keep us with modern system.	Westpac	Westpac	Not applicable
10	Yes	Reduce time spent commuting	Westpac	Westpac	Not applicable
11	Yes	Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
12	Yes	Avoid waiting in a queue	Westpac	Westpac	Not applicable
13	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting Avoid physical attack from robbers.	Commonwealth bank ANZ bank	Commonwealth bank ANZ bank	Not applicable
14	Yes	Convenience.	Commonwealth bank Bank West	Commonwealth bank Bank West	Not applicable
15	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank First Interstate Bank	Commonwealth bank	No answer
16	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank HSBC bank	ANZ bank	I closed my account.
17	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable
18	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank	ANZ bank	Not applicable

Respondent's ID	B1	B2	B3	B4	B5
19	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank National bank HSBC bank	ANZ bank	No answer
20	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
21	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank	ANZ bank	Not applicable
22	Yes	Avoid waiting in a queue Reduce time spent commuting	ANZ bank	ANZ bank	Not applicable
23	Yes	Avoid waiting in a queue	Commonwealth bank	Commonwealth bank	Not applicable
24	Yes	Avoid waiting in a queue Reduce time spent commuting Easy to pay bills.	SEB	SEB	Not applicable
25	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
26	Yes	Reduce time spent commuting	Bank West ANZ bank	Bank West ANZ bank	Not applicable
27	Yes	Faster service computer operation Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
28	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank HSBC bank	ANZ bank HSBC bank	Not applicable
29	Yes	Avoid waiting in a queue	Bank West	Bank West	Not applicable
30	Yes	Faster service computer operation Convenience.	Commonwealth bank Bank West	I prefer not to answer	Not applicable
31	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
32	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank National bank	ANZ bank National bank	Not applicable
33	Yes	Uncertain I thought it's more secure.	ANZ bank	ANZ bank	Not applicable
34	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
35	Yes	Faster service computer operation Convenience.	Commonwealth bank ANZ bank	Commonwealth bank ANZ bank	Not applicable
36	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable
37	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank	Not applicable	I've received an e-mail from stranger similar to ANZ e-mail to provide him my personal detail.
38	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank	ANZ bank	Not applicable
39	Yes	Faster service computer operation	Westpac ANZ bank	Westpac ANZ bank	Not applicable

Respondent's ID	B1	B2	B3	B4	B5
40	Yes	Avoid waiting in a queue Reduce time spent commuting	Commonwealth bank Bank West	Commonwealth bank Bank West	Not applicable
41	Yes	Reduce time spent commuting	Westpac	Westpac	Not applicable
42	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank	ANZ bank	Not applicable
43	No	Not applicable	Not applicable	Not applicable	Not applicable
44	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank	ANZ bank	Not applicable
45	Yes	Reduce time spent commuting	Bank West	Bank West	Not applicable
46	Yes	Avoid waiting in a queue Faster service computer operation Convenience.	ANZ bank	ANZ bank	Not applicable
47	Yes	Uncertain Parents opened the account for me when I was younger.	Commonwealth bank	Commonwealth bank	Not applicable
48	Yes	Faster service computer operation Reduce time spent commuting	Bank West	Bank West	Not applicable
49	Yes	Avoid waiting in a queue	Commonwealth bank ANZ bank	Commonwealth bank ANZ bank	Not applicable
50	Yes	Avoid waiting in a queue Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
51	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable
52	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
53	Yes	Avoid waiting in a queue Faster service computer operation	Citibank CIBC	Citibank CIBC	Not applicable
54	Yes	Uncertain I wanted an account that was not linked to a card so that I could save money. And this account offered a higher rate of interest.	Westpac	Westpac	Not applicable
55	Yes	Faster service computer operation	I prefer not to answer	I prefer not to answer	Not applicable
56	Yes	Avoid waiting in a queue Faster service computer operation I can do it at a time to suit me.	Bank West Westpac ANZ bank HSBC bank	ANZ bank HSBC bank	No answer
57	Yes	Uncertain We are living in a rural area, more convenient-can't get to a bank during business hours.	Citibank ANZ bank St. George Bank ME Bank	I prefer not to answer	Closed the accounts-Changed home loans, refinanced for better rate.
58	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank	ANZ bank	Not applicable
59	Yes	Avoid waiting in a queue	Commonwealth bank Bank West Citibank	Commonwealth bank Bank West Citibank	Not applicable

Respondent's ID	B1	B2	B3	B4	B5
60	Yes	Uncertain It is convenient- all of your banking details are clearly displayed and is easy to follow and understand.	Westpac	Westpac	Not applicable
61	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank	ANZ bank	Not applicable
62	Yes	Uncertain More convenient.	Westpac Credit Union.	Westpac Credit Union.	Not applicable
63	Yes	Faster service computer operation	National bank Big Sky Credit Union	National bank Big Sky Credit Union	Not applicable
64	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable
65	Yes	Avoid waiting in a queue Reduce time spent commuting	I prefer not to answer	I prefer not to answer	Not applicable
66	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank ANZ bank	Commonwealth bank ANZ bank	Not applicable
67	Yes	Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West National bank HSBC bank First Direct Barclays Ing Direct	National bank HSBC bank First Direct Barclays Ing Direct	Closed Account
68	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting Convenience.	Bank West	Bank West	Not applicable
69	Yes	Avoid waiting in a queue Reduce time spent commuting	National bank	National bank	Not applicable
70	Yes	Uncertain Bank does not have branches only by machine on Internet.	I prefer not to answer	Commonwealth bank	Not applicable
71	Yes	Uncertain Convenience- doing when I want to do it. i.e. late at night.	Commonwealth bank	Commonwealth bank	Not applicable
72	Yes	Uncertain I can do my banking at a time that's convenient.	ANZ bank Cooperative UK	ANZ bank	No answer
73	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West	Bank West	Changed bank
74	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank Westpac ANZ bank St. George Bank	Westpac ANZ bank St George Bank	No answer
75	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank ANZ bank	Commonwealth bank ANZ bank	Not applicable

Respondent's ID	B1	B2	B3	B4	B5
76	Yes	No answer	Commonwealth bank	Commonwealth bank	Not applicable
77	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank	ANZ bank	Not applicable
78	Yes	Faster service computer operation	I prefer not to answer	I prefer not to answer	Not applicable
79	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Bank West Westpac	Westpac	Moved to a different Bank.
80	Yes	Avoid waiting in a queue	Commonwealth bank Bank West	Commonwealth bank Bank West	Not applicable
81	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting A lot more convenient than physically going to a bank.	Commonwealth bank Westpac	Westpac	No answer
82	Yes	No answer	Bank West ANZ bank	Bank West ANZ bank	Not applicable
83	Yes	Faster service computer operation Reduce time spent commuting	Citibank	No answer	No answer
84	Yes	Easy to use.	Bank West	Bank West	Not applicable
85	Yes	Faster service computer operation	Commonwealth bank ANZ bank	Commonwealth bank	No answer
86	Yes	Avoid waiting in a queue Faster service computer operation	Westpac ANZ bank Citibank	Westpac ANZ bank Citibank	Not applicable
87	No	Not applicable	Not applicable	Not applicable	Not applicable
88	Yes	Avoid waiting in a queue	Westpac	Westpac	Not applicable
89	Yes	Avoid waiting in a queue	ANZ bank	ANZ bank	Not applicable
90	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable
91	Yes	Avoid waiting in a queue	Westpac	Westpac	Not applicable
92	No	Not applicable	Not applicable	Not applicable	Not applicable
93	No	Not applicable	Not applicable	Not applicable	Not applicable
94	No	Not applicable	Not applicable	Not applicable	Not applicable
95	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable
96	Yes	Not applicable	No answer	No answer	Not applicable
97	Yes	Faster service computer operation	No answer	No answer	Not applicable
98	Yes	Avoid waiting in a queue Faster service computer operation	Commonwealth bank ANZ bank National bank Bendigo	Commonwealth bank ANZ bank National bank Bendigo	Not applicable
99	Yes	Convenience	Bank West	Bank West	Not applicable
100	Yes	Reduce time spent commuting	Bendigo Police-Nurses	Bendigo	No answer

Respondent's ID	B1	B2	B3	B4	B5
101	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	United Credit Union Ing Direct	United Credit Union Ing Direct	Not applicable
102	No	Not applicable	Not applicable	Not applicable	Not applicable
103	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West Westpac	Commonwealth bank Bank West Westpac	Not applicable
104	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Bank West ANZ bank St. George	Bank West St. George	No answer
105	Yes	Avoid waiting in a queue Faster service computer operation	Commonwealth bank St. George	Commonwealth bank St. George	Not applicable
106	Yes	Avoid waiting in a queue	Westpac	Westpac	Not applicable
107	No	Not applicable	Not applicable	Not applicable	Not applicable
108	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
109	Yes	Faster service computer operation	ANZ bank National bank	ANZ bank National bank	Not applicable
110	Yes	Avoid waiting in a queue Reduce time spent commuting	Commonwealth bank National bank	National bank	No answer
111	No	Not applicable	Not applicable	Not applicable	Not applicable
112	Yes	Faster service computer operation	ANZ bank National bank	ANZ bank	Not applicable
113	Yes	Reduce time spent commuting	No answer	No answer	Not applicable
114	Yes	Faster service computer operation	Commonwealth bank Bank West	Bank West	Forgot login/password.
115	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
116	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
117	No	Not applicable	Not applicable	Not applicable	Not applicable
118	Yes	Faster service computer operation	I prefer not to answer	Bank West	Not applicable
119	Yes	Faster service computer operation	National bank Macquarie	National bank Macquarie	Not applicable
120	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West	Commonwealth bank Bank West	Not applicable
121	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ME Bank	ME Bank	Not applicable
122	Yes	Faster service computer operation	Commonwealth bank Bank West Westpac ANZ bank	Commonwealth bank ANZ bank National bank	No answer

Respondent's ID	B1	B2	B3	B4	B5
123	No	Not applicable	Not applicable	Not applicable	Not applicable
124	No	Not applicable	Not applicable	Not applicable	Not applicable
125	Yes	Avoid waiting in a queue Reduce time spent commuting	HSBC bank SCB KBANK BBG	HSBC bank SCB KBANK BBG	Not applicable
126	Yes	Uncertain	Commonwealth bank ANZ bank National bank	I prefer not to answer	Not applicable
127	Yes	Avoid waiting in a queue Reduce time spent commuting	ANZ bank	ANZ bank	Not applicable
128	No	Not applicable	Not applicable	Not applicable	Not applicable
129	Yes	Avoid waiting in a queue	Commonwealth bank National bank	Commonwealth bank National bank	Not applicable
130	Yes	Avoid waiting in a queue	Commonwealth bank ANZ bank National bank Macquarie	Commonwealth bank National bank	Not applicable
131	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank Westpac	Commonwealth bank Westpac	Not applicable
132	Yes	Avoid waiting in a queue Faster service computer operation	Bank West ANZ bank	Bank West ANZ bank	No answer
133	Yes	More convenient	Bank West Westpac National bank	Bank West Westpac National bank	Not applicable
134	Yes	Avoid waiting in a queue Faster service computer operation	Bank West ANZ bank National bank	ANZ bank	Closed account and has changed to another bank.
135	Yes	Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West	Commonwealth bank Bank West	Not applicable
136	Yes	Avoid waiting in a queue	Commonwealth bank ANZ bank	ANZ bank	No answer
137	Yes	Avoid waiting in a queue	National bank	National bank	Not applicable
138	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank	ANZ bank	Not applicable
139	Yes	Faster service computer operation	Bank West Westpac	Bank West Westpac	Not applicable
140	Yes	No answer	No answer	No answer	Not applicable
141	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank HSBC bank DBS	ANZ bank HSBC bank DBS	Not applicable
142	No	Not applicable	Not applicable	Not applicable	Not applicable
143	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable

Respondent's ID	B1	B2	B3	B4	B5
144	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West	Bank West	Has transferred to main account.
145	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable
146	No	Not applicable	Not applicable	Not applicable	Not applicable
147	Yes	Avoid waiting in a queue Ad-hoc convenience	Westpac National bank	Westpac National bank	Not applicable
148	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Westpac	I prefer not to answer	Not applicable
149	Yes	Faster service computer operation Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
150	No	Not applicable	Not applicable	Not applicable	Not applicable
151	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank	I prefer not to answer	Not applicable
152	Yes	Avoid waiting in a queue Reduce time spent commuting	ANZ bank	ANZ bank	Not applicable
153	Yes	Avoid waiting in a queue	Westpac	Westpac	Not applicable
154	Yes	Faster service computer operation	Westpac ANZ bank	ANZ bank	No longer have an account with that.
155	Yes	Faster service computer operation Convenience	Westpac	Westpac	Not applicable
156	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
157	Yes	Avoid waiting in a queue	Other, please specify	No answer	Not applicable
158	Yes	Avoid waiting in a queue	Westpac	Westpac	Not applicable
159	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting Flexibility of managing my account.	Commonwealth bank Westpac ANZ bank	Commonwealth bank Westpac ANZ bank	Not applicable
160	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West Macquarie	Commonwealth bank Bank West Macquarie	Not applicable
161	Yes	Avoid waiting in a queue	Bank West Westpac St. George	Bank West Westpac St. George	Not applicable
162	No	Not applicable	Not applicable	Not applicable	Not applicable
163	Yes	Faster service computer operation	Commonwealth bank	No answer	Not Trust
164	Yes	Faster service computer operation	Bank West Westpac ANZ bank	No answer	No answer
165	No	Not applicable	Not applicable	Not applicable	Not applicable
166	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
167	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
168	No	Not applicable	Not applicable	Not applicable	Not applicable

Respondent's ID	B1	B2	B3	B4	B5
169	Yes	Avoid waiting in a queue Reduce time spent commuting	Bank West Westpac	Westpac	No answer
170	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
171	Yes	Faster service computer operation	ANZ bank Bank of Queensland	ANZ bank Bank of Queensland	Not applicable
172	Yes	Reduce time spent commuting	Commonwealth bank Bank West National bank Citibank	ANZ bank National bank	Changed bank
173	Yes	Avoid waiting in a queue	Commonwealth bank ANZ bank	Commonwealth bank ANZ bank	Not applicable
174	No	Not applicable	Not applicable	Not applicable	Not applicable
175	Yes	Reduce time spent commuting Prices are more faire.	Commonwealth bank	Commonwealth bank	Not applicable
176	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Police and Nurses Credit Society	Police and Nurses Credit Society	Not applicable
177	No	Not applicable	Not applicable	Not applicable	Not applicable
178	Yes	Avoid waiting in a queue	ANZ bank	ANZ bank National bank	Not applicable
179	Yes	Faster service computer operation	I prefer not to answer National bank	National bank	Not applicable
180	Yes	Faster service computer operation Reduce time spent commuting	Westpac	Westpac National bank	Not applicable
181	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank	National bank	Not applicable
182	Yes	Faster service computer operation Reduce time spent commuting	Westpac	Westpac National bank	Not applicable
183	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Bank West Westpac ANZ bank	Bank West Westpac	No answer
184	Yes	Certain goods are only available on the net.	Westpac	Westpac	Not applicable
185	Yes	Reduce time spent commuting	Bank West	Bank West	Not applicable
186	Yes	Faster service computer operation Reduce time spent commuting	ANZ bank	ANZ bank	Not applicable
187	Yes	Avoid waiting in a queue	Bank West	Bank West	Not applicable
188	Yes	Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable
189	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank ANZ bank	Commonwealth bank	Not applicable
190	Yes	Faster service computer operation	National bank	National bank	Not applicable
191	Yes	Avoid waiting in a queue Faster service computer operation	Commonwealth bank	Commonwealth bank	Not applicable

Respondent's ID	B1	B2	B3	B4	B5
192	Yes	Faster service computer operation Reduce time spent commuting	Westpac	Westpac	Not applicable
193	Yes	Avoid waiting in a queue Faster service computer operation	Commonwealth bank ANZ bank	Commonwealth bank ANZ bank	Not applicable
194	Yes	Avoid waiting in a queue Faster service computer operation	ANZ bank	ANZ bank	Not applicable
195	Yes	Avoid waiting in a queue	No answer	No answer	Not applicable
196	Yes	Uncertain	Westpac	Westpac	Not applicable
197	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
198	Yes	Reduce time spent commuting	No answer	No answer	Not applicable
199	Yes	Faster service computer operation Reduce time spent commuting	Commonwealth bank ANZ bank	ANZ bank	No answer
200	Yes	Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West ANZ bank	Commonwealth bank Bank West	I have money these account.
201	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank National bank	ANZ bank National bank	Not applicable
202	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	ANZ bank National bank	ANZ bank National bank	Not applicable
203	Yes	Faster service computer operation	Westpac	Westpac	Not applicable
204	Yes	Faster service computer operation	Bank West ANZ bank	Bank West ANZ bank	Not applicable
205	Yes	Faster service computer operation	ANZ bank	ANZ bank	Not applicable
206	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank Bank West ANZ bank	Commonwealth bank ANZ bank	Because I have lost my money for 3,000$ from online banking.
207	Yes	Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
208	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank	Commonwealth bank	Not applicable
209	Yes	Avoid waiting in a queue Faster service computer operation Reduce time spent commuting	Commonwealth bank GE Money ING Direct	Commonwealth bank GE Money ING Direct	Not applicable

Part 2: Respondents' behaviours when using online banking services

Respondent's ID	B6	B7	B8	B9	B10
1	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. I do not have an online banking account. I am concerned about security.
2	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. I am concerned about security.
3	Not Applicable	Not applicable	Not applicable	Not applicable	I am concerned about security.
4	More than 20 times	Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank	My house My workplace via mobile phone/palmtop	Not applicable
5	3 - 5 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
6	1 or 2 times	Pay bill(s) Viewing balance and summary information	Best lending rate.	My house	Not applicable
7	3 - 5 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My workplace	Not applicable
8	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. I do not know how to use online banking. I do not have an online banking account. I am concerned about security.
9	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace via mobile phone/palmtop	Not applicable
10	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
11	1 or 2 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
12	More than 20 times	Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
13	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information Buy mortgage.	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
14	More than 20 times	Money transfer Pay bill(s) Viewing balance and summary information	It was my first employer.	My house My workplace	Not applicable
15	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My house	Not applicable
16	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	Recommendation	My house	Not applicable
17	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
18	11 - 20 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	Friend's recommended.	My house	Not applicable
19	11 - 20 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank There are branch banks in my home country.	My house My workplace	Not applicable
20	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	My sponsorship sends money to this bank.	My house School/ university/ college	Not applicable
21	1 or 2 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The brand name of the bank The excellent service offered by this bank The security protection offered by bank for online banking	My house School/ university/ college	Not applicable
22	1 or 2 times	Pay bill(s)	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
23	6 - 10 times	Viewing balance and summary information	The brand name of the bank	My house School/ university/ college	Not applicable
24	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The excellent service offered by this bank The security protection offered by bank for online banking	My house My friend's house Internet cafe My workplace	Not applicable
25	1 or 2 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
26	3 - 5 times	Money transfer Viewing balance and summary information	The brand name of the bank High interest rate.	My house	Not applicable
27	1 or 2 times	Money transfer Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
28	6 - 10 times	Pay bill(s) Viewing balance and summary information	I needed to access my accounts, which are in the different countries, but at the same bank.	My house	Not applicable
29	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
30	More than 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
31	3 - 5 times	Money transfer Viewing balance and summary information	The excellent service offered by this bank	My house	Not applicable
32	3 - 5 times	Money transfer	I have (had) a traditional bank account with the same bank	My house via mobile phone/palmtop	Not applicable
33	6 - 10 times	Money transfer	I have (had) a traditional bank account with the same bank The brand name of the bank	My house	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
34	1 or 2 times	Money transfer	The excellent service offered by this bank	School/ university/ college via mobile phone/palmtop	Not applicable
35	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
36	3 - 5 times	Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank	My house My friend's house	Not applicable
37	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	Have many ATMs available.	My house	Not applicable
38	1 or 2 times	Pay bill(s)	The excellent service offered by this bank	My house	Not applicable
39	3 - 5 times	Money transfer	The excellent service offered by this bank	My house	Not applicable
40	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The excellent service offered by this bank	My house	Not applicable
41	1 or 2 times	Money transfer	I have (had) a traditional bank account with the same bank	My house My friend's house	Not applicable
42	3 - 5 times	Money transfer Viewing balance and summary information	The brand name of the bank	No answer	Not applicable
43	Not Applicable	Not applicable	Not applicable	Not applicable	I do not have an online banking account. I am concerned about security.
44	More than 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house School/ university/ college	Not applicable
45	3 - 5 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
46	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable
47	6 - 10 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank Parents use it.	My house	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
48	3 - 5 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable
49	No answer	No answer	No answer	No answer	Not applicable
50	6 - 10 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	School/ university/ college	Not applicable
51	11 - 20 times	Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
52	6 - 10 times	Money transfer	I have (had) a traditional bank account with the same bank	My house School/ university/ college via mobile phone/palmtop	Not applicable
53	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
54	6 - 10 times	Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My house	Not applicable
55	1 or 2 times	Update personal information Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank	My house via mobile phone/palmtop	Not applicable
56	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
57	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	Had set up home loan & general accounts at the same time.	My house My workplace	Not applicable
58	1 or 2 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
59	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house My workplace	Not applicable
60	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
61	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace via mobile phone/palmtop	Not applicable
62	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable
63	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable
64	1 or 2 times	Money transfer Viewing balance and summary information	The brand name of the bank	My friend's house	Not applicable
65	No answer	No answer	The security protection offered by bank for online banking	My house	Not applicable
66	1 or 2 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank Friend Recommended.	My house	Not applicable
67	6 - 10 times	Money transfer Viewing balance and summary information	The excellent service offered by this bank	My house My workplace	Not applicable
68	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace via mobile phone/palmtop	Not applicable
69	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	School/ university/ college My workplace	Not applicable
70	More than 20 times	Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My house	Not applicable
71	1 or 2 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
72	3 - 5 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
73	6 - 10 times	Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The brand name of the bank	My house	Not applicable
74	More than 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
75	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My house	Not applicable
76	6 - 10 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house School/ university/ college	Not applicable
77	3 - 5 times	Money transfer Viewing balance and summary information	The brand name of the bank The excellent service offered by this bank	My house School/ university/ college	Not applicable
78	3 - 5 times	Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The security protection offered by bank for online banking	My house My workplace	Not applicable
79	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	My mortgage is with this bank.	My house My workplace	Not applicable
80	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank Convenience and bank special interest rates.	My house School/ university/ college My friend's house My workplace	Not applicable
81	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information Online Investing	I have (had) a traditional bank account with the same bank	My workplace	Not applicable
82	3 - 5 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace via mobile phone/palmtop	Not applicable
83	1 or 2 times	Viewing balance and summary information	The brand name of the bank	My house My workplace	Not applicable
84	More than 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
85	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My friend's house My workplace	Not applicable
86	More than 20 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My house	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
87	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. I do not have an online banking account. I do not see any real value in using online banking or having an online banking account.
88	1 or 2 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
89	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The brand name of the bank	My house	Not applicable
90	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
91	More than 20 times	Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
92	Not Applicable	Not applicable	Not applicable	Not applicable	I do not know how to use computer. I do not have an online banking account.
93	Not Applicable	Not applicable	Not applicable	Not applicable	I am concerned about security. I have not had time to open an account.
94	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. I am concerned about security.
95	3 - 5 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
96	No answer	Not applicable	No answer	No answer	Not applicable
97	More than 20 times	Update personal information Pay bill(s)	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
98	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The excellent service offered by this bank	My house Public library via mobile phone/palmtop	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
99	11 - 20 times	Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
100	3 - 5 times	Money transfer Viewing balance and summary information	No answer	No answer	Not applicable
101	3 - 5 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
102	Not Applicable	Not applicable	Not applicable	Not applicable	No answer
103	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My workplace	Not applicable
104	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace via mobile phone/palmtop	Not applicable
105	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
106	1 or 2 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
107	Not Applicable	Not applicable	Not applicable	Not applicable	No answer
108	6 - 10 times	Money transfer Viewing balance and summary information	No answer	My house	Not applicable
109	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information Share trading	I have (had) a traditional bank account with the same bank The security protection offered by bank for online banking	My house My workplace	Not applicable
110	1 or 2 times	Money transfer Pay bill(s)	The excellent service offered by this bank I have (had) a traditional bank account with the same bank The security protection offered by bank for online banking	No answer	I do not see any real value in using online banking or having an online banking account.
111	Not Applicable	Not applicable	Not applicable	Not applicable	No answer
112	6 - 10 times	Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My house My workplace	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
113	1 or 2 times	Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
114	3 - 5 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable
115	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
116	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house via mobile phone/palmtop	Not applicable
117	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking.
118	3 - 5 times	Pay bill(s)	I have (had) a traditional bank account with the same bank	My workplace	Not applicable
119	3 - 5 times	Money transfer	Don't really care.	My house My workplace	Not applicable
120	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	Best interest on money and loan.	My house	Not applicable
121	6 - 10 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The excellent service offered by this bank The security protection offered by bank for online banking	My house My workplace	Not applicable
122	1 or 2 times	Money transfer Pay bill(s)	The excellent service offered by this bank	My house	Not applicable
123	Not Applicable	Not applicable	Not applicable	Not applicable	I do not know how to use online banking. I do not have an Internet connection. I am concerned about security.
124	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. My husband does so I don't need to.
125	3 - 5 times	Money transfer Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house My workplace	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
126	1 or 2 times	Pay bill(s)	The security protection offered by bank for online banking	My house	Not applicable
127	3 - 5 times	Update personal information Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
128	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. I am concerned about security. It is too new. I would like to see how it works, and then I may open an account.
129	1 or 2 times	Money transfer	I have (had) a traditional bank account with the same bank	My house	Not applicable
130	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
131	6 - 10 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
132	6 - 10 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	The security protection offered by bank for online banking	My house Public library	Not applicable
133	More than 20 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The security protection offered by bank for online banking	My house My workplace	Not applicable
134	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
135	3 - 5 times	Pay bill(s) Viewing balance and summary information	The brand name of the bank The excellent service offered by this bank	My house	Not applicable
136	3 - 5 times	Pay bill(s) Viewing balance and summary information	The brand name of the bank	My house	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
137	6 - 10 times	Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank	My workplace	Not applicable
138	1 or 2 times	Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
139	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
140	No answer	No answer	No answer	No answer	Not applicable
141	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
142	Not Applicable	Not applicable	Not applicable	Not applicable	I do not have an online banking account.
143	1 or 2 times	Viewing balance and summary information	The excellent service offered by this bank	My house	Not applicable
144	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
145	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	The brand name of the bank	My house School/ university/ college My workplace	Not applicable
146	Not Applicable	Not applicable	Not applicable	Not applicable	I am concerned about security.
147	3 - 5 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
148	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
149	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable
150	Not Applicable	Not applicable	Not applicable	Not applicable	I do not know how to use Internet. I am concerned about security.

Respondent's ID	B6	B7	B8	B9	B10
151	1 or 2 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank The security protection offered by bank for online banking	My house	Not applicable
152	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable
153	1 or 2 times	Money transfer	I have (had) a traditional bank account with the same bank	My house	Not applicable
154	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house via mobile phone/palmtop	Not applicable
155	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	The security protection offered by bank for online banking	My house	Not applicable
156	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
157	3 - 5 times	Viewing balance and summary information	I have (had) a traditional bank account with the same bank	Internet cafe	Not applicable
158	More than 20 times	Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
159	6 - 10 times	Viewing balance and summary information Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank Business banking benefits.	My house My workplace via mobile phone/palmtop	Not applicable
160	1 or 2 times	Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
161	11 - 20 times	Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank Ease of use and feature offered	My house My workplace	Not applicable
162	Not Applicable	Not applicable	Not applicable	Not applicable	No answer
163	1 or 2 times	Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
164	11 - 20 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
165	Not Applicable	Not applicable	Not applicable	Not applicable	I do not see any real value in using online banking or having an online banking account.
166	11 - 20 times	Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My workplace	Not applicable
167	1 or 2 times	Money transfer Pay bill(s)	The excellent service offered by this bank	My house Internet cafe	Not applicable
168	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. I am concerned about security.
169	11 - 20 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house School/ university/ college Internet cafe My workplace via mobile phone/palmtop	Not applicable
170	6 - 10 times	Viewing balance and summary information	The excellent service offered by this bank	My house	Not applicable
171	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	The brand name of the bank The security protection offered by bank for online banking	My house My workplace	Not applicable
172	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	Once provided to personal bankers-This has now changed.	My house via mobile phone/palmtop	Not applicable
173	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	The brand name of the bank	My house	Not applicable
174	Not Applicable	Not applicable	Not applicable	Not applicable	I am not interested in online banking. I am concerned about security.
175	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	The security protection offered by bank for online banking	My house My workplace	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
176	1 or 2 times	Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
177	Not Applicable	Not applicable	Not applicable	Not applicable	I am concerned about security. I do not see any real value in using online banking or having an online banking account.
178	6 - 10 times	Money transfer Pay bill(s)	The brand name of the bank	My house	Not applicable
179	3 - 5 times	Money transfer	I have (had) a traditional bank account with the same bank	My house	Not applicable
180	6 - 10 times	Viewing balance and summary information	Relative said it was easy to open a bank account.	My house	Not applicable
181	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The brand name of the bank	My house	Not applicable
182	6 - 10 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The security protection offered by bank for online banking	My house School/ university/ college My workplace via mobile phone/palmtop	Not applicable
183	More than 20 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
184	6 - 10 times	Viewing balance and summary information	Easy to open a bank account over the web.	My house	Not applicable
185	1 or 2 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house School/ university/ college	Not applicable
186	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
187	3 - 5 times	Money transfer	The excellent service offered by this bank	My house	Not applicable
188	1 or 2 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house School/ university/ college	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
189	11 - 20 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The excellent service offered by this bank	My house School/ university/ college My workplace via mobile phone/palmtop	Not applicable
190	3 - 5 times	Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
191	3 - 5 times	Pay bill(s)	The security protection offered by bank for online banking	My house	Not applicable
192	6 - 10 times	Update personal information Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house Public library	Not applicable
193	More than 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The brand name of the bank	My house In the bank.	Not applicable
194	1 or 2 times	Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
195	No answer	Money transfer	I have (had) a traditional bank account with the same bank	School/ university/ college	Not applicable
196	6 - 10 times	Money transfer Viewing balance and summary information	I have (had) a traditional bank account with the same bank The brand name of the bank	My house	Not applicable
197	3 - 5 times	Money transfer Pay bill(s)	I have (had) a traditional bank account with the same bank	My house	Not applicable
198	3 - 5 times	Check the bill	The security protection offered by bank for online banking	My house	Not applicable
199	11 - 20 times	Money transfer	I have (had) a traditional bank account with the same bank	My house My workplace	Not applicable
200	3 - 5 times	Money transfer	I have (had) a traditional bank account with the same bank	My house	Not applicable
201	11 - 20 times	Update personal information Money transfer Pay bill(s) Viewing balance and summary information	The excellent service offered by this bank	My house via mobile phone/palmtop	Not applicable

Respondent's ID	B6	B7	B8	B9	B10
202	11 - 20 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house	Not applicable
203	1 or 2 times	Money transfer	I have (had) a traditional bank account with the same bank	My house	Not applicable
204	3 - 5 times	Update personal information	The brand name of the bank The excellent service offered by this bank	My house School/ university/ college	Not applicable
205	6 - 10 times	Money transfer Pay bill(s)	The brand name of the bank	My house	Not applicable
206	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	The brand name of the bank The excellent service offered by this bank	My house	Not applicable
207	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The brand name of the bank The excellent service offered by this bank The security protection offered by bank for online banking	My house	Not applicable
208	3 - 5 times	Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank The brand name of the bank	My house	Not applicable
209	3 - 5 times	Money transfer Pay bill(s) Viewing balance and summary information	I have (had) a traditional bank account with the same bank	My house via mobile phone/palmtop	Not applicable

APPENDIX J: Data of respondents' experiences in relation to online banking security

Part 1: Respondents' devices information

Respondent's ID	C1.1	C2	C3	C4	C5
1	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
2	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
3	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
4	ADSL wired broadband	Windows XP Windows 7	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
5	ADSL wireless broadband	Windows XP	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	I am not sure	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
6	I am not sure what type of Internet connection I use	Windows 7	Yes, I have installed firewall application. Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	I am not sure	I am not sure.
7	Coaxial Cable	Windows Vista	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	Auto update	I am not sure.
8	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
9	ADSL wired broadband	Windows 98 Windows Vista	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
10	ADSL wireless broadband	Windows XP	Yes, I have installed popup windows blocking tool.	My partner checks our internet security.	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
11	ADSL wireless broadband	Macintosh	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Every 3 months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
12	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
13	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Every 4-6months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
14	Dial-up modem	Windows Vista	Managed by my employer	Done automatically by my employer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
15	ADSL wired broadband	Windows Vista Linux	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
16	Coaxial Cable	Windows XP	Yes, I have installed anti-virus software.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
17	ADSL wired broadband	Windows 7	No, I do not use computer security software protection (go to question C5).	No answer	I am not sure.
18	ADSL wired broadband	Windows Vista	Yes, I have installed anti-virus software. Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	I do not need to update	I am not sure.
19	ADSL wired broadband	Windows Vista Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
20	I am not sure what type of Internet connection I use	Windows XP	Yes, I have installed anti-virus software.	Once a day	I am not sure.
21	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	I am not sure.
22	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Auto update	Not applicable

Respondent's ID	C1.1	C2	C3	C4	C5
23	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Once a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
24	ADSL wireless broadband	Windows Vista	No, I do not use computer security software protection (go to question C5).	Don't have computer security software protection .	I am not sure.
25	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
26	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
27	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software.	Once a month	Bank provides software that operates and residents on PC and connects to the bank.
28	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
29	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
30	ADSL wired broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
31	ADSL wired broadband	Windows 7	Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
32	ADSL wired broadband	Windows Vista Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Once a week	Bank provides software that operates and residents on PC and connects to the bank.
33	ADSL wireless broadband	Windows XP	I am not sure whether I have security protection or not (go to question C5).	No answer	I am not sure.

Respondent's ID	C1.1	C2	C3	C4	C5
34	ADSL wired broadband	Windows Vista Macintosh	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
35	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
36	ADSL wired broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day	I am not sure.
37	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day	Bank provides software that operates and residents on PC and connects to the bank.
38	I am not sure what type of Internet connection I use	Windows Vista	Yes, I have installed anti-virus software.	Once a week	Bank provides software that operates and residents on PC and connects to the bank.
39	ADSL wired broadband	Windows 7	Yes, I have installed anti-virus software.	Every 3 months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
40	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
41	I am not sure what type of Internet connection I use	Windows Vista	No, I do not use computer security software protection (go to question C5).	No answer	I am not sure.
42	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Twice a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
43	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
44	ADSL wired broadband	Windows XP Windows Vista Windows 7	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
45	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software.	Once a day	I am not sure.
46	ADSL wired broadband	Windows XP Windows 7	Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
47	I am not sure what type of Internet connection I use	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Every 2 weeks	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
48	ADSL wired broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update Completed by IT central at university -updated regularly.	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
49	ADSL wired broadband	No answer	No answer	No answer	No answer
50	I am not sure what type of Internet connection I use	I am not sure what operating system I use	I am not sure whether I have security protection or not (go to question C5).	No answer	I am not sure.

Respondent's ID	C1.1	C2	C3	C4	C5
51	No answer	Windows 7	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
52	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Once a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
53	ADSL wireless broadband	Macintosh	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Once a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
54	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	I have an IT consultant that looks after my computer security at home. He looks after the updates too.	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
55	ADSL wired broadband	Windows Vista Windows 7 Banking Sim Card	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
56	ADSL wireless broadband	Windows 7	Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
57	ADSL wired broadband	Windows XP Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool. Mail server protection, spam assas in & phulk brute force attack protection on my Linux mail server.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
58	I am not sure what type of Internet connection I use	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
59	ADSL wireless broadband	Windows XP Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	2 yearly subscription	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
60	ADSL wired broadband	Windows 2000	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
61	ADSL wired broadband	Windows XP	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
62	ADSL wired broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
63	ADSL wireless broadband	Windows 2000	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	Company Installed and updated	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
64	ADSL wired broadband	Windows 98	Yes, I have installed anti-virus software.	Once a week	I am not sure.
65	ADSL wireless broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	I am not sure	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
66	ADSL wireless broadband	Windows Vista Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Other, please specify
67	ADSL wired broadband	Linux Macintosh	Little Snitem (MAC OS)	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
68	ADSL wired broadband	Windows XP Windows 7 Linux	No, I do not use computer security software protection (go to question C5).	No answer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
69	No answer	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Every 3 months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
70	ADSL wired broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
71	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Once a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
72	Coaxial Cable	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
73	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
74	ADSL wireless broadband	Windows 2000 Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
75	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Every 4-6months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
76	ADSL wireless broadband	Windows XP Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
77	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
78	ISDN broadband	Windows XP	Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
79	ADSL wired broadband	Windows Vista	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
80	ADSL wireless broadband	Windows XP Windows Vista Windows 7	Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	No answer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
81	ADSL wired broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	I am not sure	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
82	ADSL wired broadband	Windows 7 Macintosh	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
83	ADSL wireless broadband	Windows Vista	I am not sure whether I have security protection or not (go to question C5).	Auto update	I am not sure.
84	ADSL wired broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
85	ADSL wired broadband	Windows 98 Windows XP	Yes, I have installed anti-virus software.	I am not sure	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
86	ADSL wired broadband	Windows Vista Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
87	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
88	ADSL wireless broadband	Windows 2000	Yes, I have installed firewall application. Yes, I have installed popup windows blocking tool.	Twice a week Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
89	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software.	Every 4-6months	I am not sure.
90	I am not sure what type of Internet connection I use	I am not sure what operating system I use	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
91	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application.	Twice a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
92	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
93	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
94	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
95	No answer	No answer	No answer	No answer	No answer
96	No answer	No answer	No answer	Every 4-6months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
97	ADSL wired broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Once a week	Bank provides software that operates and residents on PC and connects to the bank.
98	ADSL wireless broadband	Windows Vista Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Once a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
99	Not applicable	Windows Vista	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
100	No answer	No answer	No answer	I do not need to update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
101	No answer	No answer	No answer	I am not sure	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
102	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
103	I am not sure what type of Internet connection I use	Windows 7	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	I am not sure	I am not sure.
104	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
105	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
106	No answer	No answer	No answer	No answer	No answer
107	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
108	ADSL wireless broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	I am not sure.
109	ADSL wired broadband	Windows 98 Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
110	ADSL wired broadband	Windows 7 Windows Mobile	I am not sure whether I have security protection or not (go to question C5).	No answer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
111	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
112	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
113	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
114	ADSL wired broadband	Windows XP	Yes, I have installed anti-virus software.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
115	ADSL wireless broadband	Windows 7	Yes, I have installed anti-virus software.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
116	ADSL wired broadband	Windows XP Macintosh	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day	No answer
117	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
118	ADSL wireless broadband	Macintosh	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	Once a week	I am not sure.
119	ADSL wireless broadband	Windows XP	Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Once a week	I am not sure.
120	No answer	No answer	No answer	No answer	No answer
121	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application.	Every 4-6months	I am not sure.
122	ADSL wired broadband	Windows Vista	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
123	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable

Respondent's ID	C1.1	C2	C3	C4	C5
124	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
125	ADSL wireless broadband	Windows XP Macintosh	Yes, I have installed anti-virus software.	Every 4-6months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
126	I am not sure what type of Internet connection I use	Windows 98	Yes, I have installed anti-virus software.	Once a month	Bank provides software that operates and residents on PC and connects to the bank.
127	ADSL wired broadband	Windows Vista	Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
128	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
129	No answer	Windows XP	Yes, I have installed anti-virus software.	Every 4-6months	I am not sure.
130	No answer	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Other, please specify	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
131	ADSL wireless broadband	I am not sure what operating system I use	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	I am not sure	I am not sure.
132	ADSL wired broadband	Windows XP	Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	I am not sure	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
133	ADSL wireless broadband	I am not sure what operating system I use	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
134	ADSL wireless broadband	Windows Vista Windows 7	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
135	ADSL wireless broadband	Macintosh	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
136	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
137	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application.	Every 4-6months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
138	ADSL wireless broadband	Windows 7	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
139	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
140	No answer	No answer	No answer	No answer	No answer
141	ADSL wired broadband	Windows XP Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
142	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
143	I am not sure what type of Internet connection I use	Windows XP	No, I do no t use computer security software protection (go to question C5).	No answer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
144	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Every 3 months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
145	ADSL wired broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Twice a week	I am not sure.
146	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
147	ADSL wireless broadband	Windows XP Windows 7	Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
148	ADSL wireless broadband	Windows 7	I am not sure whether I have security protection or not (go to question C5).	No answer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
149	ADSL wireless broadband	No answer	No answer	No answer	No answer
150	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
151	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day Auto update	I am not sure.
152	I am not sure what type of Internet connection I use	Windows XP Windows 7	Yes, I have installed anti-virus software.	Every 4-6months	I am not sure.
153	ADSL wireless broadband	I am not sure what operating system I use	No answer	No answer	No answer
154	ADSL wired broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
155	I am not sure what type of Internet connection I use	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	I am not sure	I am not sure.
156	ADSL wireless broadband	Windows 98	Yes, I have installed anti-virus software.	Every 4-6months	Bank provides software that operates and residents on PC and connects to the bank.
157	Other, please specify	Windows XP Windows 7	No, I do not use computer security software protection (go to question C5).	No answer	Bank provides software that operates and residents on PC and connects to the bank.

Respondent's ID	C1.1	C2	C3	C4	C5
158	ADSL wired broadband	Windows 2000	I am not sure whether I have security protection or not (go to question C5).	No answer	I am not sure.
159	ADSL wired broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
160	ADSL wired broadband	Macintosh	No, I do not use computer security software protection (go to question C5).	No answer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
161	Coaxial Cable	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
162	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
163	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application.	Every 4-6months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
164	ADSL wired broadband	Windows XP Windows Vista	No, I do not use computer security software protection (go to question C5).	No answer	I am not sure.
165	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
166	ADSL wireless broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Once a day Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
167	ADSL wired broadband	Windows 98 Windows 2000	Yes, I have installed firewall application.	Once a week	Bank provides a software that operates and resident on PC and coonect the the bank.
168	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
169	ADSL wired broadband	Windows XP Windows Vista Windows Mobile	No, I do not use computer security software protection (go to question C5).	No answer	Other, please specify

Respondent's ID	C1.1	C2	C3	C4	C5
170	ISDN broadband	Windows Vista	Yes, I have installed anti-virus software.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
171	No answer	No answer	No answer	No answer	No answer
172	ADSL wired broadband	Windows XP Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Every 4-6months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
173	ADSL wireless broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Once a week	I am not sure.
174	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
175	ADSL wired broadband	Windows 7	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
176	ADSL wired broadband	Windows XP I am not sure what operating system I use	Yes, I have installed firewall application.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
177	Not applicable	Not applicable	Not Applicable	Not applicable	Not applicable
178	ADSL wired broadband	Windows XP	Yes, I have installed firewall application.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
179	ADSL wireless broadband	Macintosh	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	Once a week	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
180	ADSL wireless broadband	Windows XP Windows Vista Windows 7 Linux	Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
181	I am not sure what type of Internet connection I use	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Every 4-6months	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
182	ADSL wired broadband	Windows Vista	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	Twice a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
183	ADSL wired broadband	Windows XP Windows Vista Windows 7	Yes, I have installed anti-virus software.	Once a week	Bank provides software that operates and residents on PC and connects to the bank.
184	ADSL wireless broadband	Windows XP Windows 7 Linux	Yes, I have installed firewall application. Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
185	ADSL wired broadband	Windows Vista	Yes, I have installed anti-virus software.	Once a week	I am not sure.
186	ADSL wireless broadband	Macintosh	Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
187	ADSL wired broadband	Windows XP	Yes, I have installed anti-virus software.	Once a day	Bank provides software that operates and residents on PC and connects to the bank.
188	ADSL wireless broadband	Windows 7	Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
189	ADSL wired broadband	Windows Vista Windows 7	Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Twice a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
190	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software. Yes, I have installed popup windows blocking tool.	I am not sure	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
191	ADSL wired broadband	Windows XP	Yes, I have installed anti-virus software.	Once a week	I am not sure.
192	Other, please specify	Windows XP	Yes, I have installed anti-virus software.	I am not sure	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Respondent's ID	C1.1	C2	C3	C4	C5
193	ADSL wired broadband	Windows 7	Yes, I have installed firewall application.	Auto update	Bank provides software that operates and residents on PC and connects to the bank.
194	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Once a day	Bank provides software that operates and residents on PC and connects to the bank.
195	ADSL wired broadband	Windows 2000	Yes, I have installed security protection, but I am not sure what type of security protection I have in my computer.	No answer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
196	ADSL wired broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
197	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software. Yes, I have installed anti-spyware/ adware/ Trojan/ backdoor.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
198	ADSL wired broadband	Windows XP	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
199	ADSL wireless broadband	Windows Vista Macintosh	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	I am not sure	I am not sure.
200	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application.	Every 3 months	I am not sure.
201	ADSL wireless broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	Twice a week	Bank provides software that operates and residents on PC and connects to the bank.
202	ADSL wired broadband	Windows 7	No answer	Once a day	Bank provides software that operates and residents on PC and connects to the bank.
203	ADSL wireless broadband	Windows 7	Yes, I have installed firewall application. Yes, I have installed anti-virus software.	I am not sure	I am not sure.
204	ADSL wireless broadband	Windows 7	Yes, I have installed firewall application.	Once a day	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
205	ADSL wireless broadband	Windows XP	Yes, I have installed firewall application.	Once a day	I am not sure.

Respondent's ID	C1.1	C2	C3	C4	C5
206	ADSL wireless broadband	Windows XP	Yes, I have installed anti-virus software.	Once a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
207	ADSL wireless broadband	Windows Vista	Yes, I have installed anti-virus software.	Once a month	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
208	ADSL wired broadband	Macintosh	I am not sure whether I have security protection or not (go to question C5).	No answer	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.
209	ADSL wired broadband	Macintosh	Yes, I have installed firewall application. Yes, I have installed popup windows blocking tool.	Auto update	Web browser, but the actual banking resides on the bank's server in the form of bank's home page.

Part 2: Respondents' authentication security provided

Respondent's ID	C6	C7	C8	C9	C10
1	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
3	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
4	Login + password + mobile (SMS) verification code Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank.	8	No	Not applicable	Call number provided on 'contact us' page
5	Login + password + mobile (SMS) verification code	6	No	Not applicable	Call number provided on 'contact us' page
6	Login + password Login + password + mobile (SMS) verification code	8	Yes	No	Call number provided on 'contact us' page
7	Login + password + token device	I prefer not to answer	No	Not applicable	I do not report
8	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
9	Login + password	I prefer not to answer	Yes	Yes	Call number provided on 'contact us' page
10	Login + password Login + password + mobile (SMS) verification code	4 and 2	No	Not applicable	Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
11	Login + password + mobile (SMS) verification code	10	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
12	Login + password	No answer	No	Not applicable	Call number provided on 'contact us' page
13	Login + password Login + password + mobile (SMS) verification code	10	No	Not applicable	Report via e-mail provided Report via the report form on web page Call number provided on 'contact us' page
14	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
15	Login + password + mobile (SMS) verification code	8	Yes	No	Report via e-mail provided Report via the report form on web page Call number provided on 'contact us' page
16	Login + password	8	Yes	Yes	Call number provided on 'contact us' page
17	Login + password	8	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
18	Login + password + token device	I prefer not to answer	Yes	Yes	Call number provided on 'contact us' page Direct inform by walking into the branch office
19	Login + password Login + password + mobile (SMS) verification code Login + password + random verification code	4 and 6	No	Not applicable	Direct call to the bank I known, not just use 'contact us' page.
20	Login + password	9	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
21	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office

Respondent's ID	C6	C7	C8	C9	C10
22	Login + password Login + password + random verification code	10	Yes	Yes	Call number provided on 'contact us' page
23	Login + password + mobile (SMS) verification code	10	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
24	Login + password + token device	8	No	Not applicable	Report via e-mail provided Report via the report form on web page Call number provided on 'contact us' page Direct inform by walking into the branch office
25	Login + password + random verification code	4	No	Not applicable	Report via the report form on web page Call number provided on 'contact us' page Direct inform by walking into the branch office
26	Login + password	8	No	Not applicable	Report via e-mail provided Call number provided on 'contact us' page Direct inform by walking into the branch office
27	Login + password + security questions (e.g. what is your mother's maiden name?)	4	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
28	Login + password Login + password + token device	8	No	Not applicable	Direct inform by walking into the branch office
29	Login + password	2	No	Not applicable	Report via the report form on web page
30	Other, please specify	I prefer not to answer	No answer	No answer	No answer
31	Login + password + random verification code	8	Yes	Yes	No answer
32	Login + password + token device	I prefer not to answer	Yes	No	Call number provided on 'contact us' page
33	Login + password	8	No	Not applicable	Direct inform by walking into the branch office

Respondent's ID	C6	C7	C8	C9	C10
34	Login + password	15	Yes	No	Report via e-mail provided Report via the report form on web page Call number provided on 'contact us' page Direct inform by walking into the branch office
35	Login + password Login + password + mobile (SMS) verification code	10	No	Not applicable	Report via the report form on web page
36	Login + password + mobile (SMS) verification code	No Answer	Yes	No	No answer
37	Login + password	10	Yes	No	Call number provided on 'contact us' page
38	Login + password + mobile (SMS) verification code	I prefer not to answer	No	Not applicable	Direct inform by walking into the branch office
39	Login + password + token device	8	No	Not applicable	Report to police
40	Login + password	10	Yes	Yes	Call number provided on 'contact us' page
41	Login + password	2	No	Not applicable	Call number provided on 'contact us' page
42	Login + password	11	No	Not applicable	Report via e-mail provided Call number provided on 'contact us' page Direct inform by walking into the branch office
43	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
44	Login + password	8	No	Not applicable	Report via the report form on web page Call number provided on 'contact us' page
45	Login + password	I prefer not to answer	No	Not applicable	Report via e-mail provided Report via the report form on web page Call number provided on 'contact us' page
46	Login + password	10	Yes	No	Call number provided on 'contact us' page Direct inform by walking into the branch office
47	Login + password	11	No	Not applicable	Report via the report form on web page
48	Login + password + random verification code	10	No	Not applicable	Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
49	No answer	No answer	No answer	No answer	No answer
50	No answer	9	No	Not applicable	Direct inform by walking into the branch office
51	Login + password	I prefer not to answer	Yes	Yes	Call number provided on 'contact us' page
52	Login + password	10	No	Not applicable	Report via e-mail provided Call number provided on 'contact us' page
53	Login + password	8	No	Not applicable	Call number provided on 'contact us' page
54	Login + password	10	Yes	No	Call number provided on 'contact us' page Direct inform by walking into the branch office
55	Login + password + mobile (SMS) verification code	10	No	Not applicable	Call Bank Call Centre to ask about the problem.
56	Login + password Login + password + mobile (SMS) verification code	8	No	Not applicable	Report via the report form on web page
57	Login + password Login + password + security questions (e.g. what is your mother's maiden name?)	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
58	Login + password	10	Yes	Yes	No answer
59	Login + password	2	No	Not applicable	Report via e-mail provided Call number provided on 'contact us' page
60	Login + password	I prefer not to answer	Yes	Yes	Call number provided on 'contact us' page
61	Login + password	10	No	Not applicable	Call number provided on 'contact us' page
62	Login + password Login + password + mobile (SMS) verification code	I prefer not to answer	Yes	No	No answer
63	Login + password	2	No	Not applicable	Call number provided on 'contact us' page
64	Login + password	10	Yes	Yes	Call number provided on 'contact us' page
65	Login + password	No answer	No	Not applicable	Direct inform by walking into the branch office
66	Login + password	10	No	Not applicable	Direct inform by walking into the branch office

Respondent's ID	C6	C7	C8	C9	C10
67	Login + password + mobile (SMS) verification code Login + password + security questions (e.g. what is your mother's maiden name?)	8	Yes	No	Call number provided on 'contact us' page
68	Login + password Login + password + token device Use ID and PIN entered via mouse (cannot be typed).	2	No	Not applicable	Report via the report form on web page Call number provided on 'contact us' page
69	Login + password	10	No	Not applicable	Report via the report form on web page
70	Login + password	8	Yes	No	No answer
71	Login + password + mobile (SMS) verification code	I prefer not to answer	No	Not applicable	Report via e-mail provided
72	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page
73	Login + password	No answer	No	Not applicable	Report via the report form on web page Call number provided on 'contact us' page
74	Login + password Login + password + token device	I prefer not to answer	Yes	No	Other, please specify
75	Login + password	10	No	Not applicable	Call number provided on 'contact us' page
76	Login + password + mobile (SMS) verification code	8	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
77	Login + password	2	No	Not applicable	Direct inform by walking into the branch office
78	Login + password	I prefer not to answer	No	Not applicable	Direct inform by walking into the branch office
79	Login + password	2	Yes	No	Call number provided on 'contact us' page
80	Login + password + random verification code	8	Yes	Yes	Call number provided on 'contact us' page Direct inform by walking into the branch office
81	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
82	Login + password	I prefer not to answer	No	Not applicable	Report via e-mail provided Report via the report form on web page Call number provided on 'contact us' page Report to police Depends on the problem.
83	Login + password + token device Login + password + mobile (SMS) verification code	8	Yes	No	Report via e-mail provided Direct inform by walking into the branch office
84	Login + password	2	Yes	No	Call number provided on 'contact us' page
85	Login + password	10	No	Not applicable	Report via e-mail provided Call number provided on 'contact us' page
86	Login + password Login + password + token device	8	Yes	Yes	Report via e-mail provided Report via the report form on web page
87	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
88	Login + password	8	No	Not applicable	No answer
89	Login + password	8	Yes	Yes	Direct inform by walking into the branch office
90	Login + password	8	Yes	Yes	No answer
91	Login + password	2	No	Not applicable	Report via e-mail provided
92	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
93	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
94	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
95	No answer	No answer	No answer	No answer	No answer
96	Login + password Login + password + mobile (SMS) verification code	9	No	Not applicable	Call number provided on 'contact us' page
97	Login + password	8	No	Not applicable	No answer
98	Login + password	2	Yes	No	Report via e-mail provided Call number provided on 'contact us' page
99	Login + password	9	Yes	No	Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
100	Login + password + token device	8	No	Not applicable	Other, please specify
101	Login + password Login + password + token device	10	No	Not applicable	No answer
102	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
103	Login + password + biometric Login + password + token device Login + password + mobile (SMS) verification code	8	Yes	Yes	I do not report
104	Login + password Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank.	8	No	Not applicable	Call number provided on 'contact us' page
105	Login + password + mobile (SMS) verification code	8	No	Not applicable	I am not sure
106	No answer	No answer	No answer	No answer	No answer
107	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
108	Login + password	8	Yes	Yes	Call number provided on 'contact us' page
109	Login + password + mobile (SMS) verification code	I prefer not to answer	No	Not applicable	No answer
110	Login + password + biometric Login + password + security questions (e.g. what is your mother's maiden name?)	2	No	Not applicable	I am not sure
111	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
112	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page
113	Login + password	4	No	Not applicable	I am not sure
114	Login + password	2	Yes	Yes	Call number provided on 'contact us' page
115	Login + password	8	No	Not applicable	Not applicable
116	No answer	No answer	No answer	No answer	No answer
117	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
118	Login + password + security questions (e.g. what is your mother's maiden name?)	I prefer not to answer	No	Not applicable	I am not sure
119	Login + password	2	No	Not applicable	I do not report
120	No answer	7	No answer	No answer	No answer
121	Login + password	10	Yes	No	Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
122	Login + password	2	Yes	Yes	Call number provided on 'contact us' page
123	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
124	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
125	Login + password + mobile (SMS) verification code	8	No	Not applicable	Call number provided on 'contact us' page
126	Login + password	Other, please specify	No	Not applicable	Call number provided on 'contact us' page
127	Login + password	10	Yes	No	Call number provided on 'contact us' page
128	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
129	Login + password	4	No	Not applicable	Direct inform by walking into the branch office
130	Login + password Login + password + mobile (SMS) verification code	2	No	Not applicable	Call number provided on 'contact us' page
131	Login + password Login + password + security questions (e.g. what is your mother's maiden name?)	2	No	Not applicable	I am not sure
132	Login + password + mobile (SMS) verification code	2	Yes	No	Call number provided on 'contact us' page
133	Login + password Login + password + token device	4	No	Not applicable	Call number provided on 'contact us' page
134	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page
135	Login + password	4	No	Not applicable	I am not sure
136	Login + password	8	No	Not applicable	Report via e-mail provided Report via the report form on web page Direct inform by walking into the branch office
137	Login + password	8	Yes	Yes	Call number provided on 'contact us' page
138	Login + password	2	Yes	Yes	I do not report
139	Login + password	I prefer not to answer	No	Not applicable	Not applicable
140	No answer	No answer	No answer	No answer	No answer
141	Login + password Login + password + token device Login + password + mobile (SMS) verification code	8	Yes	Yes	Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
142	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
143	Login + password	8	No	Not applicable	Call number provided on 'contact us' page
144	Login + password	8	No	Not applicable	Call number provided on 'contact us' page
145	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page
146	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
147	Login + password Login + password + biometric Login + password + mobile (SMS) verification code	8	No	Not applicable	No answer
148	Login + password + security questions (e.g. what is your mother's maiden name?)	I prefer not to answer	No	Not applicable	Report via e-mail provided
149	No answer	No answer	No answer	No answer	No answer
150	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
151	Login + password Login + password + mobile (SMS) verification code	2	Yes	No	I am not sure
152	Login + password	10	No	Not applicable	No answer
153	Login + password	2	No	Not applicable	Report via e-mail provided
154	Login + password	8	No	Not applicable	Call number provided on 'contact us' page
155	Login + password	I prefer not to answer	No	Not applicable	I am not sure
156	Login + password	I prefer not to answer	Yes	Not applicable	Report via e-mail provided
157	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page
158	Login + password	2	No	Not applicable	I am not sure
159	Login + password	8	Yes	No	Call number provided on 'contact us' page
160	Login + password	8	No	Not applicable	Report via e-mail provided
161	Login + password	I prefer not to answer	Yes	Yes	Call number provided on 'contact us' page
162	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
163	Login + password	2	No	Not applicable	Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
164	Login + password Login + password + random verification code Login + password + security questions (e.g. what is your mother's maiden name?)	I prefer not to answer	No	Not applicable	Report via e-mail provided Call number provided on 'contact us' page
165	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
166	Login + password	8	Yes	No	Call number provided on 'contact us' page
167	Login + password	4	Yes	Yes	Report via the report form on web page
168	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
169	Password via online keyboard+ mobile verification codes.	2	No	Not applicable	Call number provided on 'contact us' page
170	Login + password + mobile (SMS) verification code	10	Yes	Yes	I am not sure
171	No answer	No answer	No answer	No answer	No answer
172	Login + password Login + password + mobile (SMS) verification code	I prefer not to answer	Yes	Yes	Call number provided on 'contact us' page
173	Login + password	I prefer not to answer	Yes	No	Call number provided on 'contact us' page
174	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
175	Login + password	I prefer not to answer	Yes	No	Call number provided on 'contact us' page
176	Login + password + token device	2	Yes	No	Call number provided on 'contact us' page
177	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
178	Login + password	8	Yes	Yes	No answer
179	Login + password	I prefer not to answer	Yes	No	Call number provided on 'contact us' page
180	Login + password	2	No	Not applicable	Report via e-mail provided Report via the report form on web page
181	Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank.	8	Yes	Yes	Call number provided on 'contact us' page Direct inform by walking into the branch office
182	Login + password	8	No	Not applicable	Report via e-mail provided Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
183	Login + password Login + password + token device	2	No	Not applicable	Call number provided on 'contact us' page
184	Login + password	2	No	Not applicable	Report via e-mail provided Report via the report form on web page
185	Login + password	No Answer	No	Not applicable	Call number provided on 'contact us' page Direct inform by walking into the branch office
186	Login + password	No Answer	No	Not applicable	Direct inform by walking into the branch office
187	Login + password	10	No	Not applicable	Report via e-mail provided
188	Login + password + mobile (SMS) verification code	8	Yes	Yes	Direct inform by walking into the branch office
189	Login + password Login + password + mobile (SMS) verification code	10	No	Not applicable	Report via e-mail provided Call number provided on 'contact us' page
190	Login + password + mobile (SMS) verification code	8	No	Not applicable	I am not sure
191	Login + password	No answer	Yes	No	Report via e-mail provided Call number provided on 'contact us' page Direct inform by walking into the branch office
192	Login + password + mobile (SMS) verification code	2	No	Not applicable	Not applicable
193	Login + password	11	Yes	Yes	Call number provided on 'contact us' page Direct inform by walking into the branch office
194	Login + password	No Answer	No	Not applicable	Report via the report form on web page
195	Login + password + security questions (e.g. what is your mother's maiden name?)	10	Yes	Yes	Call number provided on 'contact us' page
196	Login + password	I prefer not to answer	No	Not applicable	Call number provided on 'contact us' page
197	Login + password	10	No	Not applicable	Report via the report form on web page
198	Login + password + biometric	10	No	Not applicable	I do not report
199	Login + password + mobile (SMS) verification code	10	No	Not applicable	Call number provided on 'contact us' page

Respondent's ID	C6	C7	C8	C9	C10
200	Login + password	8	Yes	Yes	Call number provided on 'contact us' page
201	Login + password Login + password + mobile (SMS) verification code	No answer	Yes	No	Call number provided on 'contact us' page Direct inform by walking into the branch office
202	Login + password Login + password + mobile (SMS) verification code	12	No	Not applicable	Call number provided on 'contact us' page
203	Login + password	2	Yes	Yes	No answer
204	Login + password	8	Yes	Yes	No answer
205	No answer	No Answer	No	Not applicable	No answer
206	Login + password	15	No	No	I am not sure
207	Login + password + security questions (e.g. what is your mother's maiden name?)	No Answer	No	Not applicable	No answer
208	Login + password	2	Yes	Yes	Report via the report form on web page
209	Login + password + mobile (SMS) verification code	I prefer not to answer	No	Not applicable	Call number on card.

Part 3: Respondents' trust in financial institution

Respondent's ID	C11	C12
1	Not applicable	Not applicable
2	Not applicable	Not applicable
3	Not applicable	Not applicable
4	Bank	I do not know.
5	Online payment processing company (e.g. PayPal)	"In my experience, they SEEM to have the best security."
6	I am not sure.	Not applicable
7	Credit card company	"They scan everyone's credit card habits."
8	Not applicable	Not applicable
9	Bank	Never had a problem.
10	Bank	"The bank website does not store my personal information (login details) whereas some sites remember my address & telephone numbers."
11	I am not sure.	I do not know.
12	Online payment processing company (e.g. PayPal)	"Password authentication."
13	I am not sure.	Not applicable

Respondent's ID	C11	C12
14	I am not sure.	I do not know.
15	Bank	"Their high standards."
16	I am not sure.	I do not know.
17	Bank	"Because, they refund for any unauthorised attack."
18	I am not sure.	"Password/PIN"
19	Bank	"Protect customer information. Provide convenience service in a security way."
20	I am not sure.	I do not know.
21	I am not sure.	I do not know.
22	Bank	I do not know.
23	Bank	I do not know.
24	Bank	"My digipass and the strong encryption."
25	Bank	I do not know.
26	Bank	I do not know.
27	Bank	I do not know.
28	Bank	"Most banks have various levels of protection which make it more efficient."
29	I am not sure.	Not applicable
30	I am not sure.	Not applicable
31	Bank	"It is safe to visit the bank's homepage."
32	Online shopping websites (e.g. eBay, Amazon)	I do not know.
33	Credit card company	I do not know.
34	Bank	No answer
35	I am not sure.	I do not know.
36	I am not sure.	I do not know.
37	I am not sure.	Not applicable
38	Bank	"The bank is government built."
39	Credit card company	No answer
40	Online payment processing company (e.g. PayPal)	"Constantly updating & confirming our details."
41	I am not sure.	I do not know.
42	Bank	No answer
43	Not applicable	Not applicable
44	Online payment processing company (e.g. PayPal)	"Must go into an e-mail and confirm that you have chosen the option on the website."
45	I am not sure.	I do not know.
46	I am not sure.	I do not know.
47	Online payment processing company (e.g.	"They are anonymous your information which makes it harder for others to steal your information/ money."

Respondent's ID	C11	C12
	PayPal)	
48	I am not sure.	"Often security is not advised i.e. they don't tell you what they have in place."
49	No answer	No answer
50	I am not sure.	Not applicable
51	Bank	"Confirming transaction by SMS."
52	Bank	Not applicable
53	Bank	I do not know.
54	I am not sure.	I do not know.
55	Bank	No answer
56	I am not sure.	Not applicable
57	Bank	"Randomised virtual keypad for password input. It's painful, because it is encrypted and doesn't use the keypad, but rather uses mouse clicks, it's safer from keyloggers."
58	I am not sure.	Not applicable
59	I am not sure.	Not applicable
60	I am not sure.	Not applicable
61	I am not sure.	I do not know.
62	I am not sure.	Not applicable
63	Bank	No answer
64	Bank	I do not know.
65	I don't trust anyone.	Not applicable
66	I am not sure.	Not applicable
67	Bank	"It is time least bad."
68	I am not sure.	Not applicable
69	Online stock brokers	"They have to provide information for tax purposes, so I guess they are more likely to be careful."
70	I am not sure.	Not applicable
71	I am not sure.	Not applicable
72	I am not sure.	Not applicable
73	I am not sure.	Not applicable
74	Bank	"It has been saved for me."
75	Bank	I do not know.
76	Bank	I do not know.
77	Bank	I do not know.
78	Bank	Their Guarantee.
79	I am not sure.	"I don't like or dislike it. I just assume they make it a secure as possible."
80	Bank	"Assuming the banks are big organisation, I trust their protection system more than the others since they will have more money to invest on online protection."
81	Bank	I do not know.
82	I am not sure.	Not applicable
83	Bank	I do not know.
84	Bank	"The option to change the password whenever I request."
85	Bank	"I am with them, so I use their security."
86	Bank	"If you make a big mistake you must contact the provider to correct it again."

Respondent's ID	C11	C12
87	Not applicable	Not applicable
88	Bank	I do not know.
89	Bank	I do not know.
90	Bank	No answer
91	Bank	"Security with accessing account is good."
92	Not applicable	Not applicable
93	Not applicable	Not applicable
94	Not applicable	Not applicable
95	No answer	No answer
96	No answer	No answer
97	Bank	I do not know.
98	Bank	"They ask authentic question & lock you out if they are incorrect or unsure."
99	Bank	I do not know.
100	I am not sure.	Not applicable
101	Online payment processing company (e.g. PayPal)	I do not know.
102	Not applicable	Not applicable
103	Bank	"Verification code."
104	Bank	I do not know.
105	Bank	"Needing to use a sms verification code before money can be transferred to a new account."
106	No answer	No answer
107	Not applicable	Not applicable
108	I am not sure.	Not applicable
109	Bank	"Both password and mobile authorise."
110	Bank	I do not know.
111	Not applicable	Not applicable
112	I am not sure.	Not applicable
113	Bank	"Appears to be secured."
114	I am not sure.	I do not know.
115	Bank	"Allowed to use long passwords with both letters and numbers for added security."
116	No answer	No answer
117	Not applicable	Not applicable
118	Credit card company	"Security Questions."
119	Bank	No answer
120	No answer	No answer
121	I am not sure.	Not applicable
122	I am not sure.	Not applicable
123	Not applicable	Not applicable
124	Not applicable	Not applicable

Respondent's ID	C11	C12
125	Bank	"Notification of accessing the service via e-mail."
126	Bank	I do not know.
127	Bank	I do not know.
128	Not applicable	Not applicable
129	Bank	No answer
130	Bank	"They invest into security & responsibility for any loss of money from me."
131	I am not sure.	Not applicable
132	I am not sure.	Not applicable
133	Bank	No answer
134	Bank	No answer
135	Online payment processing company (e.g. PayPal)	"Password security."
136	I am not sure.	Not applicable
137	I am not sure.	Not applicable
138	Bank	I do not know.
139	Bank	No answer
140	No answer	No answer
141	Bank	"SMS, Token"
142	Not applicable	Not applicable
143	I am not sure.	Not applicable
144	I am not sure.	Not applicable
145	Bank	Not applicable
146	Not applicable	Not applicable
147	I am not sure.	Not applicable
148	Bank	Not applicable
149	No answer	Not applicable
150	Not applicable	Not applicable
151	Bank	Not applicable
152	Companies that also use an external code on special remote.	"Feel safe."
153	Bank	No answer
154	Bank	"Strong encrypted but still easy to use."
155	I am not sure.	Not applicable
156	Bank	No answer
157	I am not sure.	Not applicable
158	Bank	No answer
159	I am not sure.	Not applicable
160	I am not sure.	Not applicable
161	Bank	"Offers a level that I need to give me confidence to use their online banking."
162	Not applicable	Not applicable

Respondent's ID	C11	C12
163	No answer	No answer
164	Online payment processing company (e.g. PayPal)	I do not know.
165	Not applicable	Not applicable
166	I am not sure.	Not applicable
167	Bank	I do not know.
168	Not applicable	Not applicable
169	Bank	"Sms code."
170	Online payment processing company (e.g. PayPal)	I do not know.
171	No answer	No answer
172	Bank	I do not know.
173	Bank	No answer
174	Not applicable	Not applicable
175	I am not sure.	Not applicable
176	Bank	No answer
177	Not applicable	Not applicable
178	Bank	I do not know.
179	I am not sure.	Not applicable
180	They are all equally bad.	"That you are "usually" insured against financial losses related to hacking."
181	Bank	I do not know.
182	Bank	"Password encryption and selected with mouse (keyloggers are of no use)."
183	I am not sure.	Not applicable
184	Credit card company	"Average user doesn't know who they are to start with."
185	Bank	I do not know.
186	I am not sure.	Not applicable
187	Bank	I do not know.
188	I am not sure.	Not applicable
189	Bank	"HTTPS secure web."
190	Bank	"I do not know."
191	Online payment processing company (e.g. PayPal)	"Strong encryption."
192	Bank	I do not know.
193	Bank	I do not know.
194	Credit card company	No answer
195	Online shopping websites (e.g.	I do not know.

Respondent's ID	C11	C12
	eBay, Amazon)	
196	Bank	I do not know.
197	Online payment processing company (e.g. PayPal)	I do not know.
198	Bank	I do not know.
199	Bank	I do not know.
200	Bank	I do not know.
201	Bank	I do not know.
202	Bank	I do not know.
203	I am not sure.	Not applicable
204	I am not sure.	Not applicable
205	Credit card company	I do not know.
206	Bank	I do not know.
207	Bank	"SMS code."
208	Online payment processing company (e.g. PayPal)	"Token Device."
209	Bank	"SMS Verification Code."

APPENDIX K: Data of respondents' preferences in a deployment of online banking security protection

Part 1: Authentication security preferences

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
1	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
3	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
4	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	Not applicable	8
5	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + biometric Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason Would not remember the passwords therefore would have to write it down which is an added security risk.	Never Unless it has been compromised.	8
6	Yes (go to qD3)	$2-$5 per month	Lower case alphabets (e.g. abc)	Login + password + biometric	Yes, I would agree (go to D7)	Never	8
7	No (go to qD4)	Not applicable	Mixed of numbers and upper case alphabets	Login + password + token device	No, I would not agree, Please specify your reason Convenience.	I am not sure.	10-20
8	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
9	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every month	No answer
10	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every 3 months	6

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
11	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric Login + password + token device Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every month	15
12	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + token device	Yes, I would agree (go to D7)	Once a year	10
13	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason Only Password doesn't protect.	Once a year	10
14	Yes (go to qD3)	I am not sure	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + biometric Login + password + mobile (SMS) verification code	No answer	No answer	No answer
15	Yes (go to qD3)	I am not sure	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Just when there is a need.	8
16	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	Every 3 months	8
17	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets Mixed of numbers and upper case alphabets	Login + password + mobile (SMS) verification code Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every 6 months	8
18	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	Every 3 months	6

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
19	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7) For security I agree. But I still think not very well ask their customers to change always. They should do lots of work, not customers.	Never If no need, never.	6-8
20	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and upper case alphabets	Login + password Login + password + token device Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	No answer	6
21	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	No answer	Yes, I would agree (go to D7)	I am not sure.	10
22	No (go to qD4)	Not applicable	Special characters (e.g. @#%&*)	No answer	Yes, I would agree (go to D7)	I am not sure.	10
23	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	Every 3 months	10
24	Yes (go to qD3)	$1 per month	Numbers	Login + password + token device	No, I would not agree, Please specify your reason They all should use digipass.	No need to change when using digipass.	8
25	Yes (go to qD3)	$2-$5 per month	Mixed of number and special characters	Login + password + random verification code	Yes, I would agree (go to D7)	No answer	7
26	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	No answer	8
27	Yes (go to qD3)	$2-$5 per month	I prefer not to answer	Login + password + biometric	Yes, I would agree (go to D7)	No answer	5-6
28	No (go to qD4)	Not applicable	No answer	No answer	No, I would not agree, Please specify your reason It means that bank has a problem with security system. I prefer to change bank.	No answer	8

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
29	No (go to qD4)	Not applicable	I prefer not to answer	Login + password + biometric Login + password + random verification code Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every month	10
30	No (go to qD4)	Not applicable	I prefer not to answer	Other, please specify	Yes, I would agree (go to D7)	Every month	9
31	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and upper case alphabets	Login + password + random verification code	Yes, I would agree (go to D7)	Every 3 months	No answer
32	No (go to qD4)	Not applicable	Special characters (e.g. @#%&*)	Login + password + biometric	Yes, I would agree (go to D7)	Every 3 months	11
33	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	Every 3 months	No answer
34	No (go to qD4)	Not applicable	No answer	Login + password + token device Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	No answer	8
35	Yes (go to qD3)	$1 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + security questions (e.g. what is your mother's maiden name?)	No, I would not agree, Please specify your reason Already too many passwords to remember.	Never	10
36	Yes (go to qD3)	$2-$5 per month	No answer	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	I am not sure.	10
37	Yes (go to qD3)	$6-$10 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password	Yes, I would agree (go to D7)	Every month	12

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
38	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + biometric	Yes, I would agree (go to D7)	Every 3 months	10
39	Yes (go to qD3)	More than $10 per month	No answer	Login + password + token device	Yes, I would agree (go to D7)	I am not sure.	No answer
40	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password + biometric Login + password + mobile (SMS) verification code Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every month	10-12
41	Yes (go to qD3)	$6-$10 per month	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every 3 months	6
42	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank.	Yes, I would agree (go to D7)	Once a year	No answer
43	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
44	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every month	8
45	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank.	Yes, I would agree (go to D7)	I am not sure.	8

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
46	Yes (go to qD3)	$1 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + random verification code	Yes, I would agree (go to D7)	Every 3 months	8
47	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + token device	Yes, I would agree (go to D7)	Never	6
48	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets Not sure if it matters if there is a verification (image) device + passwords are changed regularly. Maybe need to remind customers to change passwords as per the university.	Login + password + random verification code	Yes, I would agree (go to D7)	Every 3 months	Unlimited
49	No answer	No answer	No answer	No answer	No answer	No answer	No answer
50	No (go to qD4)	Not applicable	Numbers	Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every month	10
51	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	Not applicable	No answer
52	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric	Yes, I would agree (go to D7)	Every 6 months	10-15
53	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	Every 6 months	8
54	Yes (go to qD3)	No answer	No answer	Login + password + token device	Yes, I would agree (go to D7)	Every month	8

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
55	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric Login + password + token device Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 6 months	8
56	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 3 months	8
57	Yes (go to qD3)	$2-$5 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric Login + password + security questions (e.g. what is your mother's maiden name?)	No, I would not agree, Please specify your reason It's too painful, and takes too much admin to track it.	No answer	7
58	Yes (go to qD3)	No answer	No answer	Login + password + token device	No, I would not agree, Please specify your reason I can't remember my password.	No answer	8
59	Yes (go to qD3)	I am not sure	Mixed of numbers and lower case alphabets	Login + password Login + password + random verification code	Yes, I would agree (go to D7)	Every 6 months	6
60	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password + mobile (SMS) verification code Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every 6 months	6
61	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	No answer	No answer

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
62	No (go to qD4)	Not applicable	Numbers	Login + password	Yes, I would agree (go to D7)	Every 6 months	6
63	Yes (go to qD3)	$1 per month	Mixed of numbers and lower case alphabets	Login + password + biometric	Yes, I would agree (go to D7)	Every 3 months	6
64	Yes (go to qD3)	$1 per month	Numbers	Login + password Login + password + token device	Yes, I would agree (go to D7)	Every 3 months	12
65	Yes (go to qD3)	More than $10 per month	No answer	Login + password + random verification code	No, I would not agree, Please specify your reason I cannot think of many decent passwords and remember it.	Security Risk (I don't like changing, but that doesn't mean I don't change it.)	16
66	No (go to qD4)	Not applicable	No answer	No answer	No, I would not agree, Please specify your reason Easy to forget the password.	I am not sure.	8
67	No (go to qD4)	Not applicable	Other, please specify	Login + password + biometric	No, I would not agree, Please specify your reason Frequently changing password means I cannot remember them so have to write them down.	When I choose to.	8
68	No (go to qD4)	Not applicable	No answer	No answer	No, I would not agree, Please specify your reason Arbitrarily changing passwords make people write them down.	Never	8
69	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + biometric	Yes, I would agree (go to D7)	No answer	9

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
70	Yes (go to qD3)	$6-$10 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric Login + password + token device Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	No answer	12
71	No (go to qD4)	Not applicable	No answer	No answer	Yes, I would agree (go to D7)	No answer	7
72	No (go to qD4)	Not applicable	I prefer not to answer	Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Once a year	6
73	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password	No, I would not agree, Please specify your reason Privacy	Once a year	6
74	No (go to qD4)	Not applicable	No answer	No answer	No, I would not agree, Please specify your reason No answer	Once a year	More than10.
75	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 6 months	10
76	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + token device Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 3 months	6

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
77	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code Login + password + random verification code	No, I would not agree, Please specify your reason	Never	8
78	Yes (go to qD3)	I am not sure	I prefer not to answer	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 3 months	4
79	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password + biometric Login + password + token device	Yes, I would agree (go to D7)	Every 3 months	6
80	Yes (go to qD3)	$1 per month	Mixed of numbers and lower case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 6 months	8
81	No (go to qD4)	Not applicable	I prefer not to answer	Login + password	No, I would not agree, Please specify your reason I would be skeptical that it is a scam; it would depend on how they contacted me and the procedure to change the password.	Every 3 months	8
82	Yes (go to qD3)	$1 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric	Yes, I would agree (go to D7)	I am not sure.	8
83	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password + token device Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason No answer	No answer	8
84	No (go to qD4)	Not applicable	Upper case alphabets (e.g., ABC)	Login + password	Yes, I would agree (go to D7)	Every month	6

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
85	No (go to qD4)	Not applicable	Numbers	Login + password + biometric	Yes, I would agree (go to D7)	Every 3 months	8-10
86	Yes (go to qD3)	$1 per month	Mixed of numbers and upper case alphabets	Login + password + token device Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 6 months	8-10
87	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
88	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every 6 months	8
89	Yes (go to qD3)	I am not sure	Lower case alphabets (e.g. abc)	Login + password	Yes, I would agree (go to D7)	Every 6 months	10
90	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 6 months	8
91	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every 3 months	6
92	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
93	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
94	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
95	No answer	No answer	No answer	No answer	No answer	No answer	No answer
96	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	I am not sure.	9
97	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every month	8
98	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	No, I would not agree, Please specify your reason Waste of time to be complicated.	Once a year	6

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
99	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every month	7
100	Yes (go to qD3)	Other, please specify.....	Mixed of numbers and lower case alphabets	Login + password + token device	No, I would not agree, Please specify your reason No answer	No answer	8
101	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + token device	Yes, I would agree (go to D7)	Never	10
102	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
103	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Other, please specify	Yes, I would agree (go to D7)	Every 3 months	16
104	No (go to qD4)	Not applicable	Mixed of number and special characters	Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank.	No, I would not agree, Please specify your reason No answer	Never	8
105	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password + biometric	Yes, I would agree (go to D7)	Every 3 months	8
106	No answer	No answer	No answer	No answer	No answer	No answer	No answer
107	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
108	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password	No, I would not agree, Please specify your reason Can't be bothered.	Never	6
109	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric	Yes, I would agree (go to D7)	Every month	8

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
110	No (go to qD4)	Not applicable	Mixed of number and special characters	Login + password Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Never	No answer
111	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
112	No answer	No answer	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + token device	No, I would not agree, Please specify your reason I'd forget.	Once a year	8
113	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every month	No answer
114	Yes (go to qD3)	I am not sure	Mixed of number and special characters	Login + password + biometric Login + password + token device	Yes, I would agree (go to D7)	Every 3 months	6
115	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password Login + password + mobile (SMS) verification code Login + password + security questions (e.g. what is your mother's maiden name?)	No, I would not agree, Please specify your reason Fear of forgetting password.	Never	8
116	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + random verification code	Yes, I would agree (go to D7)	Every 6 months	8
117	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
118	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + random verification code	Yes, I would agree (go to D7)	I am not sure.	10
119	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	3-6 months	8
120	No answer	No answer	No answer	No answer	No answer	No answer	No answer
121	Yes (go to qD3)	$1 per month	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every 6 months	8
122	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password	Yes, I would agree (go to D7)	I am not sure.	6-8
123	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
124	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
125	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Once a year	More than 5
126	Yes (go to qD3)	I am not sure	Numbers	Login + password	Yes, I would agree (go to D7)	Every month	6
127	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every 6 months	8
128	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
129	Yes (go to qD3)	$2-$5 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + token device	Yes, I would agree (go to D7)	Every 3 months	9
130	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Once a year	6
131	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	I am not sure.	No answer
132	Yes (go to qD3)	I am not sure	I prefer not to answer	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	It depends on my feeling.	No answer
133	Yes (go to qD3)	$2-$5 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason It's easy to forget	Never	6-10
134	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason Might get confused	Never	8
135	No (go to qD4)	Not applicable	Other, please specify	Login + password Login + password + biometric	No, I would not agree, Please specify your reason Do not want to remember a new password.	No answer	More than 4.
136	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	Yes, I would agree (go to D7)	Every 6 months	6
137	Yes (go to qD3)	More than $10 per month	Numbers	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Never	No answer
138	No (go to qD4)	Not applicable	Special characters (e.g. @#%&*)	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 6 months	6

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
139	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every 6 months	10
140	No answer	Not applicable	No answer	No answer	No answer	No answer	No answer
141	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric Login + password + token device Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason Too troublesome & mess up password. Too many versions over the time.	No answer	Doesn't matter
142	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
143	No (go to qD4)	Not applicable	Upper case alphabets (e.g., ABC) Special characters (e.g. @#%&*)	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	I am not sure.	6
144	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and upper case alphabets	Login + password	Yes, I would agree (go to D7)	Every 3 months	8
145	Yes (go to qD3)	$1 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password	Yes, I would agree (go to D7)	Every 3 months	8
146	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
147	No (go to qD4)	Not applicable	I prefer not to answer	Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason I want to choose when to change.	Once a year	8-10
148	Yes (go to qD3)	$6-$10 per month	No answer	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every month	7

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
149	No answer	No answer	No answer	No answer	No answer	No answer	No answer
150	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
151	Yes (go to qD3)	$1 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	No answer	10
152	Yes (go to qD3)	$1 per month	Mixed of numbers and lower case alphabets	No answer	Yes, I would agree (go to D7)	Once a year	No answer
153	No answer	No answer	No answer	No answer	No answer	No answer	No answer
154	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	All combined from 1-7.	Yes, I would agree (go to D7)	Every month	8
155	No (go to qD4)	Not applicable	I prefer not to answer	Login + password	Yes, I would agree (go to D7)	Every month	No answer
156	No (go to qD4)	Not applicable	Lower case alphabets (e.g. abc)	Login + password	Yes, I would agree (go to D7)	Every month	No answer
157	No (go to qD4)	Not applicable	I prefer not to answer	Login + password	Not applicable	No answer	Not applicable
158	Yes (go to qD3)	I am not sure	I prefer not to answer	Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every 6 months	No answer
159	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + biometric Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every month	7
160	No (go to qD4)	Not applicable	Numbers	Login + password + biometric	Yes, I would agree (go to D7)	Every 6 months	8

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
161	Yes (go to qD3)	$2-$5 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + token device	Yes, I would agree (go to D7)	Every 3 months	No answer
162	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
163	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Other, please specify	No, I would not agree, Please specify your reason No answer	Never	8
164	No (go to qD4)	Not applicable	Lower case alphabets (e.g. abc)	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	I am not sure.	No answer
165	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
166	Yes (go to qD3)	I am not sure	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password	Yes, I would agree (go to D7)	Every 3 months	8
167	No (go to qD4)	Not applicable	Numbers	Login + password	Yes, I would agree (go to D7)	Every month	5
168	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
169	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 3 months	10
170	Yes (go to qD3)	$1 per month	Numbers	Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank.	No, I would not agree, Please specify your reason No answer	Once a year	5
171	No answer	No answer	No answer	No answer	No answer	No answer	No answer

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
172	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + mobile (SMS) verification code	Not applicable	I am not sure.	6
173	Yes (go to qD3)	$1 per month	Mixed of number and special characters	Login + password + random verification code	Yes, I would agree (go to D7)	Every month	No answer
174	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
175	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password	Yes, I would agree (go to D7)	Every 6 months	8
176	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + token device Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Once a year	6-8
177	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
178	No (go to qD4)	Not applicable	Numbers	Login + password	No, I would not agree, Please specify your reason No answer	Never	9
179	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	No, I would not agree, Please specify your reason Too difficult.	I am not sure.	5
180	Yes (go to qD3)	$2-$5 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + token device Login + password + random verification code	Yes, I would agree (go to D7)	Every month	8

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
181	Yes (go to qD3)	$6-$10 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank. Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every 3 months	6
182	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + token device	Yes, I would agree (go to D7)	Every 6 months	7
183	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + token device	No, I would not agree, Please specify your reason No answer	I am not sure.	15
184	Yes (go to qD3)	$2-$5 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + random verification code	Yes, I would agree (go to D7)	When I feel like doing (after every transaction over the web).	8
185	Yes (go to qD3)	$1 per month	I prefer not to answer	Login + password + token device	Yes, I would agree (go to D7)	Every 3 months	8
186	Yes (go to qD3)	$6-$10 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 3 months	8
187	No (go to qD4)	Not applicable	Mixed of numbers and upper case alphabets	Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason Too troublesome.	Never	10

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
188	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + biometric	Yes, I would agree (go to D7)	Every 3 months	8
189	Yes (go to qD3)	$1 per month	Mixed of number and special characters Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + biometric Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason Hard to remember because there so many passwords and pins these days.	Every 6 months	10
190	No (go to qD4)	Already pay enough bank fees for this to be covered.	Lower case alphabets (e.g. abc)	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Every 6 months	8
191	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Every month	8
192	No answer	No answer	No answer	No answer	No answer	No answer	No answer
193	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason Troublesome.	Never	8
194	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password	No, I would not agree, Please specify your reason No answer	Every month	8
195	Yes (go to qD3)	$1 per month	Lower case alphabets (e.g. abc) Mixed of numbers and upper case alphabets	Login + password + token device	Yes, I would agree (go to D7)	Every 3 months	No answer

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
196	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + static verification code attached on your credit card, EFTPOS, or written on your paper given by bank. Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Once a year	6
197	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password Login + password + token device	Yes, I would agree (go to D7)	Once a year	6
198	No (go to qD4)	Not applicable	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password Login + password + security questions (e.g. what is your mother's maiden name?)	No, I would not agree, Please specify your reason It makes trouble.	Never	6
199	No (go to qD4)	Not applicable	Mixed of numbers and lower case alphabets	Login + password + mobile (SMS) verification code	No, I would not agree, Please specify your reason No answer	Every 3 months	No answer
200	Yes (go to qD3)	$2-$5 per month	Mixed of numbers, special characters, lower case and upper case alphabets	Login + password	Yes, I would agree (go to D7)	Every 6 months	8
201	No (go to qD4)	Not applicable	Mixed of number and special characters	Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Once a year	10
202	No (go to qD4)	Not applicable	Mixed of number and special characters	Login + password Login + password + mobile (SMS) verification code	Yes, I would agree (go to D7)	Never	8

Respondent's ID	D1	D2	D3	D4	D5	D6	D7
203	No (go to qD4)	Not applicable	I prefer not to answer	Login + password + biometric Login + password + mobile (SMS) verification code Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	I am not sure.	8
204	Yes (go to qD3)	$2-$5 per month	Numbers Lower case alphabets (e.g. abc)	Login + password	Yes, I would agree (go to D7)	Every 3 months	8
205	No answer	No answer	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
206	No (go to qD4)	Not applicable	I prefer not to answer	Login + password + biometric	Yes, I would agree (go to D7)	Every 3 months	15
207	No (go to qD4)	Not applicable	I prefer not to answer	Login + password + security questions (e.g. what is your mother's maiden name?)	Yes, I would agree (go to D7)	Once a year	8
208	Yes (go to qD3)	$2-$5 per month	Mixed of numbers and lower case alphabets	Login + password + token device	No, I would not agree, Please specify your reason It might be a phishing.	Every 3 months	9
209	Yes (go to qD3)	$1 per month	I prefer not to answer	Login + password + token device	Yes, I would agree (go to D7)	Every 3 months	15

Part 2: Authentication security prioritised

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
1	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
3	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
4	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
5	The minimum protection	The fourth maximum protection	The second maximum protection	The maximum protection	The sixth maximum protection	The fifth maximum protection	The third maximum protection
6	The fourth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The sixth maximum protection	The minimum protection	The fifth maximum protection
7	The maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
8	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
9	The second maximum protection	The fourth maximum protection	The maximum protection	The third maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
10	The minimum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The second maximum protection	The maximum protection	The sixth maximum protection
11	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
12	The third maximum protection	The second maximum protection	The maximum protection	The fourth maximum protection	The fifth maximum protection	The minimum protection	The sixth maximum protection
13	The minimum protection	The second maximum protection	The sixth maximum protection	The maximum protection	The third maximum protection	The fourth maximum protection	The fifth maximum protection
14	No answer	No answer	No answer	No answer	No answer	No answer	No answer
15	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The maximum protection	The second maximum protection
16	The maximum protection	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection
17	The minimum protection	The third maximum protection	The fourth maximum protection	The maximum protection	The sixth maximum protection	The fifth maximum protection	The second maximum protection
18	No answer	No answer	No answer	No answer	No answer	No answer	No answer
19	The minimum protection	The third maximum protection	The second maximum protection	The maximum protection	The fifth maximum protection	The sixth maximum protection	The fourth maximum protection

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
20	The minimum protection	The fourth maximum protection	The third maximum protection	The second maximum protection	The sixth maximum protection	The fifth maximum protection	The maximum protection
21	The fourth maximum protection	The sixth maximum protection	The fifth maximum protection	The maximum protection	The third maximum protection	The minimum protection	The second maximum protection
22	The minimum protection	The sixth maximum protection	The fifth maximum protection	The second maximum protection	The fourth maximum protection	The third maximum protection	The maximum protection
23	The sixth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The minimum protection
24	The minimum protection	The sixth maximum protection	The maximum protection	The fifth maximum protection	The fourth maximum protection	The second maximum protection	The third maximum protection
25	No answer	No answer	No answer	No answer	No answer	No answer	No answer
26	The minimum protection	The second maximum protection	The sixth maximum protection	The third maximum protection	The fifth maximum protection	The maximum protection	The fourth maximum protection
27	The minimum protection	The maximum protection	The fourth maximum protection	The fifth maximum protection	The third maximum protection	The second maximum protection	The sixth maximum protection
28	The minimum protection	The maximum protection	The second maximum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection
29	The sixth maximum protection	The second maximum protection	The fourth maximum protection	The fifth maximum protection	The minimum protection	The maximum protection	The third maximum protection
30	The minimum protection	The fifth maximum protection	The sixth maximum protection	The second maximum protection	The third maximum protection	The maximum protection	The fourth maximum protection
31	The minimum protection	The third maximum protection	The fourth maximum protection	The second maximum protection	The sixth maximum protection	The maximum protection	The fifth maximum protection
32	The second maximum protection	The sixth maximum protection	The minimum protection	The fifth maximum protection	The maximum protection	The third maximum protection	The fourth maximum protection
33	The minimum protection	The second maximum protection	The third maximum protection	The sixth maximum protection	The fifth maximum protection	The maximum protection	The fourth maximum protection
34	The sixth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The minimum protection	The fifth maximum protection	The fourth maximum protection
35	The minimum protection	The sixth maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The second maximum protection	The maximum protection
36	The minimum protection	The sixth maximum protection	The third maximum protection	The maximum protection	The fifth maximum protection	The second maximum protection	The fourth maximum protection
37	The maximum protection	The third maximum protection	The second maximum protection	The fourth maximum protection	The sixth maximum protection	The minimum protection	The fifth maximum protection

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
38	The maximum protection	The minimum protection	The sixth maximum protection	The fourth maximum protection	The fifth maximum protection	The third maximum protection	The second maximum protection
39	The fifth maximum protection	The third maximum protection	The fourth maximum protection	The minimum protection	The second maximum protection	The maximum protection	The sixth maximum protection
40	The third maximum protection	The second maximum protection	The minimum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection	The maximum protection
41	The minimum protection	The fifth maximum protection	The third maximum protection	The second maximum protection	The fourth maximum protection	The sixth maximum protection	The maximum protection
42	The minimum protection	The fourth maximum protection	The maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection
43	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
44	The minimum protection	The maximum protection	The second maximum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection	The third maximum protection
45	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The maximum protection	The second maximum protection	The third maximum protection
46	The minimum protection	The maximum protection	The third maximum protection	The fourth maximum protection	The second maximum protection	The sixth maximum protection	The fifth maximum protection
47	The minimum protection	The third maximum protection	The fourth maximum protection	The fifth maximum protection	The maximum protection	The second maximum protection	The sixth maximum protection
48	The fifth maximum protection	The fourth maximum protection	The maximum protection	The sixth maximum protection	The minimum protection	The second maximum protection	The third maximum protection
49	The maximum protection	The second maximum protection	The sixth maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The minimum protection
50	The maximum protection	The fourth maximum protection	The third maximum protection	The fifth maximum protection	The minimum protection	The sixth maximum protection	The second maximum protection
51	The minimum protection	The maximum protection	The third maximum protection	The second maximum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection
52	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
53	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection	The maximum protection
54	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
55	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
56	The minimum protection	The maximum protection	The third maximum protection	The second maximum protection	The sixth maximum protection	The fourth maximum protection	The fifth maximum protection
57	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
58	The sixth maximum protection	The second maximum protection	The maximum protection	The third maximum protection	The minimum protection	The fourth maximum protection	The sixth maximum protection
59	No answer	No answer	No answer	No answer	No answer	No answer	No answer
60	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
61	The minimum protection	The maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection	The sixth maximum protection
62	The second maximum protection	The fifth maximum protection	The fourth maximum protection	The maximum protection	The sixth maximum protection	The minimum protection	The third maximum protection
63	The third maximum protection	The maximum protection	The second maximum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
64	The second maximum protection	The maximum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection	The third maximum protection
65	The maximum protection	The fifth maximum protection	The fourth maximum protection	The second maximum protection	The third maximum protection	The minimum protection	The sixth maximum protection
66	The minimum protection	The sixth maximum protection	The fifth maximum protection	The second maximum protection	The maximum protection	The third maximum protection	The fourth maximum protection
67	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
68	The minimum protection	The second maximum protection	The maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
69	The minimum protection	The sixth maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The maximum protection	The second maximum protection
70	The minimum protection	The third maximum protection	The fourth maximum protection	The sixth maximum protection	The fifth maximum protection	The second maximum protection	The maximum protection
71	The minimum protection	The sixth maximum protection	The fifth maximum protection	The maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection
72	The minimum protection	The maximum protection	The sixth maximum protection	The fourth maximum protection	The third maximum protection	The fifth maximum protection	The second maximum protection
73	No answer	No answer	No answer	No answer	No answer	No answer	No answer

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
74	The minimum protection	The third maximum protection	The fourth maximum protection	The maximum protection	The fifth maximum protection	The second maximum protection	The sixth maximum protection
75	The minimum protection	The fourth maximum protection	The fifth maximum protection	The maximum protection	The third maximum protection	The second maximum protection	The sixth maximum protection
76	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
77	The maximum protection	The minimum protection	The sixth maximum protection	The third maximum protection	The second maximum protection	The fifth maximum protection	The fourth maximum protection
78	The third maximum protection	The minimum protection	The second maximum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection	The maximum protection
79	The minimum protection	The maximum protection	The second maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The sixth maximum protection
80	The minimum protection	The second maximum protection	The maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
81	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
82	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The sixth maximum protection	The fifth maximum protection
83	The third maximum protection	The fourth maximum protection	The maximum protection	The second maximum protection	The sixth maximum protection	The minimum protection	The fifth maximum protection
84	The maximum protection	The second maximum protection	The minimum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The sixth maximum protection
85	The minimum protection	The second maximum protection	The fifth maximum protection	The maximum protection	The sixth maximum protection	The fourth maximum protection	The third maximum protection
86	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The second maximum protection	The maximum protection	The third maximum protection
87	No answer	No answer	No answer	No answer	No answer	No answer	No answer
88	The maximum protection	The second maximum protection	The fourth maximum protection	The minimum protection	The fifth maximum protection	The third maximum protection	The sixth maximum protection
89	No answer	No answer	No answer	No answer	No answer	No answer	No answer
90	The third maximum protection	The maximum protection	The fourth maximum protection	The second maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
91	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection	The maximum protection
92	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
93	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
94	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
95	No answer	No answer	No answer	No answer	No answer	No answer	No answer
96	The second maximum protection	The third maximum protection	The fourth maximum protection	The maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
97	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
98	The maximum protection	The third maximum protection	The second maximum protection	The fourth maximum protection	The minimum protection	The fifth maximum protection	The sixth maximum protection
99	The maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection	The minimum protection	The second maximum protection
100	The minimum protection	The fourth maximum protection	The maximum protection	The second maximum protection	The fifth maximum protection	The third maximum protection	The sixth maximum protection
101	The minimum protection	The maximum protection	The second maximum protection	The sixth maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection
102	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
103	The sixth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The fifth maximum protection	The minimum protection
104	The minimum protection	The sixth maximum protection	The third maximum protection	The fifth maximum protection	The maximum protection	The fourth maximum protection	The second maximum protection
105	The minimum protection	The maximum protection	The third maximum protection	The fourth maximum protection	The fifth maximum protection	The second maximum protection	The sixth maximum protection
106	No answer	No answer	No answer	No answer	No answer	No answer	No answer
107	No answer	No answer	No answer	No answer	No answer	No answer	No answer
108	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The second maximum protection	The maximum protection	The third maximum protection
109	The third maximum protection	The second maximum protection	The fourth maximum protection	The maximum protection	The fifth maximum protection	The minimum protection	The sixth maximum protection
110	No answer	No answer	No answer	No answer	No answer	No answer	No answer
111	No answer	No answer	No answer	No answer	No answer	No answer	No answer
112	The minimum protection	The sixth maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection	The maximum protection	The fifth maximum protection
113	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
114	The minimum protection	The maximum protection	The second maximum protection	The sixth maximum protection	The fifth maximum protection	The third maximum protection	The fourth maximum protection

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
115	The minimum protection	The sixth maximum protection	The fourth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection
116	The minimum protection	The sixth maximum protection	The third maximum protection	The second maximum protection	The fifth maximum protection	The maximum protection	The fourth maximum protection
117	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
118	The fourth maximum protection	The fifth maximum protection	The third maximum protection	The sixth maximum protection	The minimum protection	The maximum protection	The second maximum protection
119	No answer	No answer	No answer	No answer	No answer	No answer	No answer
120	No answer	No answer	No answer	No answer	No answer	No answer	No answer
121	The minimum protection	The fifth maximum protection	The sixth maximum protection	The fourth maximum protection	The third maximum protection	The maximum protection	The second maximum protection
122	The maximum protection	The fifth maximum protection	The sixth maximum protection	The second maximum protection	The minimum protection	The third maximum protection	The fourth maximum protection
123	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
124	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
125	The minimum protection	The sixth maximum protection	The fifth maximum protection	The third maximum protection	The second maximum protection	The maximum protection	The fourth maximum protection
126	No answer	No answer	No answer	No answer	No answer	No answer	No answer
127	The minimum protection	The maximum protection	The third maximum protection	The sixth maximum protection	The fourth maximum protection	The fifth maximum protection	The second maximum protection
128	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
129	The maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The fifth maximum protection	The minimum protection	The sixth maximum protection
130	The minimum protection	The maximum protection	The third maximum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The second maximum protection
131	The minimum protection	The fifth maximum protection	The sixth maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection	The maximum protection
132	The maximum protection	The second maximum protection	The fourth maximum protection	The minimum protection	The third maximum protection	The sixth maximum protection	The fifth maximum protection
133	No answer	No answer	No answer	No answer	No answer	No answer	No answer
134	The minimum protection	The fourth maximum protection	The maximum protection	The sixth maximum protection	The fifth maximum protection	The third maximum protection	The second maximum protection
135	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
136	The fourth maximum protection	The maximum protection	The second maximum protection	The fifth maximum protection	The minimum protection	The sixth maximum protection	The third maximum protection
137	The fourth maximum protection	The third maximum protection	The second maximum protection	The maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
138	The minimum protection	The fifth maximum protection	The second maximum protection	The maximum protection	The sixth maximum protection	The fourth maximum protection	The third maximum protection
139	The minimum protection	The fourth maximum protection	The third maximum protection	The second maximum protection	The maximum protection	The sixth maximum protection	The fifth maximum protection
140	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
141	The sixth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The minimum protection	The fifth maximum protection
142	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
143	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The maximum protection	The minimum protection	The third maximum protection	The second maximum protection
144	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The sixth maximum protection	The fourth maximum protection	The fifth maximum protection
145	The third maximum protection	The second maximum protection	The fourth maximum protection	The maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
146	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
147	The fifth maximum protection	The sixth maximum protection	The minimum protection	The maximum protection	The fourth maximum protection	The second maximum protection	The third maximum protection
148	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The maximum protection	The second maximum protection
149	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
150	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
151	The minimum protection	The sixth maximum protection	The fifth maximum protection	The maximum protection	The third maximum protection	The second maximum protection	The fourth maximum protection
152	The fourth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
153	No answer	No answer	No answer	No answer	No answer	No answer	No answer
154	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
155	No answer	No answer	No answer	No answer	No answer	No answer	No answer
156	No answer	No answer	No answer	No answer	No answer	No answer	No answer

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
157	No answer	No answer	No answer	No answer	No answer	No answer	No answer
158	No answer	No answer	No answer	No answer	No answer	No answer	No answer
159	The minimum protection	The maximum protection	The third maximum protection	The second maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection
160	The fifth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The sixth maximum protection	The minimum protection
161	The second maximum protection	The minimum protection	The maximum protection	The sixth maximum protection	The fifth maximum protection	The third maximum protection	The fourth maximum protection
162	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
163	No answer	No answer	No answer	No answer	No answer	No answer	No answer
164	No answer	No answer	No answer	No answer	No answer	No answer	No answer
165	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
166	The minimum protection	The second maximum protection	The maximum protection	The third maximum protection	The fourth maximum protection	The sixth maximum protection	The fifth maximum protection
167	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
168	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
169	No answer	No answer	No answer	No answer	No answer	No answer	No answer
170	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
171	No answer	No answer	No answer	No answer	No answer	No answer	No answer
172	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
173	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
174	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
175	The maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The fifth maximum protection	The minimum protection	The sixth maximum protection
176	The maximum protection	The fourth maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
177	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
178	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
179	The minimum protection	The maximum protection	The second maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The sixth maximum protection
180	The minimum protection	The fifth maximum protection	The second maximum protection	The fourth maximum protection	The third maximum protection	The maximum protection	The sixth maximum protection

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
181	The minimum protection	The maximum protection	The sixth maximum protection	The fifth maximum protection	The third maximum protection	The second maximum protection	The fourth maximum protection
182	The fourth maximum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
183	The second maximum protection	The third maximum protection	The maximum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection
184	The sixth maximum protection	The fifth maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The maximum protection	The minimum protection
185	The minimum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The second maximum protection	The maximum protection	The fifth maximum protection
186	No answer	No answer	No answer	No answer	No answer	No answer	No answer
187	The minimum protection	The sixth maximum protection	The fifth maximum protection	The fourth maximum protection	The third maximum protection	The maximum protection	The second maximum protection
188	No answer	No answer	No answer	No answer	No answer	No answer	No answer
189	The minimum protection	The third maximum protection	The maximum protection	The fourth maximum protection	The second maximum protection	The fifth maximum protection	The sixth maximum protection
190	The minimum protection	The fifth maximum protection	The third maximum protection	The fourth maximum protection	The sixth maximum protection	The maximum protection	The second maximum protection
191	The minimum protection	The maximum protection	The fifth maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection	The second maximum protection
192	No answer	No answer	No answer	No answer	No answer	No answer	No answer
193	The minimum protection	The fourth maximum protection	The sixth maximum protection	The second maximum protection	The fifth maximum protection	The third maximum protection	The maximum protection
194	The fourth maximum protection	The third maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection	The second maximum protection	The maximum protection
195	The third maximum protection	The fourth maximum protection	The fifth maximum protection	The sixth maximum protection	The minimum protection	The second maximum protection	The maximum protection
196	The minimum protection	The fourth maximum protection	The third maximum protection	The maximum protection	The fifth maximum protection	The sixth maximum protection	The second maximum protection
197	No answer	No answer	No answer	No answer	No answer	No answer	No answer
198	uncompleted	uncompleted	uncompleted	uncompleted	uncompleted	uncompleted	uncompleted
199	No answer	No answer	No answer	No answer	No answer	No answer	No answer
200	No answer	No answer	No answer	No answer	No answer	No answer	No answer
201	The minimum protection	The sixth maximum protection	The fifth maximum protection	The second maximum protection	The fourth maximum protection	The maximum protection	The third maximum protection

Respondent's ID	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7
202	The maximum protection	The minimum protection	The sixth maximum protection	The second maximum protection	The fourth maximum protection	The fifth maximum protection	The third maximum protection
203	No answer	No answer	No answer	No answer	No answer	No answer	No answer
204	No answer	No answer	No answer	No answer	No answer	No answer	No answer
205	No answer	No answer	No answer	No answer	No answer	No answer	No answer
206	No answer	No answer	No answer	No answer	No answer	No answer	No answer
207	The minimum protection	The sixth maximum protection	The fifth maximum protection	The second maximum protection	The third maximum protection	The fourth maximum protection	The maximum protection
208	The minimum protection	The maximum protection	The second maximum protection	The fourth maximum protection	The fifth maximum protection	The third maximum protection	The sixth maximum protection
209	The minimum protection	The maximum protection	The second maximum protection	The third maximum protection	The fifth maximum protection	The fourth maximum protection	The sixth maximum protection

Part 3: Respondents' trust in online banking security system

Respondent's ID	D9.1	D9.2	D9.3	D9.4	D9.5	D9.6	D9.7	D9.8
1	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
3	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
4	strongly believe	believe	believe	neither	neither	believe	believe	strongly believe
5	neither	neither	neither	believe	not believe	neither	not believe	believe
6	believe	believe	believe	believe	not believe	strongly believe	strongly believe	strongly believe
7	believe	believe	believe	neither	neither	believe	strongly believe	believe
8	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
9	believe	neither	believe	No answer	believe	believe	strongly believe	No answer
10	believe	believe	strongly believe	neither	strongly not believe	neither	neither	believe
11	believe	believe	believe	neither	neither	believe	neither	strongly believe
12	neither	neither	believe	not believe	not believe	neither	believe	strongly believe
13	neither	neither	believe	strongly not believe	believe	believe	strongly believe	strongly believe
14	believe	believe	believe	not believe	believe	believe	neither	believe
15	believe	neither	believe	not believe	strongly believe	strongly believe	strongly believe	neither

Respondent's ID	D9.1	D9.2	D9.3	D9.4	D9.5	D9.6	D9.7	D9.8
16	believe	believe	believe	neither	neither	believe	neither	neither
17	strongly not believe	neither	neither	believe	neither	believe	believe	strongly believe
18	neither	neither	believe	neither	believe	not believe	believe	believe
19	believe	neither	believe	believe	believe	believe	believe	strongly believe
20	neither	believe	strongly believe	neither	believe	strongly believe	neither	neither
21	neither	neither	neither	not believe	neither	believe	strongly believe	strongly believe
22	neither	believe	believe	believe	neither	believe	believe	neither
23	neither	believe	believe	believe	neither	believe	not believe	believe
24	believe	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe	believe	believe
25	neither	not believe	strongly believe	No answer	No answer	believe	strongly not believe	No answer
26	strongly believe	neither	believe	believe	not believe	neither	neither	not believe
27	strongly believe	believe	strongly believe	believe	believe	strongly believe	strongly believe	believe
28	neither	not believe	neither	neither	neither	believe	believe	strongly believe
29	neither	neither	believe	not believe	strongly not believe	believe	strongly believe	strongly believe
30	not believe	believe	believe	not believe	not believe	believe	strongly believe	believe
31	believe	strongly believe	believe	strongly believe	neither	believe	believe	believe
32	neither	neither	neither	believe	not believe	believe	not believe	believe
33	believe	believe	believe	not believe	neither	believe	believe	believe
34	neither	believe	believe	believe	neither	believe	believe	believe
35	neither	not believe	believe	believe	not believe	believe	believe	believe
36	neither	believe	believe	neither	neither	No answer	believe	believe
37	not believe	believe	believe	neither	neither	not believe	neither	strongly not believe
38	believe	believe	believe	not believe	neither	believe	strongly believe	strongly believe
39	believe	strongly believe	not believe	believe	strongly believe	No answer	neither	believe
40	neither	believe	believe	believe	not believe	believe	believe	strongly believe
41	neither	not believe	not believe	not believe	neither	neither	strongly not believe	not believe
42	believe	neither	not believe	strongly believe	strongly not believe	neither	believe	strongly believe

Respondent's ID	D9.1	D9.2	D9.3	D9.4	D9.5	D9.6	D9.7	D9.8
43	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
44	neither	neither	believe	believe	strongly believe	believe	neither	neither
45	believe	neither	believe	believe	believe	believe	believe	believe
46	believe	believe	believe	believe	neither	believe	believe	neither
47	believe	neither	believe	believe	strongly believe	neither	strongly believe	neither
48	neither	neither	neither	believe	not believe	neither	not believe	believe
49	strongly not believe	not believe	not believe	not believe	believe	believe	neither	believe
50	neither	neither	neither	not believe	strongly not believe	neither	strongly believe	strongly believe
51	neither	neither	believe	not believe	strongly not believe	neither	not believe	believe
52	believe	believe	believe	neither	neither	believe	believe	believe
53	believe	believe	believe	neither	neither	believe	believe	believe
54	neither	believe	believe	not believe	believe	believe	believe	neither
55	believe	strongly believe	strongly believe	strongly believe	believe	strongly believe	strongly believe	strongly believe
56	believe	strongly believe	strongly believe	believe	not believe	believe	believe	strongly believe
57	believe	believe	believe	not believe	believe	neither	strongly believe	strongly believe
58	believe	believe	believe	not believe	neither	neither	believe	believe
59	strongly believe	strongly believe	strongly believe	believe	believe	believe	strongly believe	neither
60	believe	believe	believe	believe	neither	believe	believe	believe
61	believe	believe	neither	strongly not believe	not believe	neither	No answer	No answer
62	believe	believe	believe	believe	strongly not believe	believe	neither	neither
63	believe	believe	believe	neither	strongly not believe	strongly believe	believe	strongly believe
64	strongly believe	strongly believe	believe	believe	neither	believe	strongly believe	strongly believe
65	neither	neither	neither	strongly not believe	neither	neither	strongly believe	strongly believe
66	neither	believe	neither	neither	neither	neither	believe	believe
67	strongly believe	strongly not believe	neither	strongly not believe	strongly believe	not believe	believe	believe
68	strongly believe	believe	believe	neither	strongly believe	believe	believe	neither
69	neither	not believe	not believe	strongly not believe	strongly not believe	not believe	believe	neither
70	strongly not believe	strongly not believe	not believe	strongly not believe	not believe	not believe	believe	strongly believe

Respondent's ID	D9.1	D9.2	D9.3	D9.4	D9.5	D9.6	D9.7	D9.8
71	not believe	not believe	believe	believe	neither	believe	neither	strongly believe
72	believe	strongly believe	strongly believe	believe	strongly not believe	believe	believe	neither
73	believe	strongly believe	believe	not believe	believe	believe	believe	believe
74	neither	neither	neither	strongly not believe	neither	neither	strongly believe	strongly believe
75	believe	believe	strongly believe	strongly not believe	believe	believe	believe	strongly believe
76	believe	believe	believe	neither	not believe	believe	not believe	neither
77	believe	believe	believe	strongly believe	strongly believe	strongly believe	neither	neither
78	believe	believe	believe	believe	neither	believe	strongly believe	believe
79	neither	believe	believe	neither	believe	neither	believe	believe
80	believe	believe	believe	neither	neither	believe	believe	believe
81	believe	believe	strongly believe	believe	believe	strongly believe	neither	believe
82	neither	neither	neither	believe	not believe	neither	not believe	believe
83	believe	believe	neither	neither	not believe	believe	not believe	neither
84	neither	believe	believe	believe	believe	believe	neither	neither
85	believe	believe	strongly believe	believe	believe	strongly believe	strongly believe	strongly believe
86	believe	believe	strongly believe	neither	believe	believe	strongly believe	strongly believe
87	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
88	not believe	not believe	not believe	not believe	not believe	neither	not believe	not believe
89	strongly believe	strongly believe	strongly believe	No answer	No answer	No answer	No answer	strongly believe
90	strongly not believe	strongly not believe	strongly not believe	neither	not believe	strongly not believe	strongly not believe	strongly not believe
91	strongly believe	strongly believe	strongly believe	believe	believe	strongly believe	strongly believe	strongly believe
92	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
93	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
94	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
95	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
96	believe	believe	believe	believe	neither	believe	believe	neither
97	believe	strongly believe	believe	believe	strongly believe	believe	strongly believe	strongly believe

Respondent's ID	D9.1	D9.2	D9.3	D9.4	D9.5	D9.6	D9.7	D9.8
98	not believe	neither	believe	neither	strongly believe	strongly believe	strongly believe	strongly believe
99	believe	strongly believe	believe	believe	not believe	strongly believe	strongly believe	strongly believe
100	believe	believe	believe	not believe	neither	neither	believe	believe
101	believe	believe	believe	strongly not believe	believe	believe	not believe	neither
102	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
103	neither	neither	neither	neither	neither	neither	neither	neither
104	neither	neither	believe	neither	strongly believe	believe	neither	believe
105	neither	believe	believe	neither	neither	believe	strongly believe	believe
106	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
107	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
108	believe	believe	believe	believe	not believe	believe	believe	believe
109	not believe	neither	believe	strongly believe	No answer	No answer	strongly not believe	No answer
110	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
111	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
112	believe	believe	believe	not believe	strongly not believe	believe	strongly not believe	strongly believe
113	neither	neither	neither	not believe	not believe	believe	believe	strongly believe
114	neither	strongly believe	believe	strongly not believe	neither	believe	believe	believe
115	believe	believe	believe	believe	not believe	believe	believe	believe
116	neither	neither	believe	strongly not believe	not believe	No answer	strongly believe	strongly believe
117	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
118	neither	neither	not believe	neither	not believe	neither	believe	neither
119	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
120	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
121	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe
122	not believe	not believe	neither	not believe	strongly not believe	not believe	strongly not believe	not believe
123	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
124	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
125	believe	believe	strongly believe	not believe	not believe	believe	strongly believe	strongly believe

Respondent's ID	D9.1	D9.2	D9.3	D9.4	D9.5	D9.6	D9.7	D9.8
126	strongly not believe	not believe	neither	strongly not believe	strongly not believe	neither	strongly believe	strongly believe
127	believe	believe	believe	neither	neither	neither	believe	strongly believe
128	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
129	neither	not believe	not believe	strongly believe	strongly not believe	not believe	strongly believe	strongly believe
130	believe	believe	believe	not believe	believe	believe	strongly believe	strongly believe
131	neither	neither	believe	neither	neither	believe	believe	strongly believe
132	neither	neither	believe	neither	neither	neither	neither	believe
133	strongly believe	strongly believe	strongly believe	not believe	strongly not believe	strongly believe	strongly believe	strongly believe
134	strongly believe	believe	strongly believe	neither	neither	strongly believe	neither	neither
135	believe	believe	believe	believe	believe	believe	believe	neither
136	neither	neither	believe	neither	neither	neither	neither	believe
137	believe	believe	believe	believe	neither	believe	believe	believe
138	neither	not believe	believe	neither	neither	neither	strongly believe	believe
139	neither	strongly believe	strongly believe	No answer	believe	strongly believe	strongly believe	strongly believe
140	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
141	strongly believe	strongly believe	believe	believe	believe	believe	strongly believe	strongly believe
142	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
143	neither	neither	not believe	not believe	not believe	neither	not believe	strongly believe
144	believe	believe	believe	neither	neither	believe	believe	believe
145	believe	believe	believe	believe	believe	believe	believe	believe
146	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
147	neither	neither	believe	neither	not believe	neither	not believe	not believe
148	believe	believe	believe	believe	not believe	believe	believe	believe
149	believe	believe	neither	neither	neither	believe	believe	believe
150	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
151	neither	neither	neither	neither	neither	neither	neither	neither
152	neither	neither	neither	neither	neither	neither	believe	strongly believe
153	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
154	strongly believe	strongly believe	strongly believe	believe	strongly believe	strongly believe	believe	believe
155	strongly believe	strongly believe	strongly believe	strongly believe	believe	strongly believe	strongly believe	strongly believe

Respondent's ID	D9.1	D9.2	D9.3	D9.4	D9.5	D9.6	D9.7	D9.8
156	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
157	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
158	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
159	believe	believe	neither	not believe	not believe	neither	believe	believe
160	not believe	not believe	not believe	believe	strongly not believe	not believe	neither	neither
161	believe	believe	believe	neither	believe	believe	believe	neither
162	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
163	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
164	believe	neither	neither	neither	strongly not believe	believe	neither	neither
165	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
166	neither	not believe	neither	neither	strongly not believe	neither	neither	strongly believe
167	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
168	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
169	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
170	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
171	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
172	strongly believe	strongly believe	believe	believe	neither	believe	believe	believe
173	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
174	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
175	neither	neither	neither	neither	neither	believe	not believe	strongly believe
176	believe	believe	believe	not believe	neither	believe	believe	believe
177	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
178	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
179	strongly believe	strongly believe	strongly believe	not believe	believe	believe	believe	neither
180	not believe	not believe	not believe	believe	believe	not believe	neither	neither
181	neither	believe	believe	not believe	neither	believe	strongly believe	strongly believe
182	believe	believe	neither	believe	strongly believe	strongly believe	strongly believe	not believe
183	neither	neither	neither	neither	neither	neither	neither	neither
184	not believe	not believe	not believe	neither	not believe	strongly not believe	strongly not believe	neither
185	believe	believe	neither	not believe	neither	neither	neither	strongly believe
186	not believe	not believe	not believe	believe	believe	neither	strongly believe	neither

Respondent's ID	D9.1	D9.2	D9.3	D9.4	D9.5	D9.6	D9.7	D9.8
187	believe	believe	strongly believe	strongly believe	strongly believe	believe	strongly believe	strongly believe
188	No answer	neither	believe	strongly not believe	strongly not believe	neither	not believe	strongly believe
189	neither	not believe	believe	strongly not believe	not believe	believe	strongly believe	strongly believe
190	believe	strongly believe	strongly believe	neither	not believe	believe	believe	strongly believe
191	neither	believe	believe	neither	neither	believe	strongly believe	strongly believe
192	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
193	believe	believe	neither	neither	neither	believe	strongly believe	believe
194	strongly believe	believe	neither	not believe	No answer	No answer	No answer	strongly not believe
195	strongly believe	believe	neither	not believe	strongly not believe	not believe	not believe	neither
196	neither	not believe	neither	strongly not believe	not believe	believe	neither	believe
197	believe	neither	neither	neither	neither	believe	believe	believe
198	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
199	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
200	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe	strongly believe
201	strongly believe	believe	neither	not believe	believe	neither	believe	neither
202	believe	believe	believe	neither	neither	believe	neither	neither
203	neither	not believe	not believe	not believe	neither	neither	neither	believe
204	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
205	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
206	believe	neither	neither	believe	neither	believe	believe	believe
207	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
208	believe	believe	believe	neither	believe	strongly believe	strongly believe	strongly believe
209	believe	believe	believe	believe	believe	believe	believe	strongly believe

Part 4: Respondents' security system preferences

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
1	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
3	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
4	I agree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither	Neither
5	I agree	I agree	I agree	I agree	I agree	I strongly agree	Neither	I strongly agree
6	I strongly agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I agree	I agree
7	I strongly agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
8	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
9	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
10	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
11	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
12	Disagree	Disagree	I agree	I strongly agree	I strongly agree	Disagree	I strongly agree	I strongly agree
13	I strongly agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
14	Neither	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
15	I strongly agree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
16	Disagree	Disagree	I agree	No answer	I strongly agree	I strongly agree	I agree	I agree
17	I agree	I agree	I strongly agree	I agree	I agree	I strongly agree	Neither	I agree
18	I strongly agree	I strongly agree	I strongly agree	Disagree	I strongly agree	I strongly agree	Neither	I strongly agree
19	I strongly agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I agree	I strongly agree
20	Disagree	I agree	Neither	I strongly agree	I agree	Neither	I agree	I agree
21	I strongly agree	Neither	I agree	I strongly agree	I strongly agree	I strongly agree	I agree	Neither
22	I agree	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	Neither	I agree
23	I strongly agree	Neither	I agree	I strongly agree	I strongly agree	I strongly agree	I agree	I strongly agree
24	I agree	I strongly disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
25	No answer	I agree	Disagree	No answer	I strongly agree	I strongly disagree	Disagree	No answer
26	I strongly agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
27	I strongly agree	Neither	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly disagree	I strongly agree
28	I agree	Disagree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither
29	Neither	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly disagree	I strongly disagree
30	I strongly agree	I strongly disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree
31	I strongly agree	I strongly agree	I agree	I strongly disagree	I strongly agree	I strongly agree	I strongly agree	I agree
32	I strongly agree	I agree	Neither	I strongly agree	I agree	I agree	Disagree	Neither
33	I strongly agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
34	I agree	I agree	I agree	I strongly agree	I agree	I strongly agree	I strongly agree	I strongly agree
35	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
36	I strongly agree	I agree	I agree	Neither	Neither	I strongly agree	Neither	I strongly agree
37	I agree	I strongly disagree	Disagree	I strongly disagree	I strongly disagree	I strongly disagree	I strongly disagree	I strongly disagree
38	I agree	I agree	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree
39	I strongly agree	I strongly agree	I agree	Neither	Disagree	I strongly agree	I strongly agree	I agree
40	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
41	I agree	I agree	I strongly agree	Neither	Neither	I strongly agree	I agree	I agree
42	I agree	I agree	I agree	Disagree	I strongly agree	I strongly agree	Disagree	I agree
43	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
44	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
45	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
46	Neither	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
47	I agree	Disagree	I strongly disagree	I strongly agree	Neither	I strongly agree	I strongly agree	Disagree

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
48	Neither	Neither	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
49	Disagree	Disagree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I agree
50	Neither	Neither	Neither	Neither	Neither	I strongly agree	Neither	I agree
51	I agree	Disagree	I agree	Neither	I agree	I strongly agree	I strongly agree	I strongly agree
52	I agree	I strongly agree	Neither	I strongly agree	Disagree	I strongly agree	I strongly agree	I strongly agree
53	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree	I strongly agree	Neither	I strongly agree
54	No answer	I agree	I agree	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree
55	I strongly agree	Neither	I agree	I strongly disagree	I strongly agree	I strongly agree	I strongly disagree	I strongly disagree
56	Disagree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
57	I strongly agree	Disagree	I strongly agree	I strongly disagree	I strongly agree	I strongly agree	I agree	I strongly agree
58	I strongly agree	I strongly agree	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree
59	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
60	I strongly agree	Neither	I agree	I strongly agree	I strongly agree	I agree	I agree	I strongly agree
61	I agree	Neither	I strongly agree	Neither	Neither	I strongly agree	I strongly agree	I strongly agree
62	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
63	I agree	Disagree	I strongly agree	Disagree	I strongly agree	I strongly agree	Disagree	I strongly agree
64	Neither	Neither	I strongly disagree	Disagree	Neither	I strongly agree	Disagree	Disagree
65	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
66	I agree	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
67	I agree	I strongly disagree	I strongly agree	I strongly disagree	I strongly disagree	I strongly agree	I strongly agree	I strongly agree
68	I agree	I strongly disagree	I agree	Neither	Disagree	I agree	I strongly disagree	I strongly agree
69	Neither	Neither	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly disagree	I strongly agree
70	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
71	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree
72	Neither	I strongly disagree	Neither	I agree	Neither	I strongly agree	Neither	I agree
73	Neither	Disagree	I agree	I agree	I agree	I strongly agree	Neither	I agree
74	I strongly agree	Neither	I strongly agree	Neither	I strongly agree	I strongly agree	No answer	I strongly agree
75	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
76	Disagree	Disagree	I agree	I agree	I agree	I strongly agree	Neither	Neither
77	I agree	I agree	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree
78	I agree	Neither	I agree	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree
79	I agree	Neither	I agree	I agree	I agree	I agree	I agree	I agree
80	I strongly agree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
81	I strongly agree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I agree	Disagree
82	I agree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
83	Neither	I strongly disagree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
84	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
85	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly disagree	I strongly disagree	I strongly disagree
86	I agree	Disagree	I agree	Disagree	I strongly agree	I strongly agree	Disagree	I agree
87	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
88	Disagree	I strongly agree	Disagree	I strongly agree	I strongly agree	I strongly agree	Disagree	I agree
89	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
90	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
91	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
92	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
93	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
94	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
95	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
96	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree
97	I strongly agree	Neither	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree	Neither
98	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
99	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Disagree	Disagree
100	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
101	Neither	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
102	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
103	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
104	I strongly agree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
105	I strongly agree	I agree	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree
106	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
107	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
108	Disagree	Disagree	Disagree	I agree	I agree	I agree	Neither	I agree
109	I strongly disagree	I strongly agree	I agree	Neither	Disagree	No answer	No answer	No answer
110	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
111	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
112	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree
113	I agree	I agree	I agree	Neither	Neither	I agree	I agree	I strongly agree
114	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
115	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Disagree	Neither
116	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
117	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
118	I agree	Neither	Neither	Disagree	I agree	Neither	Neither	Neither
119	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
120	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
121	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
122	I strongly agree	I strongly agree	Neither	I agree	I strongly disagree	I strongly disagree	I strongly disagree	I strongly disagree
123	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
124	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
125	Disagree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
126	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
127	I strongly agree	I strongly agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither
128	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
129	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
130	I strongly agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
131	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree	Neither	Disagree	Disagree
132	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
133	I strongly agree	Disagree	I agree	I strongly agree	I strongly agree	Disagree	Neither	I strongly disagree
134	Neither	Disagree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
135	Disagree	Disagree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
136	Neither	Disagree	I agree	I agree	I agree	I agree	Neither	I agree
137	I strongly agree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
138	I strongly agree	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
139	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
140	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
141	I strongly agree	Disagree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
142	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
143	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	No answer
144	I agree	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I agree
145	I strongly agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
146	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
147	I agree	Disagree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
148	I agree	I agree	I agree	I agree	I agree	I agree	I agree	I agree
149	I agree	Disagree	I agree	I agree	I agree	I strongly agree	I strongly agree	Disagree
150	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
151	I strongly disagree	Neither	I strongly disagree	I strongly disagree	I strongly disagree	I strongly disagree	I strongly disagree	I strongly disagree
152	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree
153	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
154	Neither	I strongly disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
155	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree
156	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
157	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
158	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
159	I strongly agree	I strongly disagree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
160	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
161	Disagree	Disagree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
162	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
163	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
164	Neither	Neither	Neither	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree
165	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
166	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
167	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
168	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
169	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
170	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
171	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
172	I strongly agree	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I agree

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
173	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
174	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
175	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
176	I agree	I agree	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree
177	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
178	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
179	Disagree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
180	I agree	Disagree	Neither	I agree	I agree	I agree	Disagree	Disagree
181	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I agree	I strongly agree
182	Neither	I strongly disagree	Neither	I strongly agree	Neither	I strongly agree	I strongly agree	I strongly agree
183	Neither	I agree	Neither	No answer	Neither	Neither	I agree	Neither
184	I agree	Disagree	I agree	I strongly agree	I strongly agree	I agree	I agree	I agree
185	I agree	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I agree
186	I agree	Neither	I agree	I agree	I agree	I agree	I agree	I agree
187	I strongly agree	I strongly agree	I strongly agree	I agree	I agree	I agree	I strongly agree	I strongly agree
188	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
189	I agree	Disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
190	I strongly agree	Disagree	Neither	Neither	Neither	I strongly agree	Disagree	Neither
191	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Neither	I strongly agree
192	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
193	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
194	Neither	I agree	No answer	I strongly agree	Disagree	I strongly disagree	No answer	No answer
195	I strongly agree	No answer	No answer	No answer	No answer	No answer	No answer	No answer
196	Neither	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
197	I agree	I agree	Neither	Neither	Disagree	I agree	Neither	I agree
198	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer

Respondent's ID	D10.1	D10.2	D10.3	D10.4	D10.5	D10.6	D10.7	D10.8
199	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
200	I agree	I strongly agree	I agree	I agree	I agree	I agree	Neither	I strongly agree
201	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I agree	I strongly agree
202	I agree	Disagree	I agree	I agree	I agree	I strongly agree	I agree	Neither
203	I agree	I agree	I agree	I agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree
204	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
205	No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
206	I agree	I agree	Neither	I agree	I agree	I strongly agree	I strongly agree	I strongly agree
207	I agree	I agree	I agree	I agree	I agree	Disagree	I strongly agree	I strongly agree
208	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	Disagree	I strongly agree
209	I strongly agree	I strongly disagree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree	I strongly agree

Respondent's ID	D11
6	"I have no opinion."
7	"It's been revolutionary for worldwide navel and ease of banking & paying bills."
9	"My bank provides many security measures so it's unfair for me to rate as I don't know what other security measures that bank offers."
10	"I always triple check the screen to identify the log in status (i.e.) [You are currently logged out] perhaps this screen can be clearer to promote a sense of security leaving/exiting the banks screen/ or computer."
13	"I have no opinion."
15	"Educating people about online security."
16	"I have no opinion."
17	"Banks should try to update their security every time."
18	"I think the bank should offer more questions to us to answer when we open an account."
19	"Banks should provide any strong security online service."
20	"I have no opinion."
21	"Account security is really important to every customer, so if the basic requirement for security cannot be reached, no one will trust online banking system."
22	"I have no opinion."
24	"Not more than I know that if banks could motivate their customers to use bank services online. They will save millions of dollars. So it is in their interests. European bank somewhat is better than Australian bank."
25	"If hacker hacks my bank account I will stop using this bank."
26	"I have no opinion."
27	"I have no opinion."
28	Online banking service is very convenient service for me. However, the rank of bank based on the level of security protection. It will be the main reason for chasing up bank.
31	"The bank must do something after someone's money in his account was stolen."
32	"Improve our knowledge of Internet."
34	"I have no opinion."
37	"My bank should prompt me with a security question, such as 'what is your mother's maiden name?' every time I log on to my online banking account."
40	"Very convenient. Haven't access into a bank in over 6 months-very happy about that, but do get worried sometimes about Internet banking security."
41	"Police or other should find the reason when people are attacked and then give them some solutions."
42	"Online banking provides us convenience."
45	"I find online banking is very convenient to use. I enjoy using it and it allows me to pay my bills at any time of the day."
46	"Banks need to educate their users but not make it too hard because then people won't use it."
47	"When using online banking, if you have credit cards you should always keep a close eye on your transactions especially if you shop online."
48	"A difficult situation-ease of use versus security. If banks make it difficult or inconvenient, people will stop using the facility. They also cannot rely on individuals to have the knowledge or education to take multiple precautions with their personal information. Therefore, banks need to ensure max level of security exist from their end. If they provide the service then responsibility for security falls legally in their domain."
51	"I have no opinion."
55	"I have no opinion."

Respondent's ID	D11
56	"Banks need to increase security to keep up with level of attacks etc. They need to stay competitive so should do this to prevent & retain customers. Banks make phenomenal profits- they should use some of this to protect their customers."
58	"I have no opinion."
59	"Online banking is acceptable to me because as I work full time, I am not able to go into a bank. I would however prefer not to use online banking."
60	"Online banking is very important to me. I use it often- is very convenient. I need it especially when travelling oversea. Banks need to be alert to any new scams that may occur."
62	"I have no opinion."
64	"I have no opinion."
65	"I hate having to use it, but it is life."
66	"I have no opinion."
71	"It is an extremely convenient way to bank; however, I believe that the security needs to be regularly reviewed by the banks to ensure its customers' accounts are safe from fraudulent activity."
73	"Feel safe so far. Bank guarantee to return stolen money, not in the bank interest to be unsecured."
74	"I have no opinion."
75	"I have no opinion."
77	"I have no opinion."
80	"Bank should promote security measures and efforts taken to ensure banking security to users. It should encourage user to be aware/ should their main website is secure/ should automatically deactivate any ongoing internet banking security immediately/ should a suspicious activity is detected."
83	"I have no opinion."
84	"I have no opinion."
86	"I have no opinion."
89	"Do not use the system overly much."
93	"Please improve more people not computers, profit & satisfaction or citizen will be as much as appreciation."
97	"I have no opinion."
101	"I have no opinion."
103	"I think it is a great facility, but it should be secure and the banks are responsible to our safety or delete the option of Internet banking."
105	"Hacking into bank accounts + identifying fraud to be a growing problem. So, Banks should be looking at new ways to increase security."
109	"My only problem with online banking is doing scam activity."
115	"The online banking should be secured but not compromised user friendliness."
116	"Generally satisfied with ANZ due to 'FALCON' system."
118	"I have no opinion."
121	"I have no opinion."
129	"This is very good survey concerning about online banking security. Bank and government should use this information to improve bank security and customer satisfaction."
130	"I would appreciate being continuously informed and educated about the best and cheapest computer security software available to me as I feel like a novice and don't know where to go to find the best security."
133	"I have no opinion."
155	"I have no opinion."

Respondent's ID	D11
163	"I would not use Internet banking. There is new scam daily."
179	"I have no opinion."
181	"I have no opinion."
184	"I have no opinion."

APPENDIX L: Data of respondents' interview

Respondent's ID	Knowledge about online banking threat (I1)
1	"Yes, through key loggers."
2	"No."
3	"Yes. Most of what I know come from the ASIC website, they have a hyperlink/webpage called Scam. I personally have received e-mail from people with long difficult to pronounce names saying that I have won a huge amount of money and that all they need is my bank account details."
4	"Yes, from media (online news stories) and my bank (warnings when logging into online banking).
5	Yes. E-mails to say that bank is changing your banking password. Click on link to make change. I never did log in or click on link so don't know what would have happened if I had."
6	"No."
7	"Client and needed customers banking details. Commonwealth Bank out a news announcement to stake this was a scam."
9	"Yes, I have a rental (holiday) property and I enquiry asked for my bank details to deposit money. This deposit was a scam from one bank to another."
10	"No. I have never heard of any threats."
11	"Yes, media. The e-mails sent asking your bank account to update info."
12	"I receive a lot of e-mails from friends."
13	"Certainly, I think it is a big threat for every banking sector including their customers."
14	"Nothing"
15	"Yes, spam e-mails that mislead some people to provide their online bank username and passwords then online theft can use that money to transfer online."
16	"I've heard of spam e-mails that ask for your username + passwords."
17	"Yes, it happened with my sister. Her credit card money was used by another person. Twice that third party got my sister's money. It was about $160 and $200."
18	"Yes, I have heard."
19	"Yes, I have. Always have some related information/news about online banking threat, and may be in order to raise our awareness of that."
20	"Yes, I have heard this from newspaper and on TV."
21	"Yes, bank security system attacks by hacker."
22	"No."
23	"I only watch this kind if threat in movies."
24	"Yes."
25	"Yes, I have heard about it."
26	"No."
27	"Yes, I have heard it. One of my friends' credit was used by one of American company."
28	"I've heard about hacking the computer system from media."
29	"Yes, fake e-mails from banks."
30	"I was on IT auditor (recently retired) so I am very conversant with the several threats. I worked in banking for 38+years."
31	"Yes, I always had seen that someone's online bank's code was stolen and lose a large number of money in the newspaper."
32	"No opinion"
33	"No."

Respondent's ID	**Knowledge about online banking threat (I1)**
34	"No."
35	"Warning from bank about false websites requesting account number, password etc."
36	"No. May be thing I will worry about is they system breakdown/ hacker attacks."
37	"No."
38	"No."
39	"Yes, transfer money."
40	"No."
41	"Yes, from friends."
42	"No."
44	"Scammers can get information through mail inside the website when the user enters their account information."
45	"Yes, fake e-mail asking for private/personal details."
46	"Yes, there are warnings about phishing scams on the bank homepage. Also, discussed at university."
47	"Yes, from the media about not giving away banking information via e-mail."
48	"Yes, ANZ reports of hackers put clients' accounts online. I have also received many requests for account information via both university and home e-mail."
49	"No."
50	"No."
51	"Yes, where e-mails are sent to people pretending to be from banks, asking them for their PIN and other information."
52	"No, I haven't."
53	"I have heard reports on the news (print and TV) of people hacking into online accounts and accessing people's funds/accountable /credit card etc."
54	"Yes."
55	"Yes."
56	"Yes, e-mail asking me for my details - if I don't respond, it could stop me from using my bank account. These e-mails seem to come from well-known banks."
57	"Yes, homepage of several of my accounts have warnings about phishing e-mails."
58	"Yes, it is from media I have heard that several times. It is about someone lost his/her money from the Internet banking because of the virus in their computer and let someone know their passwords."
59	"I have had an e-mail from my bank warning not to respond to any request per information as the bank will never ask this."
60	"From media, friends, and banks. Also, e-mail warning from employer. Banks issue warnings on website."
61	"No opinion"
62	"No."
64	"Yes, I've heard from bank advertisement."
65	"One of my friends got $600 withdrawn from her saving while paying for petrol of $50 something."
66	"I have heard the news from the Internet."
67	"Yes, they are phishing, spyware, Trojan horse, rootkit/backdoor, social engineering."
68	"I have received e-mail from my bank warning of phishing scams. My bank display warnings on its homepage."
69	"Spam/phishing e-mails from 'banks' where I don't have an account."
70	"No opinion"

Respondent's ID	**Knowledge about online banking threat (I1)**
71	"Yes, have heard through the media and had notifications from my bank. They informed us not to answer any e-mails asking for account verification."
72	"Yes, I have received warning from my bank that some e-mails ask for account details are fraudulent."
73	"Yes, from media only."
74	"Yes, mainly from media and from the bank. I often have e-mails directed to our business."
75	"I have heard that term phishing from my husband but still don't know much more about it."
77	"Yes, hacker attack, phishing website, suspect web link."
78	"I read an article that a number of years ago a computer in Asia were found to have all the customers banking details from a bank in Australia."
79	"Password security - things like phishing scams were you get an e-mail pretending to be from your bank asking for account details. Identity theft - dangers of discarding bank statements etc. without shredding. False webpages designed to look like bank webpages - try to get your account and password details."
80	"Yes. Banks have been promoting through online ads and television advertisement. Banks try to make online banking as convenient as possible, stressing on the ease of use and great accessibility having 24hrs access to one's own account."
81	"Yes, my sister has had her banking account "hacked" information before and a substantial amount stolen."
82	"Bank warns about fraudulent e-mails directing to false websites."
83	"Yes, I work in a bank and I've heard of other people hacking into personal accounts."
84	"Via Internet-browsing through travel forums and reading about how tourists have been targeted."
85	"No."
86	"Have received information from my bank requires internet banking and my user to change password."
102	"Yes."
106	"Yes."
107	"Yes, bogus e-mails requesting personal information."
111	"Yes, from media reports."
140	"Yes. Heard about isolated cases but I have been doing online banking for 15 years without problem. The token security is good and what's better is a sms notification of any transaction."
143	"No."
149	"Yes."
165	"Happened to a family's friend, fraud using PayPal. I've seen many reports on television."
177	"Yes, I have heard."
180	"From a friend originally from New Zealand. He said he gets phishing e-mails regularly."
181	"Yes, user's information was disclosed to online & tele-sales as [CONTACTS]."
183	"No."
187	"No."
188	"No."
189	"Yes. Fake website collecting personal and account information."
191	"No."
200	"Yes."
206	"No."
207	"Yes."

Respondent's ID	Knowledge about online banking threat (I1)
208	"No."
209	"Yes, I am aware of threats such as phishing and pharming."

Respondent's ID	Knowledge about phishing (I2)
1	"To be from a bank and asks for account information."
2	"Only by way of information that has been put on the TV."
3	"Not much, my time is valuable and I do rely on the expertise of Internet service providers, various pieces of legislation, the police, various 'watch dog' organisations both conservative and liberal and software designers to ensure my safety and privacy on the Internet."
4	"E-mails from people pretending to be banks, etc., that try to get customers to click a link to a web page that subsequently steals their user id and password."
5	"Nothing."
6	"Nothing."
7	"Yes."
9	"Very little"
10	"No."
11	"Nothing"
12	"Not much."
13	"According to my understanding phishing is a fraudulent activity in which users are provided with identical but fake websites."
14	"Nothing"
15	"Stealing others' online identification to use in illegal thing."
16	"I believe it works as described in number1. Spam e-mail asks for username + password."
17	"As per you said 'phishing' is like fishing which means trying to get another person money from his/her account either stealing identity or not."
18	"Monitoring software."
19	"I don't know about it unless the interviewer introduces it to us."
20	"There are some people "professional" who will transfer your balance "account" to their account."
21	"Sending e-mail to somebody by pretending bank office."
22	"Stealing people's money."
23	"I am not really sure. It is some kind of internet theft."
24	"That it is common and people got affected."
25	"Phishing is something like hacking."
26	"Stealing personal ID."
27	"I have no idea about phishing."
28	"I just read some information about it on the Internet. That is one of the ways of getting private bank information by sending mails or giving calls behalf of bank."
29	"It tries to get into your computer to steal information."
30	"Fully aware of attempts to contact/extract info using phishing."
31	"I think it is a common appearance, not only in Australia but also around the world. It is an illegal act."
32	"Nothing."

Respondent's ID	Knowledge about phishing (I2)
33	"I just know phishing is stealing money from someone's bank account."
34	"It is a fraud which is done with the credit card detail in website."
35	"People try to access to your log on details."
36	"In the field of computer security, phishing is the criminally process of attempting to acquire sensitive information such as usernames, passwords, and credit card numbers."
37	"Stealing money from someone account like fishing in the sea."
38	"Some people know your password and some information of you then they could use your online banking."
39	"I am not sure about it."
40	"Do not know about this."
41	"Get money from other's online account."
42	"Steal money from others' account."
44	"When a user enters account information on a non-banking website that looks similar to the original."
45	"It steals your personal information and most importantly your bank account."
46	"E-mail sent to you that looks like it's from your bank, but requires you to authenticate yourself, it is sophisticated."
47	"Only that it is a threat."
48	"I receive regular phishing requests via e-mail. Phishing relies on people supplying private information to someone who is not who they claim to be."
49	"No."
50	"I think it is junk information which may spread virus on computer."
51	"Not much. I think it's a fake website that pretends to be a bank and gets you to put in your passwords and user names etc. to steal your identity."
52	"Oh, use fake name and account to threat. Like we might receive an e-mail said that "I'm from xxx bank, your account is in danger now, please sending us your account name and password, and we can fix that out." Ha-ha, I think this is right."
53	"Nothing."
54	"Nothing. I don't care and know what the term phishing means."
55	"It is one of the thief identity methods via online network. Usually, e-mail and rough website are used by hacker to accumulate an identity from victims. In order to do this, e-mail will ask victims to access a rough website before the information will be gained by capturing any activity on the screen."
56	"I've heard the word but I'm not entirely sure what it is."
57	"They attempt to get details such as account and card numbers & logon details by having you go to a site that is supposedly a bank site and entering data into a form which keeps a log of your entry so the scammers have access to your account to steal money from it."
58	"What I know and what I am using is a past word key looks like a flash drive. No matter when I have to use my Internet banking, I should insert that flash drive key to log on."
59	"Not personally."
60	"Criminal and fraudulent attempt to acquire personal banking information."
61	"No opinion"
62	"Never Heard of it."
64	"Phishing seems like "Junk mail" to ask your personal detail."
65	"No opinion"
66	"Just know the hackers want to take our password."

Respondent's ID	Knowledge about phishing (I2)
67	"Specially created e-mail/conversations that mimic legitimate conversations from an advertised institution to gain credentials."
68	"Involves the creation of a website or e-mail or both that look to be from the bank but are not. Entering details into the site or replying to the e-mail will send details to the scammer."
69	"E-mails, usually, trying to capture passwords/ account details."
70	"People tried to get access to your bank details."
71	"Nothing."
72	"It's a way of persuading people to part with information that they might otherwise wish to keep secret."
73	"Stealing information."
74	"I see it quite often at work. We get direct e-mails sent to me and through our resume e-mail address."
75	"As I know it is unauthorised activity."
77	"Heard about it. Never experienced. Simply know how it works."
78	"That e-mails are sent out from what is supposed to be your bank asking for your details. Such as passwords and customer numbers."
79	"I see e-mails on a daily basis requesting banking details... I just delete. But I am aware that some people must fall for this trick and respond with their details. My bank never contacts clients by e-mail for password related issues so I just deleted these."
80	"Online banking is prone to internet hackers who can hack into one's account and saving the entered password for their remote access without user realising."
81	"It is an attempt to get someone to give private information as to steal it and use for identity theft."
82	"People create fake websites for real companies, banks, etc.to try to trick users into giving personal information."
83	"Not much so I can't really explain."
84	"According to what I have read, the scammer sets up a clumsy website similar to the bank or business and then tries to direct consumers to this. Once they will steal as much information as they can in order to take that person's identity."
85	"No."
86	"They send you a security question to confirm and will access to your bank account."
102	"It's kinds of Nigeria and winning lotto."
128	"Phishing is where hackers send e-mails to people disguised as legitimate businesses to try to gain people's account information."
140	"Something about a false site that looks similar to the original bank site. Advice is not to go on a bank site the e-mail links. Use Https directly."
149	"No."
165	"It is the same as skimming."
177	"Persons pretending to be your bank or others and trying to obtain personal details such as bank account numbers."
180	"Seen the e-mail version and the webpage version."
181	"A duplicate of website/ e-mail from an organization to gain users information illegally."
182	"It is a deception."
188	"Nothing."
189	"Phishing is trying to persuade user to click some websites that look exactly as the original website but collecting account information in a fraudulent way."
191	"Cheating to get confidential details."
206	"They can be around the house that has wireless and access to the network to copy password from people in the house."

Respondent's ID	Knowledge about phishing (I2)
208	"Phishing is an e-mail fraud scam conducted for the purposes of information or identity theft."
209	"User is directed to a fake bank website and their login details are captured."

Respondent's ID	Discussion about malicious threats (I3)
1	"Programs installed on a computer to track user activities, gain confidential information etc."
2	"Nothing."
3	"Not much again, heavily reliant on ISPs and software designers to guard against this."
4	"Software that is loaded to a computer usually without the user's permission that collects data such as keystrokes or restricts access to web sites."
5	"Nothing."
6	"Nothing."
7	"Very little"
9	"Trojans-computer viruses."
10	"All I know is that the above indicates someone is trying to access my information/screen/account."
11	"No opinion"
12	"Spyware is trying to access my computer."
13	"They are piece of programs that installed in the system without users permission and lead the system to malfunction such as delaying, displaying unwanted & unnecessary info & changing the location of files or folders."
14	"No"
15	"Spyware: software designed to spy on users and send personal information to the spyware's programmer. Adware: software sends ads, popups and spam e-mails to people. Trojans: malicious software that may damage the system."
16	"I know that Trojans can be to control your computer, for example to shut down the Internet."
17	"I think it's a virus name."
18	"Hacker"
19	"No, I don't know."
20	"I don't know anything."
21	"I am not sure."
22	"Computer virus."
23	"These are some kind of viruses."
24	"That it is common and people got affected."
25	"These are viruses that made by hackers."
26	"No."
27	"Nothing."
28	"Virus programs, created by hackers, to manage or destroy remote computers, particularly bank computers."
29	"Tracks your use of computer."
31	"All of these are computer viruses which can send viruses from the senders to the computer users."
32	"Steal account detail and password."
33	"I don't know much. I just know those are attacking on Internet."
34	"Spyware is the software that spy on our computers. Adware appears like some advertisements and pass virus into the computer."

Respondent's ID	Discussion about malicious threats (I3)
35	"Often comes with the free software downloads. Can affect PCs performance."
36	"Spyware is a type of malware that is installed on computers and collects little bits of information at a time about users without their knowledge. Trojan is a non-self-replicating malware that appears to perform a desirable function to user."
37	"It's kind of terrible viruses."
38	"If you visit unsafe network. It may have the spyware that will damage your online account."
40	"They protect the data on my computer."
41	"Nothing."
42	"No, I don't know."
44	"Virus or mini-programs that track and record online activity."
45	"I'm not sure but have heard of them."
46	"These programs collect personal information for unauthorised used."
47	"Only that they are threats."
48	"There are codes attached to e-mails & websites that can infiltrate your computer system when you activate an e-mail or enter a website. They can then be used to get into your personal files & e-mail accounts."
49	"I don't know."
50	"I know that spyware and adware are the program for detecting virus and Trojans, are the most serious virus that is difficult to clean it."
51	"Spyware records keystrokes and tells what sites you've visited, etc. Adware causes popups to appear on your desktop, spamming etc. Trojans are viruses and other programs that get into your computer attached to other programs, files or e-mails."
52	"Is that means if we receive an unnamable website from MSN for example, and we click that, we might be hacked by hackers."
53	"Nothing."
54	"I know that you can get software to protect you from these things. It is an important piece of software to install on your computer if you plan on using the Internet. Otherwise people can access information that you have recently submitted or viewed on your computer."
55	"They are one the example threats on the online network. Many approaches are used by these things to warn the information on our company. For example, damaging the information on storage, thieving our secure information from our computer, monitoring our activity during using computer. By these activities, our information is in a great danger if we do not have any method to encounter them."
56	"I've heard of it but not sure what it is."
57	"They can drop keyloggers into your system and monitor data entry such as card details, account logins etc., save the results and periodically e-mail them using their own hidden SMTP or pop client."
58	"What I know is Trojan which is a kind of virus or spyware which may let somebody else know my password."
59	"Yes, but not related to online banking."
60	"Trojan is malicious software. Spyware is virus. Adware is uninvited advertising."
61	"Spyware is software that gleans information from a personal computer without the user's knowledge. Adware is advertising supported software. Trojans are malware posing as legitimate programs in order to introduce Spyware or other malicious software to your (personal) computer."
62	"Never heard of the terminology."
64	"No, I don't know anything about that."
65	"No opinion"
66	"Just know they want to use them to collect our password and send it to another destination."

Respondent's ID	Discussion about malicious threats (I3)
67	"Viruses software and malware can damage files, steal data, password and connect to botnets."
68	"Software that steals information; displays ads or otherwise compromises a computer. Often hidden in an apparently legitimate program."
69	"I know a little from students' works."
70	"It comes via computer attachments and follows computer use - Websites visited, watches banking passwords etc."
71	"Nothing."
72	"Spyware sends information back to someone about your computer use. Adware is advertising you didn't request. A Trojan is usually something you download or accept onto your computer which when activated allows hackers access to your computer or information."
73	"Able to copy information and send on to alien party."
74	"Spyware and adware are security protection software and Trojans are a mean for hackers to gain access to PC/laptop."
75	"They are computer programs which harms."
77	"My anti-virus always warns those three items. For safety, I never install those which were warned. Adware is annoying. Trojans appears frequently although most of times it's because the anti-virus is too sensitive."
78	"These can infect your computer. Spyware can send out information to another person (Hacker) without the knowledge of the user. Adware uses a package which downloads adverts to your computer system. These can sometimes be classed as spyware. Trojans are malware which target a particular file allowing a hacker to enter your computer system."
79	"Software that downloads without your knowledge and looks for and records passwords."
80	"They include some form of tracking device/ code which monitors users' input, revealing classified details to a third party."
81	"Programs designed to automatically steal a person's private information."
82	"Spyware - software, often unintentional installed, that silently collect user data. Adware- Also often unintentionally installed ads, banners, etc. on pc. Trojans- Pretend to be software you want, but give access to your pc to others."
83	"No."
84	"These are set up to keep track of the Internet users online surfing. Once a pattern has been established. The Trojan operate then learn what sites the user should visit by installing popups."
85	"Yes."
86	"They usually alter, access, or delete your information and send back to the sender."
102	"Nothing."
140	"They are viruses that can mess-up the computer and also steal the information from the computer."
143	"No opinion"
146	"When the computer is infected it will allow the hacker to gain access to your personal detail."
149	"The Trojan program sends a bug to your PC and it can log in everything to the Trojan user. It thus makes the Trojan user capable of controlling the PC and extract data."
165	"I only know that they are bad things and you don't want them."
177	"Bugs in computer to relay your information/details to others."
178	"No opinion"
180	"They are different ways of classifying the way some malicious software work. Their purpose is the same though."
181	"Each has got their own way of working and illegally accessing user info."
188	"No idea."
189	"Malicious computer programs that try to access users personal information and account details such as username passwords or there security questions."

Respondent's ID	Discussion about malicious threats (I3)
191	"I'm not sure."
206	"There are many kinds of these viruses working differently such as copy password, keyboard change etc."
209	"Adware collects you information to sell to marketers, spyware collects information for hackers, and Trojan is a backdoor that can be used to obtain access over the computer."

Respondent's ID	Respondents' opinions on how personal information can be stolen from the Internet (I4)
1	"Characters, or cached by a search engine."
2	"No."
3	"I have a general awareness of legislation like the Privacy Act 1986 or the Electronic Funds transfer Act19?? There may be illegal software available"
4	"Fake login sites can collect user id, password, and credit card details."
5	"No."
6	"Only banking online credit card details."
7	"Yes. I'm shocked how easy it is."
9	"Not really."
10	"If a site is not secured, my personal details can be copied & my finances can be stolen."
11	"No"
12	"Never disclose any personal information"
13	"They are a variety of possibilities including phishing, hacking and identity theft."
14	"No"
15	"Spyware, keylogger, and hacking."
16	"I'm not sure about how this can be done."
17	"I do not know, but I think if we forget to log off our Internet bank website or if we tell our password to other third party then they can steal our personal information."
18	"Same people who is good at computer may use monitoring software to steal others information."
19	"I have heard related information, but I don't know more details."
20	"By cracking my "password"."
21	"Hacker, e-mail by pretending bank office and weakness of bank system."
22	"Yes, PC damaged by computer virus."
23	"May be fake websites."
24	"Yes."
25	"Yes, I know. Some hackers may hack online account of customers by stolen money from the Internet."
26	"Phishing."
27	"By tracing my password."
28	"Personal information can be stolen by request private information behalf of bank (by mail or by phone call). Moreover, the duplicate of bank Internet page may be created by changing at least one letter in spelling. For example, "original address: zaiffaizenbank.com. Another forge address: zeiffaizenbank.com > created for stealing information."
29	"By spyware and Trojans."
31	"Yes, as example, you get caught from some websites; the hacker can get your personal information by attacking the website."
32	"No opinion"

Respondent's ID	Respondents' opinions on how personal information can be stolen from the Internet (I4)
33	"Website, for example, Facebook or others which are used by many people."
34	"It can be stolen through the virus programs which enters the computer without permission."
35	"Keystroke logger or Trojans."
36	"Yes. If you click some strange links from website, and activate Trojan, then your password and account will send to other people automatically."
37	"No."
38	"Yes, I do. I think the Internet is not very safe that everyone can find information about you."
39	"Some people can use computer to steal my pin number such as e-mail information."
40	"Yes, from hacker using a virus."
41	"I'm not sure."
42	"Someone invades your computer and gets the information."
44	"No."
45	"Not really, it just a brief idea of clicking on fake e-mails from 'banks'."
46	"Spyware, dodgy online shopping sites, 'FREE' websites etc. Also, hacking your account etc."
47	"Yes, through cookies. When you sign up to social networking sites such as Facebook, you may agree without your knowledge to give out your personal information."
48	"Yes, with social networking & aggregated software using mobile technologies, personal information can be sourced from multiple sites including printed sources such as the phone book."
49	"I don't know."
50	"Yes, my personal information can be stolen in case of using some network such as Hi5 & Facebook."
51	"Recording my keystrokes, going to phishing sites and inputting my info here."
52	"If we provide our account and password to others??"
53	"I know that apparently people can access your account through "stolen" debit card and credit card numbers, which can sometimes be lifted when making a purchase at stores or when using credit cards for online purchases."
54	"I don't know a great deal that I would be able to explain. I have been taught a set of rules to follow to protect personal information over the Internet. These are: 1 I will not use internet banking in an internet cafe. (This is probably not necessary, but makes me feel safer.) 2. I change my passwords for banking etc. regularly. And I try to make the passwords complicated. 3. I also set my age at 13 when setting up a Hotmail account as this helps me avoid spam mail."
55	"Yes."
56	"No, but I'm aware it can be done."
57	"Yes."
58	"My personal information can be stolen by spyware, and some adware or website, which always required me to type a lot of information to become a member."
59	"I only know if you respond to any e-mails/ calls as mentioned."
60	"False e-mails can be sent."
62	"No."
64	"Yes, I know there is an object can be installed to steal information."
65	"No opinion"
66	"Through Trojans and viruses."
67	"Data can be sent using common protocols, crosssite scripting, buffer exploits, worms, counterfeit websites."
68	"Yes, through phishing, key loggers, on a website, theft of a database, hacking into a user account etc."

Respondent's ID	Respondents' opinions on how personal information can be stolen from the Internet (I4)
69	"No opinion"
70	"Hacking may be able to view my computer screen. Phish for my login information."
71	"No."
72	"Phishing, key loggers, hacking."
73	"No opinion"
74	"Not really. I do not have a number of security protection software in a place though."
75	"No idea."
77	"As mentioned above. Attack website."
78	"Yes. Personal information can be taken from other websites such as Facebook. By a user not using a secure site and placing credit cards details or personal details on these websites."
79	"Most communications are non-encrypted on the net. So you need to be careful about that data you use and when you use data the site must be encrypted or secure. Even that the hackers seem to be just as quick to circumvent these systems. I attempt to minimise my risk the best I can."
80	"If personal info have been entered to an untrusted site, and downloaded files and corrupted contain with virus, these information can be revealed. What is your opinion about using a combination of numbers and both upper and lower case characters can help you from an online banking scam? They make it slightly harder for those who have seen the password to guess. The combination makes the password harder to read in a quick glance."
81	"Through phishing, spyware, Trojans, and keyboard tracking."
82	"Through spyware, Trojan, and phishing."
83	"No opinion"
84	"Via misdirected e-mails and attractive looking survey asking the consumer about their details."
85	"Yes."
86	"No opinion"
102	"Giving your password."
107	"Computer in the banking system is not always foolproof. I work in a bank for a number of years."
140	"Not having anti-virus, anti-spyware software installed. Using public access Internet."
143	"No."
149	"I've heard but unsure on how it works."
165	"Once you put something on the Internet, it can never be taken down again. Generally personal info is given away by social networking sites."
177	"Yes, as above. Bugs in computer to relay your information/details to others."
178	"No opinion"
180	"Either directly or by attacking organisations, that does have information of me."
188	"No."
189	"Yes, Internet is full of such malicious programs and links and fraud people who always attempt to persuade users to click links that install Trojans, spyware to steal user information."
191	"Yes, it can be used for illegal purposes."
206	"Yes."
209	"A little bit, Facebook, cookies, spyware, fake websites etc."

Respondent's ID	Using a combination of letters and numbers in passwords can protect an online banking account (I5)
1	"Good idea"
2	"It has to be more secure than straight out 'Words'."

Respondent's ID	Using a combination of letters and numbers in passwords can protect an online banking account (I5)
3	"I do not know."
4	"They can definitely help but can be hard to remember."
5	"The more complex the pw the more difficult to 'break the code'."
6	"Too confusing."
7	"I think computer security is more important."
8	"Yes, more combination than only number."
9	"Good idea."
10	"I have no problem using this combination (or any for that matter) if it ensures security to my income/ investments."
11	"Great."
12	"Good idea."
13	"Online banking scam, phishing, captured all information entered by the user in a fake webpage. So, confusing password may protect from other fraudulence; however, will have less effect for phishing."
14	"Secure as long as you change on a regular basis."
15	"Yes, it can but not 100%, it makes it difficult for bad guys."
16	"I don't know."
17	"Not really, because scammers are really clever. They can find out combination of numbers easily."
18	"The numbers are not often used by you."
19	"That would be ok."
20	"That's good."
21	"It's quite easy and safe."
22	"Yes, the more number, the difficult for other people crack."
23	"Yes, this can help to protect your account because nobody knows what you have used in your password."
24	"It is a start but not enough."
25	"I agree with this idea. It should be combination of numbers and characters and symbols."
26	"More secure."
27	"I don't think so."
28	"It makes my security code (password) safer; however, it is not perfect anyway."
29	"Good idea but hard to remember."
30	"Very good idea if you can remember them without writing them somewhere."
31	"If it is useful, I will pay for it."
32	"No opinion"
33	"I agree because that would be hard to guess by others."
34	"It will help a bit"
35	"Probably not."
36	"Yes, it will improve your quality of your password in which no one can easily work out your password."
38	"It is not very useful."
40	"Good idea."
41	"No idea."
42	"It is difficult to steal."
44	"I think it is better and will protect you more than simple passwords."

Respondent's ID	Using a combination of letters and numbers in passwords can protect an online banking account (I5)
45	"I think it would be harder to trace."
46	"Password with a random capital letter is more secure than a capitaliser first letter i.e. 'Password' is not secured, but "paSswoRD" is more secure."
47	"Using this combination will make your password harder to get, and thus it is an effective way if securing your information."
48	"Good use of passwords with regular changes is a simple way to provide security for your banking; provided you do not give this information out to keep is private (secured) form."
49	"Alphabetically and number"
50	"I think it may help but it is complicated to do and to recognise it."
51	"So many passwords are difficult to remember, putting those restrictions makes it more likely people will forget, I think, causing more admin troubles."
52	"Not that easy to figure out by others, it's good, and I use this method as well."
53	"I understand that using a combination, including numbers, symbols etc. are more difficult to hack. I have seen on some sites when you are making a password that is a gauge or monitor that indicates how "secure" your password is."
54	"I think anything that can help to protect me from this sort of things is worthwhile, but I might have a bit of difficulty remembering which letters been upper case and which were not."
55	"It is quite secure in one step. However, this approach is not enough to prevent the banking scam. In my prospect, the out of bandwidth method should be considered to use to prevent me and other people from this thing."
56	"I'm aware that this is considered a "strong" type of password."
57	"It may prevent brute force and dictionary attacks, but is no use against keylogging - in fact, random keystrokes may be picked up as passwords from keylogger records because they are not words."
58	"When the password is complicated, it means more difficult for someone to steal your information."
59	"I don't know."
60	"Yes, best to use a password that cannot be guessed easily."
61	"I don't know if it helps, but I use combinations of letters, numbers and lower case."
62	"No opinion."
63	"Anyways that will make my account secure is ideal for me."
64	"Yes, but it might be more difficult to remember. Yes, I do. Most people chose the number as it easy to remember."
65	"It is good plus some special characters would be good, but I still don't trust Internet."
66	"That would be difficult for the hackers to guess."
67	"From a scam - unlucky, but it can protect you from brute force attempts to guess your password."
68	"They would form a slightly stronger password that would take longer to brute force attack."
69	"Apparently the more complex the string, the harder it is to crack."
70	"The more variety in the password, the better."
71	"The more difficult the password, with the combination, less chance of the online account being accessed by the other users."
72	"It's a stronger password but difficult to remember."
73	"Not needed yet."
74	"I use this method. It seems to work."
75	"I think so."
77	"It doesn't work because no matter which case, it is word processing. Besides, it's easy to forget."

Respondent's ID	Using a combination of letters and numbers in passwords can protect an online banking account (I5)
78	"It makes it harder for someone shoulders surfing to guess the combination. It will make online banking scams harder. The problem with this is that it can make it harder for someone to remember the password, or if they have more than one password, and they may write it down."
79	"I think I believe that this makes a stronger password but would not in itself completely protect anyone. For example, if you gave your password to someone it would not matter what it was."
80	"They make it slightly harder for those who have seen the password to guess. The combination makes the password harder to read in a quick glance."
81	"I'm advised that it is helpful."
82	"Not sure it actually adds much security though."
83	"I've heard of it and I'm currently doing so but I don't think that will help very much."
84	"It is one of the better ways to avoid a computer program getting your password."
85	"Both upper and lower case characters make the combination harder to hack."
86	"I agree to do so."
102	"It's a good idea."
106	"No, make it is too difficult."
107	"Helps to prevent banking."
140	"Nope, just makes the probability of finding the password harder and longer for the thief, but they can still figure out."
143	"Yes."
146	"It may be secured."
149	"Yes, enhance security."
165	"No. They can still take things from the Internet."
177	"Anything that can make it harder for others to hack into your information."
178	"Good Security."
180	"Yes, otherwise if they use dictionary attacks."
181	"Yes, increase the password security."
182	"Yes, it is harder to crack."
183	"It is hard to know the password number."
188	"I think it would but not sure how long it would take before I get used to the combinations especially if I have to change it every 3 months."
189	"There should be special characters also included in passwords"
191	"More secure."
194	"Good protection."
196	"I am not sure if the combination could protect me from an online banking scam. But I think that kind of mixture will be more secure than numbers."
200	"I guess it will be safer."
206	"Good."
207	"It would help."
208	"It would help but not 100%."
209	"Probably more secure as it means more combinations if someone is going to try a brute force attempt. Although won't protect against a phishing scam."

Respondent's ID	Respondents' opinions about using date of birth or phone number as a password is insecure (I6)
1	"Yes, if the information is available to the public (Facebook, Govt. births/deaths databases etc.)"
2	"Yes."
3	"It maybe if used in conjunction with other knowledge such as hard drive number, telephone number, ISP, Domain name."
4	"Very insecure."
5	"Yes."
6	"Yes."
7	"Yes."
8	"Not secure enough."
9	"Yes."
10	"To some extent -yes."
11	"Yes."
12	"Yes."
13	"I would like to mention an incident which had happened a year ago in Australia. A lady lost her purse in which she had bank cards and delivering license too. A person who found the purse stole some amount from her account since she had her birth year as a password. So, in my opinion it is totally insecure."
14	"Would agree."
15	"Yes, anything that can be predicted will not be fairly secured."
16	"Yes, probably."
17	"Yes, because if you lose your purse, it may have your photo id (student card) where it may have your date of birth or phone number which scammers will use this number first."
18	"Absolutely yes."
19	"No."
20	"No."
21	"Yes, it shouldn't be personal details."
22	"Yes, it is easy to guess."
23	"Yes, it is insecure because people such as friends and family can easily guess these details."
24	"Date of birth + social security number is a start of phone number, I don't know."
25	"Yes, I think that a password using my personal detail should not be from date of birth or phone number. It must create with symbols or numbers mixed together."
26	"Yes, too simple and easy to get."
27	"Yes."
28	"It is less secure than other combinations without personal information."
29	"Insecure."
30	"Yes, very insecure."
31	"No. If you use your birthday or phone number as your password, the hacker can easily guess it."
32	"Yes, it should be more difficult things."
33	"Yes."
34	"Yes."
35	"Easily discovered."
36	"Yes, maybe you lost your wallet which contained ID and bank card. If your password is your date of birth, it will be easy to work out."

Respondent's ID	Respondents' opinions about using date of birth or phone number as a password is insecure (I6)
37	"Yes."
38	"Maybe it is insecure."
39	"I don't think it is safety."
40	"Yes, too common."
41	"No."
42	"I don't think is secure. Someone can still change it."
44	"Very insecure."
45	"Yes."
46	"Well that is just silly."
47	"Yes, because that is the first thing hackers will use to and access your account."
48	"Yes, too many people already have access to this information and can then determine your password by trial and enter."
49	"Yes."
50	"Yes, some companies usually record personal information online when lead somebody can get it easily."
51	"Yes."
52	"Of course, it is easy to guess and that information is known by many people."
53	"Yes."
54	"I do agree. I tend to make my passwords as abstracted as possible and I try not to take them from my personal details such as address etc. Instead I may use my favourite brand of lollypop and the price (example allensredfrogs312)."
55	"Yes, this is because it is easy to guess."
56	"Yes, it would be inadvisable to use this type of number as a password - too easily discovered & used fraudulently."
57	"Yes. This data is available easily from the phone book or from public records."
58	"Yeah- it is very easy for someone to guess."
59	"You are always advised not to use this type of information and I would "not" be happy to do so."
60	"Yes."
61	"Yes, I think if it is predictable, it is less than 100% secure."
62	"Yes."
63	"Yes."
64	"I agree with that, but it is hard to remember."
65	"Definitely."
66	"Yes, I think so."
67	"Yes."
68	"Yes, if the attacker has that information they could use it to attack."
69	"Yes."
70	"Very easily guessed, it needs to be more obscure and something no one easily guessed."
71	"Yes, definitely!"
72	"Yes, because that information can be obtained with relative ease."
73	"Yes."
74	"Yes, I do."
75	"I think so that is why in bank do not recommend that sorts of password."
77	"Depends. It is only insecure when you lost your ID or phone. Or you are betrayed by your friend."

Respondent's ID	Respondents' opinions about using date of birth or phone number as a password is insecure (I6)
78	"Yes. These are too easy to guess."
79	"Yes."
80	"Yes. Date of birth is known to everyone, especially so with Facebook birthday reminders."
81	"Yes."
82	"Yes."
83	"Yes, especially for people like me."
84	"Yes, it's well known that quite a few people do use this D.O.B. as the system and it would be a simple case of the scammer locating the consumer phone bill or driver license."
85	"Yes."
86	"Yes, to a certain point."
102	"No."
106	"No."
107	"Yes."
111	"Yes."
128	"I think for short term or temporary then that would be ok. It may be dangerous for long term to use though."
140	"Yes, that's the first they try."
143	"No."
146	"Yes."
149	"Yes, our ID is easy to get from passport, driver license, etc."
165	"Yes, it's too obvious; you could say something from another language or something."
177	"Yes."
178	"Yes."
180	"Yes."
181	"Yes."
182	"No."
187	"Of course not."
188	"Yes."
189	"Yes it is obviously insecure."
191	"No."
194	"Yes."
196	"Not at all."
200	"No. I don't think so."
206	"Yes."
207	"Yes."
208	"Definitely not."
209	"Definitely."

Respondent's ID	Discussion about opinions if changing password every 3-6 months can protect their online banking account from phishing (I7)
1	"No, changing passwords will only help against brute force or dictionary attack."
2	"Whilst it may be secure, every 6 months is OK."

Respondent's ID	Discussion about opinions if changing password every 3-6 months can protect their online banking account from phishing (I7)
3	"Do not know how effective this strategy is because I do not know what other strategies maybe employed to protect privacy."
4	"I think it is a good practice."
5	"No."
6	"I prefer to stick to one otherwise I'd be confused"
7	"I agree it can help but too hard to keep remembering what the pin number is at present."
8	"Good to change every 3-6 months, but you must remember."
9	"Changing passwords every 3-6 months can protect online banking-this will make it harder for everyone to keep track on password or anyone that has been monitoring your password."
10	"Because it prevents repetition & reduces the 'illness' of someone obtaining my password /information."
11	"Yes. That would be great but what happen if you forget? But I believe it a great idea."
12	true."
13	"As I mentioned earlier, phisher could have every details of what have been provided in fake webpage. So, here again it may help for other kind of fraudulence activities."
14	"No"
15	"Yes, unless the hacking techniques get developed faster than 3-6 changing password technique."
16	"I don't think it would really help."
17	"I do not think so because I have been to Australia more than one and a half year. I have got same password and my money hasn't been stolen. If we are careless and tell our private things to everyone, then scammers can hack out bank account."
18	"I don't think so."
19	"The bank should do more jobs for security not customer."
20	"Yes, I agree with that and 3 months is better."
21	"I don't think it is the best solution for security."
22	"That's not useful."
23	"Passwords should change were often instead of 3-6 months."
24	"Not enough security."
25	"It is a good idea for support and protect my online account."
26	"Good to protect personal ID."
27	"No, I don't think so."
28	"It may help, but it is not a universal measure."
29	"I'm not sure. That's not frequent. Maybe it should be every week or day but that's not practical."
30	"Misleading- regular changes can offer more security but it must not be over stated. Change depends on nature of phishing method."
31	"I didn't think it is useful because the hacker can get your code once, he also can get you twice."
32	"If they can get my password once, I change it everyday they still can get it."
33	"I think so. It is not best way, but still good idea."
34	"May be."
35	"Probably not if some hacker decides you're gonna be the next victim."
36	"Any opinions can be divided into two parts. On one hand, it will be good for your right to protect your bank account. On the other hand, it will make yourself confused sometimes i.e. forget password."
37	"Actually, I cannot rely on changing password regularly can protect my online banking account from phishing at all."
38	"It can protect your account more safely."

Respondent's ID	Discussion about opinions if changing password every 3-6 months can protect their online banking account from phishing (I7)
40	"Good idea for protection."
41	"Good it protects well."
44	"Not very good. It should be changed every month at least."
45	"I think it is a good practice to change password regularly to avoid any phishing."
46	"You should change your password more often than that."
47	"This makes sense because changing your password often is a good method for preventing your information being accessed without permission."
48	"Only up to a point. Hackers can gain access to your computer files if you operate and open wireless system."
49	"As, this method is totally secure and safe."
50	"I think it is an alternative way to prevent somebody to find out password easily."
51	"It makes sense, but as above, so many passwords to remember make it hard to remember."
52	"Err~ it is trouble, but I think this might help, so I will do this if it is required."
53	"Changing passwords every 3-6 months can protect your online banking account from phishing because it will be more difficult to hack or access. Using the same password gives more opportunities for it to be used by an illegitimate source."
54	"I would change my password more frequently than 3-6 months, but I agree that more people should change their password more frequently."
55	"In my view, it is not enough to prevent from this phishing. As I stand above, the out of bandwidth communication is the best way to prevent the phishing."
56	"I agree with it and I do it!"
57	"Probably, but it's too hard to change and remember your password every three months. I think biometrics is safer, or two part encryption system."
58	"Yeah, it helps maybe, but it is also trouble for users!! It is difficult to remember the changing password."
59	"If the bank asks a change every 3-6months, it must be necessary and I would comply."
60	"It would help to prevent phishing but not necessarily prevent it."
61	"I think it should be (almost) compulsory to change regularly, but I don't know if it will help if you have already been targeted."
62	"I don't know what phishing is; therefore, no opinion."
63	"Good."
64	"I agree with that, but it's hard to remember."
65	"It is definitely a hassle for us to think of a new decent password although I don't know changing will help security."
66	"I think it is not really necessary."
67	"This would have no effect on phishing."
68	"I disagree. No matter how often you change your password, if you give it away in a phishing attack you are in trouble."
69	"I would expect that you would need to change more often."
70	"It helps, but it is not enough- need more measures and more often changed."
71	"I think that regularly changing your password is a great deterrent to having an online account phished."
72	"That presupposes that the account has been hacked and if so then changing the password is helpful but by then the damage is done."
73	"I believe it but do not want hassle of recording and memorising new passwords (fear of loss of access)."
74	"I haven't had problem with phishing so I don't know if this works."

Respondent's ID	Discussion about opinions if changing password every 3-6 months can protect their online banking account from phishing (I7)
75	"I don't know."
76	Did not answer
77	"At some level, it does. But it would not always work. And finally you may run out of your pin."
78	"It does not protect you from phishing but changing your password on a regular basis keeps it more secure."
79	"No. Phishing involves you being tricked into giving your details. Make no different if you change it."
80	"Changing details often make it harder for hackers to track and trace the banking password. Thus this can reduce Internet scamming, though online by small extend."
81	"I disagree as phishing is an attempt by malicious parties to get someone to willingly offer up their details."
82	"Only if you're not found into it by a phishing site. Wouldn't really help unless you change it right after the information is phished, but still good practice."
83	"I think it's troublesome and I'm very forgetful that is extra work for me."
84	"People should be encouraged to change their password often as human nature makes us lazy and we start repeating the same password everywhere."
85	"Changing password every 3-6 months is good and harder to trace."
86	"No opinion"
102	"It's a good idea but hard to remember."
106	"Good idea."
107	"Prefer to change password without bank notification 'prompt'."
128	"While that is a good suggestion I think I would find it impractical."
140	"I don't think so unless someone is targeting specifically on you and need time and tries to get the code."
143	"I don't know."
146	"It is quite practical but it is an inconvenience."
149	"Make it more secure but troublesome."
165	"Even if you keep changing it, if they want to get in they will."
177	"Yes, it's a good idea to change password."
178	"No, cannot."
180	"It's wrong. It can increase the protection but doesn't protect it."
181	"Changing user's password regularly would reduce the exposure to online threats such as 'phishing'."
186	"It could be changed more often."
187	"It is somehow safe."
188	"I think it will."
189	"Not necessarily, user should be aware of viruses and phishing scams."
191	"Too long, not efficient."
194	"It's confusing to keep changing passwords."
196	"Good."
200	"Yes."
206	"That is a security way to do protect the password."
207	"It would help."
208	"In my opinion, changing password every 3-6 months is not enough to protect your online baking account from phishing. The best way is using security token every time when you log in to your online banking account."

Respondent's ID	Discussion about opinions if changing password every 3-6 months can protect their online banking account from phishing (I7)
209	"If your details were captured then you may have a chance to change them before they are used."
Respondent's ID	**Respondents' experiences in receiving an email from a bank and asking respondents for confidential information (I8)**
1	"No."
2	"No."
3	"I cannot remember but I do think that encryption is the best answer for any electronic correspondence containing highly sensitive information."
4	"Yes, I deleted it."
5	"No."
6	"No, never happened before."
7	"Yes. Ignored it."
8	"Call bank. Check if information requested is correct."
9	"Yes. Did nothing, I know that was a scam."
10	"No."
11	"No, I have not"
12	"No."
13	"Not yet. Even if they ask to provide via e-mail I will not provide, rather I walk in to the closest bank branch to enquire about the information."
14	"If the e-mail has asked for information, it is a scam."
15	"I receive a lot of fake e-mails but I never respond."
16	"No."
17	"No, they have never sent me an e-mail."
18	"I have never received."
19	"No I haven't."
20	"No, I haven't received."
21	"Yes, I ignore them."
22	"No, I've never received that mail."
23	"No, I have not received this kind of e-mail."
24	"No."
25	"No, I haven't."
26	"No."
27	"No."
28	"Never."
29	"Not a real one. I guessed it was faked and I deleted it."
30	"Yes, delete it."
31	"Yes, I just did as the bank told me."
32	"No."
33	"Never."
34	"Never."
35	"No."
36	"No. if it occurs, I will check whether it reliable or not."
37	"Yes. I've received an e-mail from stranger similar to ANZ e-mail to provide him my personal detail. I called my bank and inform them."

Respondent's ID	Discussion about opinions if changing password every 3-6 months can protect their online banking account from phishing (I7)
38	"No."
40	"No."
41	"Yes, I just leave it."
42	"No, I haven't."
44	"No, I haven't."
45	"Yes. Delete!"
46	"Only the manager at the bank of Nigeria. I just deleted this e-mail."
47	"No, if I did I would just delete it."
48	"Yes, sent a copy of the message to IT central. Thus a frequent occurrence also sent copies to the bank concerned after finding their contact details on the official website."
49	"When I change my details online after that usually I am getting e-mail from bank."
50	"Never."
51	"Yes, I assume it was unreal. The first few times I tried to contact the bank, but bank purposely use their websites to make communication harder, not easier, so I have up trying and just delete."
52	"No."
53	"No."
54	"I received an e-mail that I had won a lottery. They wanted my details. They did not ask for bank details. But it was obviously a fake lottery so I didn't respond. I received another e-mail when I was job hunting saying that someone was interested to set up an interview with me, but first they needed to confirm some of my information. So I looked up the information on their e-mail signature and when I couldn't locate the company I didn't provide the details. I would never provide details to someone I didn't know over the Internet. If this was legitimate I would show identification at the interview as a way to verify my ID."
55	"No."
56	"No, never."
57	"No, but I have received a lot from phisher claiming to be banks."
58	"Never."
59	"Yes, I forwarded to the bank. Who responded?"
60	"Yes, Ignored it and deleted it. Banks emphasise that they do not send e-mails asking for confidential information."
61	"No."
62	"No."
63	"No."
64	"No, never."
65	"Nope."
66	"No."
67	"Yes, I delete it."
68	"Not rather an official e-mail."
69	"E-mails, usually, trying to capture passwords/ account details. Deleted it!"
70	"Yes, reported it & deleted message."
71	"Yes. I have deleted most of them. Once I sent it through to the bank to let them know."
72	"Yes, I deleted the e-mail."
73	"No."
74	"Yes and I called them to verify."
75	"Thanks god, I have not."

Respondent's ID	Discussion about opinions if changing password every 3-6 months can protect their online banking account from phishing (I7)
77	"No, their letter said they would never do this. It is happens, I will check the mail address first."
78	"I have received e-mails from people pretending to be my bank and I just delete the e-mails. Once I did receive a number of e-mails over a few weeks asking for information and I contacted my Bank with the details of the e-mails."
79	"Yes. At least weekly if not more. I deleted and move on with my life. My bank does not contact clients for security issues via e-mail."
80	"Bank e-mails will not provide direct link to the login page. Somewhere in the content of genuine e-mail from bank will advise all users to log on a fresh page."
81	"No."
82	"No."
83	"No. If I did, I will call my bank personally to verify before providing the information required."
84	"No. but my first step if I was I would contact my bank immediately."
85	"My bank has never sent me any e-mail regarding confidential information."
86	"Yes, delete it."
102	"Yes, but refuse to give them."
106	"No."
107	"Yes, deleted e-mail."
111	"Never received any e-mail."
128	"Yes, I have. I took a screenshot of that e-mail, deleted the e-mail & contacted the bank."
140	"Yes, confidential information only such as I forgot my access into the account but never password."
149	"No."
165	"No."
177	"No, I haven't."
178	"Yes, it was suspicious."
180	"No."
181	"Yes, ignored the e-mail. Reconfirmed with bank by calling or visiting them."
182	"Yes, disregard."
186	"Nope, and I would do it if I received a mail like that. I would directly go the bank to confirm authenticity of that mail."
187	"No."
188	"No."
189	"No."
191	"No."
194	"Never."
196	"No."
200	"No. I haven't."
206	"No."
207	"No."
208	"No."
209	"No."

Respondent's ID	Discussion about ways to determine a legitimate email (I9)
1	"Little information identifying me, "Gut feeling", asking for passwords in an e-mail."
2	"I do not receive e-mails from the bank; in the event that I did I would go to the bank with a copy and discuss its contents with them."
3	"Again if uncertain about the validity of the origins of the e-mail and its author check with your ISP and the ASIC website. Generally anything that is received that I maybe unsure about I delete. If the e-mail looks like it is genuine and it contains enough information for me to believe that it is genuine, but is not, then the problem maybe deeper than just a 'scam'. It maybe from someone who knows more about you and your personal information than just your e-mail address."
4	"I ignore all e-mails from financial institutions."
5	"I was under the impression that banks don't e-mail their clients. Any communication is sent by postal delivery."
6	"Usually get warned beforehand from a friend."
7	"Usually, because they don't want a reply it just a statement or receipt of a payment them mobile."
8	"E-mail address is mutually enclosure to that branch."
9	"My bank has advised us that any requests from them will first come by mail. Never will it be done only by e-mail."
10	"I never receive e-mails from my bank."
11	"I would discard the e-mail & contact the bank."
12	"Bank would never ask for personal information on e-mail."
13	"Few things that I consider are: 1. Bank Logo 2. Font style and size 3. Type of information asked 4. Usual/ unusual from regular page 5. Contact details of sender is provided or not."
14	"If the e-mail asks for information, it is a scam."
15	"Banks never ask for personal information."
16	"I don't respond to any."
17	"If you are not sure whether that e-mail is from bank or not, it's better to go and ask them or call them."
18	"It's hard to determine."
19	"No opinion"
20	"It is difficult so I don't trust filling document via e-mail."
21	"E-mail address is not from the bank office."
22	"Check the e-mail address."
23	"I am not sure because I never reply to any e-mail from bank."
24	"Contact information, besides my bank never sends me e-mail except some advertisements. They always keep saying that I never should provide security issue over the Internet."
25	"I ask a question or tell or e-mail to my bank."
26	"From e-mail address and contact list."
28	"Banks "never" ask confidential information by mail."
29	"I'm not sure. Normally banks don't send an e-mail, so I assume it's a scam."
30	"I always assume a scam and take necessary measure/safeguards to deal with them."
31	"I will check the website or phone to the bank."
32	"Have the logo of the bank."
33	"Read e-mail or compare real site or delete without reading."
34	"Just by giving a reply and check the correct address."
35	"Only use 'secure mail' within account."
36	"I've no idea. Maybe just trust the anti-virus system."

Respondent's ID	Discussion about ways to determine a legitimate email (I9)
37	"The end of the sender address was not .au, it was .us"
38	"No, I can't think so. Some people could make the e-mails like the banks e-mail."
40	"Never received e-mail from bank."
41	"The same telephone number."
42	"Ignore it."
44	"Logo, ask me to see them personally at the bank. Never ask for personal information."
45	"I have accounts from the particular banks or by contracting them (the bank) first."
46	"I wouldn't respond directly through the e-mail but rather log onto the bank's website to confirm."
47	"1.Paper format, spelling/ grammar and logo. 2. Does not ask for personal information."
48	"I use one bank which clearly states they will NEVER ask for private information online."
49	"Bank logo, design, and the way it appears."
50	"The topics of e-mail which indicate the name of the bank and make me know that is the e-mail from bank."
51	"They don't ask me to do anything like click a link, confirm info, etc."
52	"If that's a bank statement of mine, or advertisement but no website, I think those are not e-mail scams."
53	"I do not know but I have never responded to an e-mail that has requested personal information unless I know the source."
54	"As I have my age on my e-mail account set as age 13 I do not receive advertising e-mails. So I have not encountered this issue. But I get message from my bank once I log into my Internet banking account. They very rarely get sent to my e-mail account. I bank with Westpac."
55	"1. Checking the source very carefully. 2. Checking the purpose of the message. If it asks for providing confidential information, I try to do the out of bandwidth approach to keep my confidential information."
56	"I never receive e-mails from my bank except to tell me my instatements are ready. I would be suspicious of anything else because my bank communicates with me through secure mail through the bank website."
57	"My banks have a strict of e-mail policy- they have always said they would never send an e-mail asking for personal details or logons."
58	"From the e-mail address. Notice the details."
59	"My bank doesn't send any e-mails."
60	"Any e-mail sent by a bank, I will suspend it is a scam."
61	"I have never received an e-mail from my bank, so I would phone the bank to validate any unsolicited e-mails."
62	"Never react one."
63	"Not received any."
64	"I don't open that mail, but choose to enter bank's website."
65	"I usually don't reply e-mail."
66	"Check their e-mail address first, which is their e-mail service provider."
67	"You can never be certain; however my banks do not send any e-mail as policy. Therefore, all bank e-mails must be scams."
68	"Look at the sender address. If this has been altered, e-mail clients often report it. Look for comments in the e-mail such as "do not reply to this e-mail", "type the URL www.bankname.com into your browser." etc."
69	"Most of the banks say they would not use e-mail. Messages are from the site once you have logged in."
70	"Bank has said they will never ask for details that way."

Respondent's ID	Discussion about ways to determine a legitimate email (I9)
71	"Our bank says they NEVER ask for account information by e-mail so we know it is a scam."
72	"The scam often has spelling errors and the links have strange addresses but if they look good I ignore them."
73	"Caution."
74	"I verify with a bank with a call."
75	"I don't check e-mails from Internet banking."
77	"The part after '@'. There should be some information related to the bank, if it's from bank."
78	"A bank will not ask for banking details such as your password in an e-mail so I treat all this type of e-mails as scam."
79	"I delete all e-mails from Banks. Generally this is not how my bank communicates with me."
80	"I base on the trust of the official bank website."
81	"I don't receive e-mails from my bank."
82	"I never use link from bank e-mails. Apparently checking the line address for any links in the e-mails is a giveaway. But safer to go directly to bank website in browser."
83	"I will call my bank to verify."
84	"As well as making sun that they are not asking for my personal information. I have also introduced by bank that any e-mails need to include the address employee no. as well as their contact phone number."
85	"I do not trust any personal e-mail from the bank."
86	"No opinion"
102	"Call the bank to verify."
106	"Code and lock Sign."
107	"I don't. I contact the bank via the phone in the next working day."
128	"I would wait until I can contact a bank's representative."
140	"Really not sure but after all the Africa seems the approach is of it is too good to believe then forget it. Don't be greedy as nothing is free."
143	"Will not answer any e-mails from banks."
149	"I'm not sure. Looking at the e-mail address?"
165	"Ignore all e-mails, and take to a bank in person."
177	"Ring your bank to confirm."
178	"If they ask for personal information they are usually scams."
180	"I always throw them in the bin whether they are scams or not. If they have something to tell me, they can contact me directly."
181	"No idea how to determine if it's genuine or not!"
182	"The domain."
187	"Read carefully."
188	"Don't know."
189	"I receive my e-mails inside online banking log on as well as my personal e-mail address."
191	"Not asking anything about your confidential details."
194	"Bank name and website"
196	"I do not know as I had not received."
200	I don't know.
207	"Within the secured webpage of the bank."
208	"The bank that I'm a client usually does not send e-mails to client. So if I get one, read it carefully and phone the bank for more information."

Respondent's ID	Discussion about ways to determine a legitimate email (I9)
209	"I always assume that they are a scam regardless."

Respondent's ID	Discussion about ways to distinguish a legitimate online banking website (I10)
1	"URL"
2	"By using the information given to me by the bank i.e. Netbank etc."
3	"Do not know."
4	"I type the URL of the official site."
5	"Have no idea."
6	"Gosh never thought about it must be too trusting."
7	"Unsure."
8	"Look at copyright."
9	"My husband set it up with bank."
10	"I have my banks webpage as my favourites."
11	"The secure icon."
12	"Not sure."
13	"Few things that I consider are: 1. URL address- I do check every time, even though it is retired from cookies. 2. Appearance-Is the page looking same as previously when you did transaction? If not check URL one more time and type it manually."
14	"Never go through a link attached to an e-mail."
15	"Straight web address with [https://] before."
16	"I don't know."
17	"I don't know."
18	"I don't know."
19	"The correct address."
20	"I always know how much money I have from my balance."
21	"I'm not sure, maybe website address."
22	"Check the website address."
23	"I always put web address by myself."
24	"In order to log in I must use a digipass with algorithms."
25	"I don't distinguish."
26	"No idea."
28	"I used to check the spelling of webpage, when I enter to the bank website."
29	"I don't know."
30	"Access from 'favourites' generally but if not then I always check the address."
31	"In my own computers, there is software which can find out the computer virus and clear them."
32	"Check the website address."
33	"Compare webpage which I usually use."
34	"It is not easy actually, based on the experience only."
35	"Check web address."
36	"No idea. I just put the normal website address."

Respondent's ID	Discussion about ways to distinguish a legitimate online banking website (I10)
38	"My online banking is from ANZ, so I often visit the legitimate webpage which have the ANZ word."
40	"Not sure."
41	"Just go to the government web site to check."
44	"Address has web browser authenticity (show green tab bar for safe)."
45	"Check its authority and URL."
46	"I always type the full address into my search bar. I don't use a bookmarked page."
47	"1. URL is secure https:// 2. Correct format, spelling and logo."
48	"The online banking webpage can only be connected to from the official bank website. Takes a long time to go through security protocols."
49	"Sorry, no idea how."
50	"I am not sure. Normally, I use online banking as direct information form bank which is credible."
51	"I look at the URL."
52	"Use the official website and log in."
53	"I have only accessed through my "Favourites" on my own computer. Plus, I have never had a problem with the site."
54	"I wouldn't have any idea. I guess one way would be if it was a secured site. The colour of the background on the address bar turns green I think."
55	"1. Clicking URL very carefully. 2. Checking any eccentric on the interface in the website."
56	"I'm not sure I could."
57	"Spelling errors, grammar, logo quality, comparison to a known legitimate site."
58	"If the webpage is a legitimate webpage, the address line will have a little lock there and also the background colour will change to yellow or something."
59	"I do not save in Favourite as I have been advised that these can be corrupted. I don't know a way to ensure it is a legitimate site."
60	"Can be difficult. Look for spelling errors and layout, interpret grammar. Sometimes a scam can have grammatical errors."
61	"I use Favourites, so it "should" open to the actual bank's site. Other than that I really don't know."
62	"The web address is saved in my favourite so I just log in."
63	"I cannot. Once I log on I assume it to be the legitimate site."
64	"I always check the homepage before I log in."
65	"Checking URL in the address bar. Plus, the SSL icon in the tray."
66	"Check the website address from the bank website."
67	"I check that true sites security certificate it signed by a reputable key authority."
68	"Look at the URL. Other things like spelling mistakes can be a giveaway."
69	"I don't think I would be able to tell."
70	"Never thought about it."
71	"I don't know. I presume it is the right one."
72	"I go there from my bookmark or type in the address myself. I never click on the links in e-mails."
73	"Content and context."
74	"I check the http and access the bank quite regularly so look for inconsistencies."
75	"No idea."
77	"Get into its homepage correctly, and then those webpage you get in by links are legitimate."
78	"It can be difficult but there are some differences. Some of the layout will be different and the ads or wording may be different. I have not personally come across a counterfeit webpage. No."

Respondent's ID	Discussion about ways to distinguish a legitimate online banking website (I10)
79	"I check the URL."
80	"No."
81	"It has a verification sign at this start of the address bar."
82	"Navigate directly to it using proper/main address, e.g. ANZ.com. If the banks main site is being obverted, no idea."
83	"I can't really distinguish."
84	"By viewing what information is being requested from me."
85	"Always look for their logo and read the fine print."
86	"No opinion"
106	"I'm not sure."
140	"Sometimes the bank tells you. But one way to know is also that the sequence of process differs from the usual way I have been doing or accustom to."
143	"I don't know."
149	"It's the official website written on the address."
180	"Hard to tell but usually the address is a good start, where the link point is also good way to check."
181	"Based on the explanation and security features explained to us by the Bank Officers during the process of applying for online banking account."
182	"URL."
187	"Not sure."
188	"The padlock that appears on the webpage."
189	"By looking at URL, secure web lock symbol, graphics and logos etc."
191	"Not asking anything about your confidential details."
194	"Web Address"
196	"No. I don't know."
200	"I cannot distinguish."
207	"You go directly to the webpage of the bank."
208	"Contact information - Secure certificates."
209	"I load it from a saved link."

No.	Phishing bank account experienced (I11)	The attacker was successful in obtaining anything from the account (I12)	Use or attempt to use personal information for some other fraudulent purpose (I13)
7	Not sure. Credit card yes bank alerted us & cancelled transaction & used new card.	No	Yes, credit card in a place where never been to.
17	No, not mine. But twice with my sister's account had been attacked. We went to the bank and explained that we have not used credit card. It's unauthorised person. And bank investigated.	Yes, he used her credit card twice.	No, I don't know how they got my sister's personal information.
46	Yes, I noticed a small transaction appearing on my credit card once a month. I called the bank and had my card replaced.	Obviously, they had deducted $2-$3 each time for about 2 months- all ended up around $40.	Not that the aware of.
53	Yes. I have only been contacted once because someone was trying to use my credit card in another province.	The bank suspected it was fraud, they contacted me and I assured them the purchaser was not me. I then immediately cancelled the credit card and received a new one.	No.
69	Yes, the bank's fraud division told me that someone from New York was using my visa for shopping.	I didn't see anything on the statements but they had apparently made secure purchases.	Not as far as I know.
84	Yes. I periodically view my banking details. I once noticed that only I cent or 2 cents had been deducted from my account. I immediately contacted my bank to prior these.	Yes, as above. I cent or 2 cents had been deducted from my account.	Not via banking; however, did have license plates stolen from my car which was then used on another car without the police checking their own details. IT was claimed to be my car which meant they felt I was liable for the costs.
101	Not sure. I had only one of my blogs hacked and a phishing site was installed. Westpac called me and I changed my password and deleted the phishing directories.	Not sure. I had only one of my blogs hacked and a phishing site was installed. Westpac called me and I changed my password and deleted the phishing directories.	No answer
178	Yes, my NAB had been hacked when I booked the air ticket. The hacker came from Greece.	Yes, the hacker took $5,000.	I'm not sure if they did.
206	Yes.	Yes, because I have lost my money for 3,000$ from online banking.	Not applicable

Respondent's ID	Respondents' opinions about the vulnerabilities of online banking (I14)
1	"Uneducated users."
2	"Do not know."
4	"Easy to guess passwords, bank web sites with only one level of protection, e.g. single password."
5	"Password & security # being left lying"
6	"Only when literature gives on the credit card info."
7	"Unsecure, computers and naive computer/Internet users"
8	"Personal information is somehow known (either unintentional or stolen) easily guessed passwords."
9	"Not applicable"
10	"Not sure."
11	"'Phishing'. I do not know what that is."
12	"Not enough security."
13	"1. Users careless behaviour. 2. Banking policies including users right to get access to the information. 3. Security of banking websites 4. Government policies to deal with system penetrator. 5. Minor responsibilities go to cyber operators too. There was an incident regarding this matter. 6. Some responsibilities to ISPs. If only ISPs have strong firewall or other security measures, it could be remarkably reduced."
14	"People trust email."
15	"Low security standards->"
16	"I don't know."
17	"1. If we provide our personal detail to others. 2. If we lose our purse/bag having bank details. 3. If we use our date of birth as password."
18	"Due to man people do not have enough knowledge to distinguish the phishing."
19	"Protecting personal information quite well. Raise strong security service."
20	"The victims themselves because they don't know when they pass to their account."
21	"Banking security system."
22	"Click the unknown website."
23	"I am not sure because I have been using internet banking only for 3 months."
24	"People do not aware of the risk."
25	"No opinion"
28	"Trustful of clients."
29	"I don't know."
30	"Gullible/ stupid/ inexperienced users."
31	"Maybe the bank's website and the email which bank sent to their customers."
32	"Knowledge of online banking and Internet."
33	"Security system in bank."
35	"Limited layers of password protection."
36	"Maybe the system of bank or some bugs of software of personal computer."
37	"No enough security program between the bank and the users."
38	"People visit the unsafe webpage and put their own information everywhere."
41	"No opinion"
42	"People who save money to banks.
44	"Websites that look professional and information that looks legitimate & helps the user gain money."

Respondent's ID	Respondents' opinions about the vulnerabilities of online banking (I14)
45	"Easy detectable or easy to hack of the passwords."
46	"User ignorance, people not being able to identify what is legal and what could be fake."
47	"People are not educated enough in the use of computers to determine what is fake or real."
48	"People are ignorant. Forget the bank's advice re online banking or in a hurry & click & provide information without thinking about it. Some emails also manage to look very official & use return addresses that mimic a possible email for the bank."
49	"Good copy version which is similar to others."
50	"A bad security system in online banking may cause phishing to access easily."
51	"Websites look real."
52	"People want cheap stuff or free stuff, and click the website which is provided, and fill out the form or something in order to get a gift or something."
53	"I think the vulnerable points are not the bank websites but sites/business that sells things on line. Once you have given out the card and personal information, it is impossible to know where it goes and who has accessed to it."
55	"The carelessness of victim to access the information on website. The reluctance of victim to follow the rough information."
56	"I'm not sure what phishing is."
57	"Fear of having your account frozen-the shock factor. Fear of being scammed by someone- being supposedly "protected' by the scam process. Belief that the scamming process is part of a legitimate security upgrade. Masquerading as a legitimate problem with your account- offering a solution."
58	"Some advertisements which are very attractive such as good jobs get money easily. And some adult webpages."
59	"No opinion"
60	"Gaining customers users and passwords to hack into the banking system."
61	"Really don't know."
62	"I have no idea."
64	"From user who reckless and careless in security."
65	"Gullible people are always easy to be tricked."
66	"Not enough awareness of virus, not yet installed anti-virus software."
67	"Poorly designed software of security usability and banking websites, wildly difficult and nonstandard authentication methods."
68	"People lack of knowledge about computers and the Internet. And sometimes greed (Nigerian scams)."
69	"People don't always know what is legitimate or not."
70	"Passwords. Phishing to fund who my bank is, so they can try to pose as my bank for information."
71	"A password that is a birth date, birth year or a password. Something easy to ascertain."
72	"The emails often look legitimate."
73	"Too complex to remember, in action, and asleep."
74	"Irregular checks on the account. Not being aware of all entries- debits and credits."
75	"Users' attention."
77	"The curiosity or careless of customers."
78	"People are just aware of the need for security of their personal details. Some people do answer these phishing emails unaware of the fact that they are not legitimate emails. For the average person there is little or no information available about the need for security only a leaflet maybe from the bank."
79	"People are stupid. They don't understand the Internet and the risks. They assume everything is legitimate. I'm amazed that phishing works to be honest."

Respondent's ID	Respondents' opinions about the vulnerabilities of online banking (I14)
80	"1. People do not log out from their online account after log in. 2. Not having an internet protection/ firewall on. 3. User does not monitor account on a regular basis."
81	"Naive people."
82	"People being ignorant of risks."
83	"Getting the person's personal information."
84	"By requesting details using offer that may appear too good to be true."
86	"No opinion"
111	"Careless use of passwords."
154	"The most vulnerable part of the system is the human elements. It doesn't matter how effective the technical increases are if the customer allows their own part of the system to be compromised."
165	"It is just too easy, and most people are unaware of the dangerous of online phishing."
180	"The awareness of the end user. Not being clearly focused and awake at the moment you login also."
181	"Almost perfect duplication of a website / email and Users lack of Internet Security knowledge."
189	"Banks not using secure web, strong password, lack of user awareness, not using anti- virus, anti-spyware, anti-malware programs etc."
191	"Not protected by internet security software."
196	"Cheating the customer for PIN no."
207	"Access point."

Respondent's ID	Discussion about methods that respondents used, or would use, to protect themselves or to solve the problems caused phishers (I15)
1	"No opinion"
4	"Maintain a complex password and changed to a bank with better online security."
5	"Would call the bank."
6	"No opinion."
7	"Excellent computer security software and only one person do the Internet banking & only one computer."
8	"Ask. Double check."
9	"No opinion."
10	"Fortunately I haven't had any problems."
11	"Contact bank and change password."
12	"Anti-phishing. Anti-Spyware."
13	"No opinion."
14	"Only respond to trusted emails."
15	"Keep my security Program up to date."
16	"No, but not sure."
17	"1. The best way to protect is don't give personal detail to others unknown people.2. Do not uses date of birth as password? 3. Contact bank time to time concerning transaction."
18	"Pay much more attentions."
19	"Never tell other about my personal detail information. Or I navel use my personal information online."
20	"I always change my password."
21	"Keep my personal information secret and follow the direction of security system."

Respondent's ID	Discussion about methods that respondents used, or would use, to protect themselves or to solve the problems caused phishers (I15)
22	"Changing all passwords as soon as possible.
23	"More careful while using webpage. Ensuring the webpage is correct."
24	"No opinion."
25	"I used anti-virus to protect my computer from hackers."
26	"Use my own laptop. Also, log on and log off all the time."
27	"Change my password."
28	"Do not provide any private information by mail or by phone. If you have some doubts about some requests for information, go to the bank office directly."
29	"No opinion."
30	"No opinion."
31	"I will clear my computer every week, not log on some strange websites, and not download some illegal software."
32	"Use online banking at home and use difficult password."
33	"I did not do anything."
34	"I will complain and require that bank for the details."
35	"No opinion."
36	"In my opinion, just rely on anti-virus software."
37	"Trying to find out the best software and not using Internet banking twice a day."
38	"Visit the legitimate webpage and protect own information."
40	"Call bank."
41	"Do not use online banking."
42	"Set password carefully."
44	"Change password. Always contact the bank concerning emails that ask for information."
45	"Use uncommon passwords & change them regularly."
46	"I read all I could about phishing scams. I was also educated about phishing attack during my time at university, but only because I did a computer security course."
48	"Do not open email from any bank."
49	"I don't know."
50	"I delete or ignore all phishing."
51	"I look at the URL and go from my own favourite link."
52	"Don't believe any cheap or discount staff from unknown website or spam."
53	"I RARELY buy things online. I usually access sites that I know to be reputable-Ticketmaster, Name Brand retailers etc. I still don't know if they are 100% safe, but they seem less likely to be operating scams."
55	"Carefully check the information on an unidentified email that ask to follow doing something."
57	"Delete any emails from banks. If I need information I phone them or login to my online banking facility."
58	"Never click in some website which I never heard and not familiar at all. And never believe the advertisement which looks very fake."
64	"Always observe strange email and don't fill in personal detail if unnecessary."
65	"Get a password that doesn't make sense at all. Be a security freak."
66	"Installed anti-virus software."
67	"I use cryptographically secured password, and very vigilant when using online banking, I only use my PC- NO NET CAFE."
68	"No opinion."

Respondent's ID	Discussion about methods that respondents used, or would use, to protect themselves or to solve the problems caused phishers (I15)
69	"The bank fixed it."
70	"No opinion."
71	"No opinion."
72	"No opinion."
73	"Caution, research, protection."
74	"Monitor my account closely. Check all entries-debits and credits and query with the bank."
75	"No opinion."
77	"Be careful. Don't easily get into those websites you didn't know."
78	"Installed an anti-virus program and I keep it up to date. Before I go onto Internet banking I check my anti-virus status."
79	"Information is power. Learn about how you can minimise risks."
80	"1. Wait for log out successful webpage to pop up before closing the window. 2. Turn on internet security. 3 Regularly check bank statement to monitor any suspicious withdrawal so as to take action immediately."
81	"I regularly change passwords; banking site has a click keyboard and is not keyboard entry."
82	"Most banking phishing (that I know of) is by fake e-mails from bank with links to phishing sites. I don't use links from bank emails."
83	"I did nothing."
84	"Rang the people and got their details i.e. fullname, employee numbers, and requested that they take the matter up with their suspicious. Then I requested a follow up and call from their supervisor as well as a letter of apology."
85	"Always contact the bank, for more information."
178	"Once my money had been taken out. I contacted the bank and I waited for 3 months for bank to investigate and to get money back."
181	"Questionnaires to the bank during the application for an online account & reconfirmation with the bank if the Users receive any email from the bank."
189	"Always use anti-spyware programs, beware of suspicious links and webpages."
191	"Install Internet software protection."
196	"Ask the bank manager."
207	"Keep everything confidential."

Respondent's ID	Respondents' opinions about installing an anti-malware application (I16)
1	"No, the user still needs to be aware."
2	"Do not know anything about Trojan etc."
3	"No. People installed with 'Rader Love' /cybernetics and who 'enjoy communication or live in community with others who are the same may have no problem in accessing personal information illegally."
4	"Yes."
5	"That's all I have."
6	"Yes, hope so."
7	"It is half the solution."
8	"No. There are stronger viruses that can break into the firewall and steal information."
9	"Anti-spyware and anti-virus is a must. But one has to also be careful in using your bank details i.e. shopping online. Check to see if webpage is secured."
10	"Unsure what level Trojans can now attack."

Respondent's ID	Respondents' opinions about installing an anti-malware application (I16)
11	"Yes."
12	"Yes, I updated regularly."
13	"Absolutely not. System penetration could be done by a variety of methods. So, penetrator may not use the same form of method to access information all the time."
14	"Yes."
15	"No, learn about security."
16	"No, but not sure."
17	"No, because there must be more powerful virus than this. But this anti-virus cannot secure computer 100%."
18	"Yes."
19	"Yes, I think so."
20	"I don't think so because the program to break these anti-viruses is improved."
21	"Not enough because some hackers still can attack people."
22	"Yes."
23	"If you have registered version of anti-virus in your computer. It may help to protect."
24	"No as you should not leave permanent information on the Internet. However, installing anti-virus program is a start, but you also have to be aware."
25	"Yes, I think that these are almost secure my computer from attacked."
26	"Yes."
28	"It is an essential measure, but it is not enough protection. Because each new released of anti-virus programs is the base for creating a new virus program."
29	"Probably 100% safe, but I'm not sure why."
30	"Depends on product and source of product. I am sure that computer use can be monitored by scanning devices but it would need to expend a lot of time/money for uncertain possibility of reward."
31	"Yes, to most of the computer users. Their way to protect their computer is very simple, so it is easy to be attacked."
32	"No. These things cannot find the newest virus."
33	"Yes, I think so."
34	"Yes, it will help."
35	"Helps with viruses but maybe not specific attacks."
36	"For my situation is enough."
37	"No, because many viruses have ability to break the anti-virus. Anti-virus companies improved their programs, the Trojans and any viruses have also improved their ability to break it."
38	"Yes, I do."
40	"Yes."
41	"No, it still has some viruses in my computer even people use anti-virus to protect online banking as well."
42	"Yes, these can secure your computer."
44	"No, in my opinion, it only protects the computer itself (not your personal information)."
45	"No, I think there is more secure protecting software."
46	"No, because if you visit insecure sites then you can pick up new viruses. Also, if you are unaware about what information you release into the web then you can be attacked."
47	"No, because there is always someone who has enough skills/technology to hack your computer. Those who can probably are not interested in hacking the average citizen."
48	"Need to do both - install security and take common sense precautious when dealing with private information."

Respondent's ID	Respondents' opinions about installing an anti-malware application (I16)
49	"Yes, it does help to protect."
50	"No, because some programs cannot kill it or some programs are out of date to kill new types of Trojans."
51	"Yes."
52	"That's not enough. Security software is needed in my computer, and account security management software as well."
53	"I don't know enough about those applications."
54	"I think it is the best place to start, but there are other steps that can be taken like changing passwords regularly, and making passwords more detailed and harder to figure out from personal information"
55	"No. it depends on a user himself to be careful about the received information."
56	"I assume it is sufficient because I don't know of other software. I believe my bank now provides security software to increase security."
57	"No. It's also crucial to be vigilant about emails offering prizes, helps, and free deals. "If it looks too good to be true, it is too good to be true." I also avoid suspect sites and check the origins of these mails. Many come from anonymous remailers and have bogus return address. I have black hole spam filters set up on my mail server, and brute force protection there, too. And I have my minimum of 8 characters, upper and lowercase and punctuation and am randomly generated. I run firewalls, antivirus that are auto updated and I have scheduled anti spyware scams. My critical data is backed up on an external drive, the family archives are in two places."
58	"Not enough because the virus types are changing all the time. Some protection software does not work in some cases. From my point of view, everyone should increase their knowledge for how to reduce the risk when using Internet."
59	"No opinion"
60	"It will help. No system would be 100% secure. Hackers or fraudulent people will not ever stop trying."
61	"Anti-virus and anti-spyware is good only if it is up-to-date."
62	"My computer is a company laptop which has anti-virus installed and updated regularly."
63	"No."
64	"Yes, I do."
65	"I don't believe/trust anything absolutely."
66	"So far, I think so, but we need to choose a good anti-virus."
67	"No- Zero day exploits and new viruses often circumvent this kind of software, and it can only prevent a small class of exploits."
68	"No. These programs can't stop you giving away your information if you get tricked into it."
69	"Probably not sufficient. My only machine is lunched to the net through a firewall and they also have anti-virus software, but spam still gets through."
70	"It's a start, but I think you need a variety of measures."
71	"I think that if someone REALLY can't to get into an account they will find a way. The only thing we can do is follow the security advice the bank gives us."
72	"Anti-virus software etc. is added protection, stealth software is also useful (if they can't see you they can't attack you) plus a common sense approach to suspect emails."
73	"Yes."
74	"I think it is a combination of spyware and checking accounts."
75	"I don't know."
77	"No. That software can prevent most of virus from your computer, but not at all. Every anti-virus has its weakness. If you don't update on time, it increases the risk to be attacked."
78	"Yes. By a using a reputable one and if it is kept up to date."

Respondent's ID	Respondents' opinions about installing an anti-malware application (I16)
79	"No. not enough. These software packages help but the hackers are always one step ahead. The software responds to new attack methods so they are always behind."
80	"No. Internet hackers are intelligent. If they want to hack into your account, they'll have hacked into the main bank organisation, not just from remote monitoring of customer's everyday usage."
81	"No."
82	"Keeps you really safe from spyware and Trojans if updated regularly."
83	"Probably it may help but not greatly."
84	"No. Quite often it takes the simplest of ideas to fool any system like the old saying 'Nothing is foolproof'."
85	"I am with Micro Trend and never been attacked before."
86	"Depends on the software but I usually have 3 types of software and this appears not to have any problem."
143	"Yes."
149	"Yes. Depending on the anti-virus."
165	"No, because they know how to get around things like that."
177	"No. Computer hackers are very skilled."
180	"No, if my computer is going to be attacked it can be attacked by a number of other things outside the classical virus/Trojan. Plus, virus coders always are a step ahead than anti-virus coders."
181	"It would reduce the risk and exposure, but Users security and reconfirmation with bank is a must before answering / replying any emails from bank."
187	"Somehow safe."
189	"Yes up to certain level, but still other security features and user awareness are important factors."
191	"Yes."
194	"Yes."
196	"Yes."
207	"No. You have to be vigilant of these attacks as well."
208	"No."
209	"No, you will still be vulnerable to phishing emails."

Respondent's ID	Respondents' opinions about countermeasures that could secure them against various kinds of online banking attacks (I17)
1	"Being aware, limiting online banking activities."
2	"Do not know."
3	"Again, ISP's anti-virus software and software designers in general, legislation and in particular log."
4	"I question every web page that I go to if I haven't specifically entered the URL or already trust the web."
5	"Don't know."
6	"Friends to be more vigilant in warning me."
7	"Not letting kids use the computer that banking is done on."
8	"Don't respond to junk or supposed "scam" mails that are obvious and should not be trusted."
9	"Never give my details to anyone that I don't know."
10	"I always 'junk' emails that I'm unsure of."
11	"I don't access account often+ change password every 6 months. I don't use birthday, maiden name."
12	"Don't open emails I not sure who is from."

Respondent's ID	Respondents' opinions about countermeasures that could secure them against various kinds of online banking attacks (I17)
13	"1. Never revealed your important information. 2. Ensure the legitimacy of the information provided."
14	"Have anti-virus software that is updated regularly."
15	"Never open an email from person I do not know."
16	"I don't know."
17	"If you are not sure whether the email comes from bank or not, then go to the bank and talk with them"
18	"I think people should have basic ability to distinguish the phishing activities or the bank should pay much more attentions."
19	"Use your related information as less as possible in public place or online."
20	"I ignore any strange mails."
21	"Keep personal information secret."
22	"Do not open the strange e-mails and websites."
23	"E-mails, webpages can be stopped by report them as abuse."
24	"Limit contacts and friends on the Internet, only use "secure" sources."
25	"I secure with combination in the keyboard and symbols and characters and numbers."
26	"Use complicated password."
28	"Do not be trustful. Do not provide your secret personal bank information to anyone."
29	"Use common sense. Be suspicious."
30	"Software methods- access methods in how pages are selected."
31	"Do not open the strange emails or websites."
32	"Do not tell anyone about my personal information on the Internet."
33	"I don't usually do not surfing and avoid entering my information in any website."
34	"No opinion."
35	"No opinion."
36	"Don't open any strange website. Sometime the link which sometime can attack you, just don't click it."
37	"Normal programme is enough to secure myself with changing password weekly."
38	"Be alert about those attacks."
41	"Don't put much true details of yourself on the Internet."
42	"Don't use personal information."
44	"Usually if it offers a "too good to be true" deal, I disregard or call to clarify."
45	"Do not open emails that do not look legitimate and do not click on the links provided."
46	"I do my major banking transaction behind the work formally. I also don't use my credit card for payment."
47	"Rely on anti-virus/spyware/Trojan software and common sense."
48	"I don't know phishing emails only use the computer with the university's firewall, even when working from home."
49	"Report spam and response that email."
50	"Using antivirus program and do not open any phishing."
51	"Don't click on links from emails or follow links to unknown places or companies."
52	"Don't believe any cheap or discount stuff from unknown website or person."
53	"I only use a work email and it has a very high-level of security."
54	"I am not familiar with the term phishing."

Respondent's ID	Respondents' opinions about countermeasures that could secure them against various kinds of online banking attacks (I17)
55	"1. Carefully check the source of email and check the detail in the email before processing something."
56	"I assume from running anti-virus software regularly & keeping it up to date."
57	"Delete any email from banks and other unknown sources without opening them. Never open a link from an unknown source If you must do so, then do it from a virtual machine that can be trashed and rebuilt Use a firewall with an auto updating blacklists, use an anti-spyware program with updating blacklists. Protect your email account with spanassasin. Demand identification from banks. Reply to borderline suspect emails to see if you get a response. Check grammar carefully in email from possibly legit sources. Check with the real organisation to see if they sent you mail."
58	"Install protection software and firewalls. And remember not to trust someone or webpages easily."
59	"I have Internet security and firewall."
60	"Employer issues warnings on possible phishing emails. I never open emails when I don't know who has sent them. I delete them."
61	"I don't know."
62	"Again as my laptop is a company laptop, all anti-virus programs are installed & updated regularly."
64	"Users need to observe before click on strange email or webpage."
65	"I trust to be a security freak of myself."
66	"Use anti-virus, don't trust the content of the email easily."
67	"Good understanding of email, website authentication and security concerns."
68	"Simply check URL, and 'from addresses' of any webpage or email I interact with."
69	"Change passwords."
70	"I turn the computer off when I'm not using it. Change the password often."
71	"Delete them or send them to the bank so they are aware it is happening."
72	"Common sense and anti-virus software."
73	"Install Norton and also care to detail."
74	"Delete cookies, check account regularly, use spyware, have a secure firewall."
75	"Confirm website address before use."
77	"Keep away from anything suspicious."
78	"By being alert to the fact that they happen. If I have any doubts about a site I do not leave any personal details."
79	"Delete all emails from banks. Never respond to any request for personal details in email. Have strong passwords, and change them often. Ensure you are using the correct URL for your bank."
80	"Use anti-spyware & virus protection."
81	"Anti-phishing software for email and web browser."
82	"Never enter personal data into anything."
83	"Do not give any private information online or through phone. Face to face is the best."
84	"I have 2 e-mails. One is used purely for business and my most trusted associates and the other is used should I need to provide one to an unfamiliar party."
85	"Install anti-virus/software."
86	"I usually do not answer or go to a site that I am not aware of."
107	"Don't open them."
128	"I'm very cautious about any emails that I receive especially if they are not people on my contact list."
140	"Deny anything that are not requested or known by me."
149	"Install a good firewall and spam detector."

Respondent's ID	Respondents' opinions about countermeasures that could secure them against various kinds of online banking attacks (I17)
165	"Unsure, will research it after completing this quiz."
177	"Do not give personal details/or any details."
180	"Be more paranoid. Seriously doesn't happen very often to me."
181	"Confirmation before and after any transactions is a must & keeping ourselves updated with banking news (threats, cases, additional online security features & etc.)."
189	"Being alert of suspicious webpages, using security software, reporting any suspicious attack to the bank."
191	"Don't open strange email & links."
196	"Prohibit or refuse to accept phishing e-mails."
207	"Updating protecting software whenever possible."
208	"Be aware of it and not giving any personal information to anyone or showing some of your personal information in public such as Facebook or Twitter."
209	"Only use trusted websites loaded from saved links. Also I ensure that for every website I sign up to I use a completely different password that is completely random instead of using a "global" password that a website could capture and use at other sites you visit."

Respondent's ID	Comments or additional opinions about the current or future situations of online scamming (I18)
1	"No opinion."
2	"No opinion."
3	"Not at this point."
4	"Improve login security for online banking."
5	"No opinion"
6	"No opinion"
7	"The banks are group to have to stay accountable and educated as the crooks out there are really computer savoy."
9	"No opinion."
10	"No opinion."
11	"Not really."
12	"TV commercials to educate users."
13	"1. ANZ has particularly started refunding the amount that customer loose in fraudulent activities. It is most welcome step which other banks have to immediately follow. 2. Financial institutions need to be more responsible and active in order to control such criminal activities. 3. Government should come with strong policies in against of such activities and in collaboration with financial institutions. 4. A number of social awareness program can be run (Unfortunately I have not seen any social awareness program in order to secure customers/individuals from predictors) 5. Commonwealth has SMS notification method which allows users to know about their spending."
14	"No."
15	"Improve the security mechanism."
16	"No."
17	"No comments."
18	"No opinion"
19	"Use your related information as less as possible in public place or online."
20	"Bank always asks people to change their passwords."
21	"Improve bank security system."

Respondent's ID	Comments or additional opinions about the current or future situations of online scamming (I18)
22	"No opinion."
23	"If the cybercrime continues to increase then bank should spend more money on Internet security."
24	"I use a digipass from my bank. 1 Personal code to access digipass.2. I type 8 numbers to get a code displayed in a digipass on a secure webpage. The security level of encryption is quite good-random digits. I believe that "hack" bank webpage is very difficult but possible. However, if money is stolen by phishing or similar cases, bank should compensate for it."
26	"No opinion."
28	"The method of banking attacks will improve in the future, because of improving security systems. Bank should spend more money to implement the newest security technologies and it will influence to clients expenses for bank services."
29	"I guess the problem is getting worse."
30	"No opinion."
32	"We cannot solve these problems."
33	"We have to secure our bank by ourselves, not rely on the bank much."
34	"Strong password required. Bank should have a very good security system."
35	"No opinion."
36	"Improve the bank system. Improve the bank identity security such as SMS security."
37	"No opinion."
38	"No opinion."
41	"No opinion."
44	"No opinion."
45	"No opinion."
46	"EDUCATED YOUR USERS! How about using your advertising budget to provide some user education on TV!"
47	"If people look the time to read the policies and terms of agreement, less people would fell for the scams."
48	"The banks need to be more protective about banking users about security issues & private use."
49	"It is a good topic and in the future, organisation must adapt changes to sustain in business from this source."
50	"Should provide more online security system."
51	"No opinion."
53	"No opinion."
54	"I almost feel that my online account is safer than the account linked to my debit card. There have been more incidents that I know of recently where people have had their accounts attacked after having used their cards at EFTPOS machines and ATMs."
55	"No opinion."
56	"Banks have a responsibility to provide a safe environment for online banking as it is in the banks' interests & to have allow customers visiting branches in person. Banks do not have enough physical branches to allow all their customers to visit & do their banking in person."
57	"We had better come up with a physical or biometric solution pretty fast if we're going to stay source. I'm OK about having an ID chip implanted, or using a fingerprint scan or finger length scan for ID."
58	"No opinion."
59	"Get to know how your bank operates."
60	"Online banking attacks will keep on happening. Banks need to be always on the lookout for new ways of phishing or hacking. Customers always need to keep checking statements and beware of any changes."

Respondent's ID	Comments or additional opinions about the current or future situations of online scamming (I18)
61	"I would like my bank to tell me more about the risks and signs of phishing."
62	"No opinion."
63	"More education from banks would be ideal."
64	"Bank's webpage can notice or warn to user about phishing or spyware before log in."
65	"All they care is changing you, not actually providing services."
66	"No opinion."
68	"No opinion."
69	"Keep us informed."
70	"I think people need more information on how to protect themselves."
71	"I believe my bank has good online security; however, I have not yet had this tested by fraudulent activity."
72	"No opinion."
73	"No problem so far."
74	"Using online site is a risk. Place limits on your accounts and check regularly and notify the bank."
75	"Users must be careful and banks must be responsible."
77	"No opinion."
78	"Unfortunately, the banks and anti-virus organisations can only be reactivating rather than proactive as it is unknown what new Trojans, spyware or adware are being developed."
80	"Make sure no one else knows your log in details. Do not log onto Internet banking more than 10 minutes per session. Using net code security token."
82	"No opinion."
83	"No opinion."
84	"Although the world is a much busier place, there still needs to be time made for phone calls. Most emails leave questions that can only be ensured by a person not a computer."
85	"No opinion"
86	"No opinion"
107	"Senior manager need to be vigilant with problems instead of results. The banking ombudsman needs to be actively involved."
140	"It's the option to use the fingerprint. An acceptable finger will further prevent copying."
143	"Banks should invest lots of money to look after our money. As we trust them with our money, they are responsible for it. As they make money from our money, so they have to look after it."
149	"No."
165	"I'd like to see that innocent people do not get attacked by things like these, and if they do the bank takes responsibility and pay for any losses."
180	"Stop thinking that customers are going to run away if you spend a little longer making sure that they are, who they are, when using your services."
181	"Banks should regularly run the test to ensure their online features, updating & increasing online security, face-to-face exposure and educating users is a must before any online account application is done."