

**A Social Networking Approach to Security
Awareness in End-User Cyber-Driven Financial
Transactions**

by

Rahul Maharaj

A Social Networking Approach to Security Awareness in End-User Cyber-Driven Financial Transactions

by

Rahul Maharaj

Dissertation

submitted in fulfilment
of the requirements
for the degree

Master of Information Technology

in the

**Faculty of Engineering, the Built Environment and
Information Technology**

of the

Nelson Mandela University

Supervisor: Prof. Rossouw Von Solms

April 2019

Declaration

I, Rahul Maharaj, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognised.
- This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institute.



Rahul Maharaj

Abstract

Cyberspace, including the internet and associated technologies have become critical to social users in their day to day lives. Social users have grown to become reliant on cyberspace and associated cyber services. As such, a culture of users becoming dependent on cyberspace has formed. This cyberculture need to ensure that they can make use of cyberspace and associated cyber services in a safe and secure manner. This is particularly true for those social users involved in cyber-driven financial transactions. Therefore, the aim of this research study is to report on research undertaken, to assist said users by providing them with an alternative educational approach to cyber security, education, awareness and training.

Acknowledgements

Foremost, I would like to express my sincere gratitude to my supervisor Prof. Rossouw von Solms for his continuous support during my Master's study. Furthermore, I would like to express my gratitude for his patience, motivation, enthusiasm, and immense knowledge. His guidance assisted me throughout the research and writing of this dissertation.

Furthermore, I would like to thank the following benefactors for their financial assistance:

- The financial assistance of the Council for Scientific and Industrial Research (CSIR) towards this research is hereby acknowledged.

Moreover, I would like to thank the following benefactors for their invaluable contribution:

- The South African Banking Risk Information Centre (SABRIC) is also hereby acknowledged, for their support in this study.

I must express my very profound gratitude to my family, my mother, father and dearest siblings for providing me with unfailing support and continuous encouragement throughout the process of researching and writing this dissertation. This accomplishment would not have been possible without you. Salisha, for being a role model. Ranvir for being there for me and pushing me to be successful. Thank you.

The RAB lab, the continuous friendship and encouragement all of you have provided shall not be forgotten. Finally, a very special person, thank you for standing by me and lifting me up on the cloudiest days. Thank you.

Contents

Declaration	i
Abstract	ii
Acknowledgements	iii
1 Introduction	1
1.1 Prologue - A Cyberspace Culture	1
1.2 Modern Services in Cyberspace	2
1.2.1 Cyberspace Usage by an Individual	3
1.2.2 Cyber-Driven Financial Transactions	3
1.2.3 Education, Awareness, and Training for Users of Cyber- Driven Financial Transactions	4
1.3 Thesis Statement	5
1.4 Research Objectives	5
1.5 Research Approach	6
1.6 Layout of the Study	7
1.7 Conclusion	8
2 Cyber Security Education, Awareness, and Training	9
2.1 Introduction	9
2.2 The Expanse of Cyberspace	10
2.2.1 Modern services in cyberspace	12
2.3 Information and Cyber Security	13

2.3.1	The "Human Factor" in Cyber Security	15
2.4	Cyber Security Education, Awareness, and Training for Organisations	19
2.4.1	ISO/IEC 27032 and National Cyber Security Framework . . .	20
2.4.2	Cyber Security Education, Awareness, and Training Defined	21
2.4.3	Cyber Security Education Awareness, and Training Mediums	22
2.5	Cyber Security Education Awareness, and Training for Social Users	24
2.6	Conclusion	26
3	Education, Awareness, and Training for Users of Cyber-Driven Financial Transactions	28
3.1	Introduction	28
3.2	Banking and Cyberspace	29
3.3	Current Education for Users of Cyber-driven Financial Transactions	32
3.3.1	Human Error - Typical User Errors and Threats	32
3.3.2	Current Educational Material Offered to Users of Cyber-driven Financial Transactions	38
3.3.3	A Critical Assessment of Educational Approaches offered . . .	40
3.4	Conclusion	42
4	Research Approach	44
4.1	Introduction	44
4.2	Research Design	45
4.3	Research Instrument Design	47
4.3.1	Criteria Influencing a Social Networking Approach	48
4.3.2	The Process to Identify Relevant Cyber Security Educational Topics	50
4.4	Conclusion	55
5	Social Networking Instrument	57
5.1	Introduction	57
5.2	Research Instrument Details	58
5.2.1	Cyber Security Quizzes	58

5.2.2	Educational Video Details	64
5.3	Data Gathering Aspect	71
5.4	Conclusion	72
6	Results and Analysis	74
6.1	Introduction	74
6.2	Implementation and Results of Experiments	75
6.2.1	Online Shopping Results	76
6.2.2	Mobile Banking Results	79
6.2.3	Card Fraud Results	82
6.2.4	Malware Results	85
6.2.5	Computer Hygiene Results	88
6.3	Analysis of Results	92
6.3.1	Lessons Learnt from Results	93
6.4	Conclusion	93
7	Conclusion	95
7.1	Introduction	95
7.2	Summary of Findings	96
7.3	Meeting the Objectives	98
7.4	Summary of Contributions	100
7.5	Future Research	100
7.6	Epilogue	101
	References	103
A	Topic Maps	110
A.1	Phase One Topic Map	110
A.2	Phase Two Topic Map	112
A.3	Phase Three Topic Map	114
B	Quiz Questions	116
B.1	Cyber Security Quizzes	116

C Results	132
C.1 Online Shopping Cyber Security Quiz Results and Video Statistics .	132
C.2 Mobile Banking Cyber Security Quiz Results and Video Statistics .	137
C.3 Card Fraud Cyber Security Quiz Results and Video Statistics . . .	142
C.4 Malware Cyber Security Quiz Results and Video Statistics	147
C.5 Computer Hygiene Cyber Security Quiz Results and Video Statistics	152
D Academic Publications	158
D.1 HAISA 2018 Publication	158

List of Tables

- 3.1 Educational Topics 39
- 3.1 Educational Topics 40

- 5.1 Online Shopping Sample Question 59
- 5.2 Mobile Banking Sample Question 60
- 5.3 Card Fraud Sample Question 61
- 5.4 Malware Sample Question 62
- 5.5 Computer Hygiene Sample Question 63

- 6.1 Educational Video Poll Results 92

List of Figures

2.1	2017 Data Breach Investigations Report Tactics Analysis (Verizon, 2017)	17
2.2	2017 Data Breach Investigations Report common (Verizon, 2017)	18
3.1	Timeline of Major Advances in Banking	31
4.1	Topic Map Version 1	52
4.2	Topic Map Version 2	53
4.3	Topic Map Version 3	54
6.1	Online Shopping Visitors and Participants	76
6.2	Online Shopping Completed Forms and Average Score	77
6.3	Online Shopping Participant Origin	77
6.4	Online Shopping Participant Device and Average Time	78
6.5	Online Shopping Video Statistics	79
6.6	Mobile Banking Visitors and Participants	80
6.7	Mobile Banking Completed Forms and Average Score	80
6.8	Mobile Banking Participant Origin	81
6.9	Mobile Banking Participant Device and Average Time	81
6.10	Mobile Banking Video Statistics	82
6.11	Card Fraud Visitors and Participants	83
6.12	Card Fraud Completed Forms and Average Score	83
6.13	Card Fraud Participant Origin	84
6.14	Card Fraud Participant Device and Average Time	84

6.15 Card Fraud Video Statistics	85
6.16 Malware Visitors and Participants	86
6.17 Malware Completed Forms and Average Score	86
6.18 Malware Participant Origin	87
6.19 Malware Participant Device and Average Time	87
6.20 Malware Video Statistics	88
6.21 Computer Hygiene Visitors and Participants	89
6.22 Computer Hygiene Completed Forms and Average Score	89
6.23 Computer Hygiene Participant Origin	90
6.24 Computer Hygiene Participant Device and Average Time	90
6.25 Computer Hygiene Video Statistics	91

Chapter 1

Introduction

Today, cyberspace, cyber-driven services and general cyber usage have become a fundamental part of modern society. This is particularly true for social users on cyberspace. These users are responsible for their own cyber well-being, including their cyber security, which leads to the problem that this particular research study investigates.

1.1 Prologue - A Cyberspace Culture

According to the Oxford Dictionary, cyberspace in the past was considered to be the environment in which communication between computer networks occurred (Oxford, 2016). Today, however, cyberspace is regarded as the internet together with connected computers and devices (Agnes, 2004). As cyberspace usage brings with it many benefits, it has made its way into users' daily lives. Cyberspace can be experienced in most aspects of life, for example on the smartphones we use to the systems that store our financial information. Therefore, reach of cyberspace is extensive and vast (Jardine, 2015).

Cyberspace has become an integral part of users day to day lives and as a result, a culture dependent on cyberspace has emerged. A cyberculture has emerged from the use of computer networks for communication, entertainment and business (Horn, 2010). As mentioned, cyberspace has become an integral part of modern

life especially to social users in a personal and professional manner. Cyberspace has grown from networks of computers to include various smart devices including smartphones and smart appliances. The Internet of Things (IoT), can be considered the latest addition to cyberspace and will continue to expand cyberspace.

1.2 Modern Services in Cyberspace

Clearly, cyberspace has and will continue to play a significant role in modern society and in general day to day usage. In addition to traditionally being regarded as communication between computer networks, cyberspace has adapted and evolved with modern times. As mentioned previously, this modern adaptation has typically formed new ways of behaving or doing things, referred to as cybercultures. These cybercultures make use of a host of services offered by cyberspace. These services vary per device but in literature three main service categories can be identified, namely; communication, entertainment and business (Horn, 2010). Smartphones are considered to be the most common form of accessing cyber-driven services, seeing an increase in adoption from 15% to 40% during the period 2011-2014 in South Africa (Kakihara, 2014). A large majority of individuals make use of cyberspace through their smartphones, making it a very individual, and private experience. As smartphones typically make use of applications or apps as its commonly known, it can be considered a general gateway to the internet and cyberspace (Carole Déglise, L Suzanne Suggs, 2012).

In March 2017, approximately 2.8 million and 2.2 million apps could be found on the Google Play Store and Apple App Store respectively (Statista, 2016). Apps may range from video games to navigation type apps. These applications are used by individuals in a very individual and personal manner. More than 50% of smartphone users have between 40 and 70 apps installed on their device and this implies that there can be vast variations in applications installed per user (Kearl, 2016).

1.2.1 Cyberspace Usage by an Individual

As smartphone applications are generally considered to be a gateway to cyber-driven services, they can be broadly classified as communication, entertainment and business type services (Horn, 2010).

Communication (mainly social networking) services often take the form of messaging and social networking applications, such as WhatsApp and Facebook. These applications allow individuals to communicate and interact with each other in various ways, from text-based communication to video communication (Madeline, 2016).

Entertainment services are based on various application types varying from video games, digital video (YouTube) to online gambling (Madeline, 2016).

Finally, business (lifestyle) services often comprise of financial banking services such as; online purchases, online banking, stock trading, etc (Madeline, 2016). Applications that fall into this category and involve some financial transactions can generally be considered to offer cyber-driven financial transactions services.

It is common knowledge that very little education and/or experience is required for individual to obtain access to and utilise any of these cyber-related services. This also holds for the users of cyber-driven financial transactions. Often it is a simple *click* or *tap*, and a user has access to various cyber service. When cyber-driven financial transactions are involved more risks and threats are normally associated. This is due to the financial nature of these services and potential financial gains for fraudsters. Many of these risks can be mitigated if the user is educated properly and made aware of associated threats (Bawazir, Mahmud, Molok, & Ibrahim, 2016). Therefore, a lack of proper education and awareness when using these cyber-driven financial transactions, puts an individual as well as the associated financial institution at risk.

1.2.2 Cyber-Driven Financial Transactions

As mentioned previously, owing to the monetary nature of cyber-driven financial transactions, users of these cyber services often face various threats. In December

2016, approximately 44 million South African users are involved in cyber-driven financial transactions (Staff Writer, 2017). Cyber-driven financial transactions constitute various tasks that involve any form of a financial transaction. These tasks range from credit card usage, online purchases, online banking and ATM usage. In 2016 a total of 8.8 million South African users of cyber-driven financial transactions, were affected negatively by cyber crime, thus roughly 20% of all users (Ombudsman Annual Report for Banking Services, 2016).

As shown from previous statements, users of cyber-driven financial transactions are indeed at great risk. Due to financial or monetary assets being involved, users of cyber-driven financial transactions are targeted far more often than regular users. It is for this reason that users of cyber-driven financial transactions need to have an acceptable level of education, awareness and training to mitigate the associated risks. The lack of an acceptable education and/or awareness levels results in a negligent or ignorant user, prone to lose of monetary assets.

1.2.3 Education, Awareness, and Training for Users of Cyber-Driven Financial Transactions

As stated in the Ombudsman Annual Report for Banking Services (2016), a large number of users are affected by cyber crime. This statement is also reflected in literature where users are often considered to be the weakest link in any information security process (Frauenstein & Von Solms, 2014). Education, awareness and training can aid in preventing incidents, which may result in a monetary loss from negligent or ignorant users (Whittman & Mattord, 2013). Through proper education, awareness and training it possible to foster a cyberculture of secure cyber users.

It is thus clear that users may be responsible for numerous cyber-driven financial incidents from their lack of related education, awareness, and training. Further, that education plays an important role in cyber-driven financial transactions to ensure that users are knowledgeable in utilising cyber services in a secure manner. Through proper education, that increases their awareness, it reduces their inherent negligence and ignorance and therefore mitigates related risks associated

with cyber-driven financial transactions.

Financial institutions, offering these cyber-driven financial services, do offer some educational material and services to help mitigate the associated risk. However, there is no standard set of educational topics nor is there a standard method of accessing such educational content. Even though the educational content is correct, the content is challenging to locate, users are not required to review the material nor is the presentation necessarily conducive to learning. It can be argued that there is a fundamental shortcoming with the approach being taken by financial institutions to educate their clients on how to safely and securely make use of cyber-driven financial transactions.

Thus, the problem that this research study aimed to address can be defined as:

Users of cyber-driven financial transactions are generally vulnerable to related security risks, because of their lack of sound cyber security education, awareness, and training.

1.3 Thesis Statement

In support of the stated research problem, the thesis statement addressed in this study can be phrased as follows:

A social networking approach can be used to make users of cyber-driven financial transactions less vulnerable to related security risks.

1.4 Research Objectives

The primary objective of this research study is to provide evidence towards proving the theory that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions, allowing them to conduct said transactions in a safer and more secure manner.

To achieve the primary objective, various secondary objectives were identified. The secondary objectives of this study are as follows:

- *Critically assess material currently offered to users of cyber-driven financial transactions.*
- *Determine an alternative educational approach, to educate users of the aforementioned audience.*
- *Determine which social networking approaches can be used.*
- *Identify typical topics and aspects that need to be educated to the audience at hand.*

This study attempts to provide evidence towards proving that a social networking approach to cyber security education, awareness, and training can be effective. Allowing users of cyber-driven financial transactions to conduct these cyber services safely and securely. Therefore, the above-mentioned secondary objectives aim to facilitate the attaining of evidence towards proving said theory. Hence, to achieve the primary objective of this research study, a suitable research approach must be devised.

1.5 Research Approach

At this stage, it is clear that there is a need to provide evidence in order to prove a theory. That theory being; a social networking approach can be used to make users of cyber-driven financial transactions less vulnerable to related security risks. As such, according to Olivier (2009), in order to prove a theory the research approach experimentation has been chosen. Therefore, the research approach followed for this research study is experimentation. More detail about the research approach and detail on the research design is presented in Chapter 4.

Notwithstanding the above, it is important to discuss the layout of the remainder of this research study.

1.6 Layout of the Study

Bearing the primary and secondary objectives of this research study in mind, this study will continue with a discussion on cybersecurity, education, awareness and training. Furthermore, the difference between cybersecurity, education, awareness, and training as they relate to organisational and home users will be highlighted. In this way, the discussion will establish the basis required for fully comprehending the research contribution made by this study.

Firstly, establishing the difference between organisational and home user efforts in cyber security, education, awareness and training will be discussed (Chapter 2). Furthermore, it is important to understand the cyber security, education, awareness and training currently available to users of cyber-driven financial transactions (Chapter 3). As such, establishing the need for the aforementioned research contribution.

Thus, in order to successfully fulfil the the primary object of this research study. A sound research approach needs to be followed (Chapter 4). The research approach aims to detail the approach taken to design the research instrument.

Subsequently, the chapter to follow (Chapter 5), discusses the research instrument and data gathering aspect in detail. Allowing for evidence to be gathered in order to fulfil the primary objective of this research study.

Chapter 6, discusses the results obtained from the aforementioned research instrument in detail, thus indicating that sufficient evidence was gathered to address the primary research objective of the study.

The final chapter (Chapter 7) concludes the research study.

- *Chapter 1: Introduction*
- *Chapter 2: Cyber Security Education, Awareness, and Training*
- *Chapter 3: Education, Awareness, and Training for Users of Cyber-Driven Financial Transactions*
- *Chapter 4: Research Approach*
- *Chapter 5: Social Networking Instrument and Data Gathering*
- *Chapter 6: Results and Analysis*
- *Chapter 7: Conclusion*

Additional information that augments the various discussions in this research study is included as appendices attached to the end of this dissertation. An academic publication that stemmed from this study has also been included in the appendices.

1.7 Conclusion

Cyberspace is of critical importance in the everyday lives of both organisations and social users. It is therefore important that they are able to make use of cyberspace and associated cyber services in a safe and secure manner. While organisations generally have best practices and international standards that assist them in ensuring safe and secure cyberspace usage, social users of cyberspace do not always have such resources available to them nor are these resources easily accessible or easy to understand.

Accordingly, the chapter to follow will discuss cyberspace, its importance in our day-to-day lives and how social users lack appropriate cyber-security education, awareness and training resources in comparison to organisations

Chapter 2

Cyber Security Education, Awareness, and Training

Today vast numbers of users are linked to cyberspace and make use of modern cyber-driven services every day. It is thus important that users understand the general cyber-related risks, specifically those related to the use of sensitive and personal information. With this in mind, it is critically important that these users are effectively educated on mitigating these risks. The aim of this chapter is to ascertain the current state of education, awareness and training among these users.

2.1 Introduction

We live in the era of technological revolutions. Approximately 200 countries worldwide are connected through a global "computer network" known as cyberspace (Polański, 2017). This linkage has been facilitated by the widespread adoption of computers, smartphones and other smart devices. At present 2.62 billion social users are actively making use of cyberspace and its associated cyber-driven services (Portal, 2018b). Social users extensively make use of cyberspace and cyber-driven services the most. In this sense social users can be defined, for the purposes of this study, as those that make use of smartphones, tablets and other internet enabled devices for personal use. These social users are everyday people, using cyberspace

and its associated cyber-driven services such as, browsing the World Wide Web or conducting mobile banking.

As organisations and social users increasingly embrace the use of technology, cyberspace is seen as the medium through which information can be transmitted, as organisations and social users embrace the technology. Furthermore, the increased access users' have to cyberspace and other cyber-driven services connects the world, thereby rendering social users' information accessible via different platforms. As such, cyberspace has laid way to an increasingly online and "*plugged in*" society. Cyberspace offers numerous cyber-driven services and social users have access to a vast array of options and platforms. As social users make use of cyberspace, there is a need for them to use these cyber-driven services in a secure manner. These safe and secure ways to utilise cyberspace is best instilled in these social users by means of cyber security education, awareness and training.

To address the need for education, awareness and training among cyberspace social users, this chapter will begin by describing cyberspace and its various associated services. Secondly, the chapter will discuss cyber and information security and finally, cyber security education, awareness, and training for both organisational and social users will be discussed. The aim of which is to contrast the efforts made in organisations compared to that of social users. Highlighting the lack of efforts in the social user space and the need for cyber security education, awareness, and training.

2.2 The Expanse of Cyberspace

Cyberspace was originally defined as an environment in which communication through computer networks occurred (Oxford, 2016). Cyberspace was seen as tool for organisations, rather a free medium for all to use. Cyberspace was used in organisations, enabling them to communicate over large distances. However, in recent times, cyberspace is regarded as the internet together with connected computers and devices such as smartphones. Hence it is being a boundless environment, providing access to information interactive communication and services

(Agnes, 2004). Therefore, cyberspace may be seen to cross boundaries connecting devices to people and *vice versa*, thereby sharing information between multiple platforms. As cyberspace became more accessible from personal devices linked to the internet and the suite of cyber-driven services grew to include numerous applications (Apps), the home or social user became much more active on the cyberspace highway. As previously mentioned, cyberspace and associated cyber-driven services have found their way into modern society, as users depend on them on a daily basis. Cyberspace and associated cyber-driven services are linked to the smartphones of social users and the information systems of organisations. The reach of cyberspace is extensive and vast, making its way into many aspects of life (Jardine, 2015).

Cyberspace has become a major part of users' day-to-day lives and as a result, a culture dependent on cyberspace has emerged. Horn (2010) asserts that, a cyber-culture is formed from the use of computer networks for communication, entertainment and business. Moreover, cyberspace has become an integral part of modern life, having grown from networks of computers to include various smart devices, such as smartphones and smart appliances, which generate, store and communicate large amounts of data and information. The internet of things (IoT), can be considered the latest addition to the ever-growing range of cyber-driven services. It can be defined as the interconnection of sensing (capturing data) and actuating (interacting with users) devices by enabling them to share information across platforms and devices (Gubbi, Buyya, & Marusic, 2013).

Cyberspace, as indicated can be seen in many aspects of day-to-day life. Users can access it from a variety of devices, for example, computers, tablets and other internet enabled devices. Nevertheless, the most common method of access is the smartphone. The smartphone has seen tremendous growth over the past few years, with current smartphone usage being estimated at 2.53 billion users as of 2018 (Portal, 2018c). Smartphone users in turn make up 52.64% of all internet traffic (Portal, 2018a). This results in a large number of social users accessing cyberspace via smartphones, constantly interacting with their cyber-driven services in some manner. The increasing usage of smartphones by social users, in turn, results in

cyberspace and cyber-driven services being accessed more frequently. Users access these cyber-driven services constantly, and this is evident by the manner in which users engage with one another via social media or perform cyber-driven financial transactions through web browsers or mobile applications.

There are numerous cyber-driven services available to those with access to cyberspace. These modern services can be grouped according to how they are used by both organisations and social users. Typically cyber-driven services allow users to access cyberspace either through computers, tablets or smartphones. These modern cyber-driven services will be discussed below.

2.2.1 Modern services in cyberspace

Clearly, cyberspace plays and will continue to play a significant role in modern society and in general day-to-day usage. In addition to being traditionally regarded as communication between computer networks, cyberspace has adapted and evolved with modern times. As mentioned previously, this modern adaption has typically formed new ways of users behaving or doing things, referred to as a cyberculture (Horn, 2010). Cyberspace today offers a host of services, these cyber-driven services are core to how users, in particular social users interact with cyberspace. Such services vary according to device but in literature three main service categories can be identified, namely; communication, entertainment and business (Horn, 2010).

As smartphones are generally considered to be a gateway to cyber-driven services, they can be broadly classified as firstly offering communication, secondly entertainment and thirdly business-related type services (Horn, 2010).

Firstly, communication (mainly social networking, e-mail and instant messaging) services often take the form of messaging and social networking applications, such as WhatsApp and Facebook. These applications allow for individuals to communicate and interact with each other in various ways, from text-based communication to video communication (Madeline, 2016).

Secondly, entertainment services are based on various application types varying from video games, digital video (YouTube) to online gambling (Madeline, 2016).

Finally, business (lifestyle) services often consist of financial banking services such as, online purchases, online banking and stock trading (Madeline, 2016). Usage that fall into this category and involve some financial transaction can generally be considered a cyber-driven financial transaction.

These cyber-driven services can be seen to form part of both organisations and social users. Organisations typically use a combination of these categories. This combination forms a complex information system which allows organisations to function seamlessly. Organisations integrate cyber-driven services through their information systems, whether that be for enabling cloud computing or online storage for example. Unlike organisations, social users typically access these cyber-driven services through applications or Apps as they are generally termed. Social users use a combination of these cyber-driven services but tend to use them individually for example, applications on smartphones or through web browsers. Therefore, as argued in above cyberspace plays a significant role in organisational and social users day-to-day activities.

Thus, both organisational and social users use and rely on cyberspace and cyber-driven services in any normal day. This strong reliance on cyberspace and the systems around it, results in users accessing various services which can be seen as sensitive or communicating information that can be classified as sensitive or private. These sensitive cyber-driven services and associated information used and communicated by social users can fall into any of the above-mentioned categories. An example of this would be a social user accessing private information in an e-mail or conducting online banking. As such this sensitive information needs to be protected by the user in some manner. The following section will discuss the need for information and cyber security.

2.3 Information and Cyber Security

As stated by Von Solms and Van Niekerk (2013), the concept of cyber security is used interchangeably with the concept of information security. The need for cyber security became apparent in the early years of the technological revolution

era (Cabaj, Domingos, Kotulski, & Respício, 2018). As the number of critical services, interconnected computers, information and "things" in cyberspace steadily increased, the impact of cyber-attacks became clear (Cabaj et al., 2018). This is true more than ever, due to the large amount of organisations and social users making use of cyberspace and its associated cyber-driven services. In previous years a large majority of users relayed on information and the systems that process, store and transmit said information in their day to day lives. Furthermore, due to this dependence users had on information, the value of information-related assets was seen to surpass that of physical assets (Von Solms, Thomson, & Maninjwa, 2011). However, today such information forms part of cyberspace and as such information security can be seen to form part of cyber security.

As information was and still is, as valuable as other assets it requires protection (Posthumus, Solms, & King, 2010). The protection of information should be a priority to anyone involved in the information process. The aim of information security is to maintain business continuity and minimise organisational damage by preventing and minimising the impact of security incidents (Von Solms, 1998). Information and its related systems face various threats, from a technical, administrative and operational level. The concept of information security, can be seen more prevalent in organisations compared to cyber security. The concept of cyber security in contrast, goes beyond traditional information security to include not just the protection of information asset but also other asset's, including the user (Von Solms & Van Niekerk, 2013).

Security is about the protection of assets from various threats and vulnerabilities. Security processes usually deal with the selection and implementation of security controls, commonly referred to as countermeasures which help to reduce the risk posed by these vulnerabilities (ISO/IEC, 2013; Gerber & Solms, 2005; Farn, Lin, & Fung, 2004). Cyber security countermeasures consists of tools, policies, security concepts, best practices and training (Von Solms & Van Niekerk, 2013). The appropriate use of these countermeasures allows for the resultant protection of both organisational and user' assets in cyberspace.

Cyber security countermeasures, as mentioned previously can consist of various

mechanisms. Furthermore, these countermeasures can be classified according to aspects of cyberspace they attempt to protect. They can broadly be classified as data security, software security, system security, organisational security and human or societal security (Cabaj et al., 2018). Each of these classifications will briefly be discussed. Data security consists of the appropriate use cryptography, data integrity and data protection (Cabaj et al., 2018). The ultimate goal being the protection of data privacy. Software security consists of countermeasures designed around software used in cyberspace. It involves secure software development, malware analysis and secure software engineering (Cabaj et al., 2018). System security, is a broad area and can include physical security of cyber enabled devices and mobile security (Cabaj et al., 2018). Organisational security focuses on protecting an organisation and its working parts, countermeasures that fall under this classification includes disaster recovery, business continuity and compliance (Cabaj et al., 2018). While organisational security focuses on protecting the organisation, human security focuses on protecting the individual. Education is a key component to each of these classifications. Whittman and Mattord (2013) defines, an information system is an organised combination of users, hardware, software, communication networks, processes and data resources in an organisation. In most, information systems the user is always present. This involvement adds an element of risk if a user is not aware of the threats (ignorance) cyberspace usage contains or acts in a careless manner (negligence), putting themselves at risk.

The understanding that user involvement is part of most cyberspace interactions is of vital importance to this research and therefore will be explained in more detail.

2.3.1 The "Human Factor" in Cyber Security

In the preceding section, it was highlighted that users play a significant role in various activities in cyberspace. Most organisations understand cyber security as a technical issue, but in recent years began to understand the importance users play regarding cyber security. However, users are a indeed key a factor in the

cyber security process as they are often gateways for causing a loss in information. Generally, users of cyber services can be regarded as those users not well versed in information technology *per se*. These typical general users are normally woefully unprepared to deal with cyber-related threats such like: phishing scams and social engineering schemes (Florentine, 2015).

As previously stated typical countermeasures in cyber security aim to protect both organisational and user's assets in cyberspace. These countermeasures are normally well designed and implemented yet no matter how well designed and implemented, countermeasures normally rely on people. An example of this would be, a user who forgets to close a security door and thus, granting unauthorised access to sensitive or private information. Consequently, no matter how complete or effective any cyber security countermeasures may be perceived to be, it will only be as effective as the associated actions of the user using it or involved in the security process.

There are numerous examples where general user error either through negligence or ignorance led to cyber security breaches which resulted in financial loss or other forms of damage. The 2017 Data Breach Investigations Report identifies user negligence or ignorance as a major point of weakness in the cyber security process (Verizon, 2017). Figure 2.1 below represents the tactics used by attackers in the 2017 Data Breach Investigations Report.

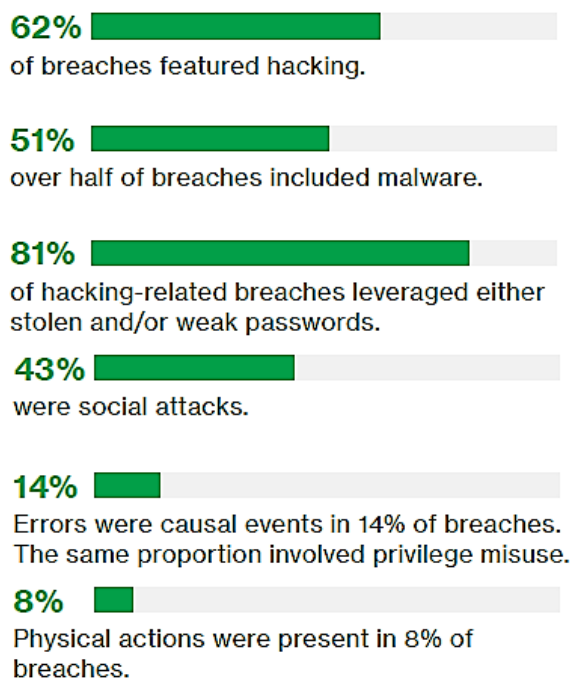


Figure 2.1: 2017 Data Breach Investigations Report Tactics Analysis (Verizon, 2017)

As seen in figure 2.1, it shows that, 81% of incidents featured breaches involving stolen or weak passwords, while 43% were social attacks. Therefore, it can be argued that a large majority of breaches may be attributed to user negligence (e.g. allowing passwords to be stolen) or ignorance (e.g. not creating strong enough passwords). Furthermore, as seen in figure 2.2, 66% of malware related breaches were caused by user negligence or ignorance as identified by the 2017 Data Breach Investigations Report (Verizon, 2017). It can be argued that even though malware is a technical threat however, due to user negligence or ignorance, malware was able to be installed on organisations information systems, compromising cyber security in some form.



Figure 2.2: 2017 Data Breach Investigations Report common (Verizon, 2017)

Frauenstein and Von Solms (2014) confirm that users are always involved in the information security process, whether directly or indirectly, and therefore an element of risk is present resulting from user negligence or ignorance. In order to address this user negligence or ignorance, general users need to have requisite knowledge of the role they play in security if they are to conduct themselves securely. Hence, users need to be educated, as such education will lead to the establishment of a culture of secure users. This is also true for social users, who may not always be aware of the risks that threaten the security of their information or the value of this information.

Thus, it may be concluded that information security forms part of cyber security, and thus the users involved in the cyber security process are critical to its success. However, in the majority of cyber security breaches the users are at fault, whether through negligence or ignorance. Consequently, human users play an important role in ensuring cyber security. As such, cyber security education, awareness and training may be used to combat the weakness users bring to the security of cyberspace.

Efforts made to educate users in order to address this inherent negligence or ignorance will be examined in the next sections.

Efforts made to educate users, in order to address negligence or ignorance will be examined in the next sections.

2.4 Cyber Security Education, Awareness, and Training for Organisations

As mentioned previously cyberspace, information and communication technology (ICT), and the internet have become core to a successful, modern organisation (Von Solms & Solms, 2008). This is also true for social users, who rely on cyberspace to conduct day-to-day tasks. As such, both organisational and social users need to ensure that they use cyberspace efficiently and securely in order to benefit from it the most. Cyberspace, can be regarded as the interaction between software, cyber services and people. Thus, due to its complex nature it needs to be managed correctly to allow organisations to make use of it successfully (ISO/IEC 27032, 2012). As such, international organisations have formed in order to ensure the correct management of cyberspace. In turn releasing various cyber security standards, frameworks, and best practices in order to aid organisations. These aforementioned standards, receive much support from industry and often are regarded highly among industry professionals. One such example of a major standard being the ISO/IEC 27032 and a major framework being the National Cyber Security Framework.

Such standards and frameworks address many issues in cyber security. One critical issue covered is that of cyber security education, awareness and training. The subsection that follows will discuss a prominent standard and framework and the cyber security education, awareness and training they envisage for users in organisations.

2.4.1 ISO/IEC 27032 and National Cyber Security Framework

Information and communication technologies have become indispensable to the modern lifestyle (Klimburg, 2012). With the increasing significance and role cyberspace plays in organisations, there is an urgent need for adequate countermeasures to ensure organisations and users security (Disterer, 2013). As such, organisations are put under pressure to ensure their cyber usage is conducted in a secure manner, including usage by users. Numerous standards and frameworks have therefore been created in order to aid organisations, by means of education, to address user negligence or ignorance. The ISO/IEC 27032 standard includes cyber security education, awareness, and training as a major point within its code of practice. As stated by ISO/IEC 27032 (2012), an effective way to confront cyber security risks involves a combination of multiple strategies. Education, awareness, and training can be seen as said strategy (ISO/IEC 27032, 2012). Education can allow other technical countermeasures to perform as intended by reducing user negligence or ignorance.

Similar to the ISO/IEC 27032 standard, the aim of the National Cyber Security Framework is to ensure cyber security is implemented effectively, however at a national level. The framework is specific to the United States of America, however the principles apply worldwide. The framework proposes five mandatory activities to ensure cyber security is maintained at national level: military cyber, counter cyber crime, intelligence and counter-intelligence, critical infrastructure, and lastly cyber diplomacy (Klimburg, 2012). Alongside the aforementioned activities three cross mandates are proposed. Education, awareness raising, and training is a key cross mandate (Klimburg, 2012). The aim of which is to tie the previous mandates together, ensuring they are implemented and used effectively. Thus, education, awareness raising, and training exercises are an important feature of a national cyber security program.

As a result, and stated by the preceding subsection, governments and organisations require cyber security education, awareness, and training in order to practice sound cyber security. As such, educating users in their organisations will allow

them to become a cyber security strength instead of a weakness. This in turn, allows them to adhere to aforementioned standards, frameworks and other best practices. These standards, frameworks and best practices serve as a road map to implement cyber security and in turn cyber security education, awareness, and training. The need for cyber security education, awareness, and training can be seen not just in organisations but also at a national and international level. Thus, it can be considered a necessity in any cyber security program for users. The following section will describe more detail of a typical cyber security education, awareness, and training programme.

2.4.2 Cyber Security Education, Awareness, and Training Defined

As stated in the ISO/IEC 270032 standard, security education awareness, and training, needs to be an ongoing endeavour by organisations (ISO/IEC 27032, 2012). Education can be regarded as key to turning a weakness into a strength, as in literature users are often referred to as the weakest link (Frauenstein & Von Solms, 2014). In order for an organisation to have adequate cyber security, users need to have the desired knowledge and attitude towards security as well as understanding the role they play in it. As such, in order for users to have said knowledge and attitude, they need to be made aware of their role and educated appropriately. Cyber security, education, awareness, and training, can be considered a "human" appropriate control (ENISA, 2012).

In order to appropriately and effectively manage users behaviour, cyber security follows three main concepts, namely: education, awareness, and training. These three concepts will briefly be described.

- **Education:** The concept of education is to combine all of the security skills and competencies for the desired user. Allowing the user to subconsciously conduct themselves in a secure manner. This will allow users to naturally go about their work in a secure manner.
- **Awareness:** The aim of awareness is to draw attention to security issues and

the role users play in security. Awareness needs to be carried out effectively in order for users to understand the importance of security and the role they have in it.

- **Training:** Training is focused on users acquiring skills in order to deal with security threats. An example of appropriate training can be users being taught the proper procedure to report phishing attacks.

As reported by SANS institute (2015), one of the best ways to make sure company employees will not make costly errors with regard to information security is to initiate company-wide security awareness training initiatives. These initiatives can include, but are not limited to, classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters (SANS Institute, 2015). These methods can help ensure employees have a solid understanding of company security policy, procedure, and best practices (Simone, 2009).

These initiatives or mediums will further be discussed in the next subsection.

2.4.3 Cyber Security Education Awareness, and Training Mediums

As mentioned previously, cyber security education, awareness, and training should be an ongoing endeavour. Cyber security education, awareness, and training can be delivered through various mediums. The mediums and options available for delivering cyber security education, awareness, and training programs are very similar to those used in delivering other employee awareness programs such as sexual harassment (Hansche, 2001). Examples of cyber security education awareness, and training mediums include:

- **Posters:** Posters with meaningful messages relating to cyber security can be placed around the work area, to serve as a reminder.
- **Posting of security slogans:** Slogans are quick and short phrases that will help jolt the memory, allowing the reader to recall lessons previously taught.

- Video: Videos are often used during formal cyber security awareness training; they serve as great educational tools, as users are more likely to pay attention to a short video.
- Classroom instruction: Usually given at certain points during a work day. This helps to break up knowledge received and make it more "digestible" for users. These are typically conducted when new employees are brought into an organisation.
- Computer-based delivery: Increasingly common, computer-based delivery can take the form of video, games and quizzes.
- Flyers and brochures: Easy to read and circulate among users. Typically used when a large number of people need to receive a short yet specific message.
- Trinkets: Trinkets serve as reminders, something small with some cyber security awareness meaning, for example a coffee mug with an awareness message.
- Monthly notices such as e-mail or messages: E-mail can serve as short reminders and reach many people
- Formal training program: A formal program often takes the most time, but may have the most impact, allowing users a more structured educational approach.

Organisations may not always make use of all the mediums; however, most organisations use a mixture of mediums in order to address continuous security education, awareness, and training. As identified by Hansche (2001), it is important to note that education, awareness, and training is an ongoing process. It is important to continuously remind users of cyber security, creating a culture of secure users. Cyber security awareness programs can take many different forms and/or approaches. No matter the method, it is vital that some form of cyber security awareness does take place. This is echoed by both the ISO/IEC 27000

family of standards and the National Cyber Security Framework (ISO/IEC 27032, 2012; Klimburg, 2012). This allows for due care and due diligence to be shown on behalf of the user and organisation. As previously mentioned, cyber security education, awareness, and training is there to turn a security weakness into a strength.

Many organisations have come to the understanding that their own employees are the biggest threat to their cyberspace assets including information. As such, cyber security education, awareness, and training needs to be an important aspect when enforcing cyber security programs (Dodge Jr, Carver, & Ferguson, 2007; Shaw, Chen, Harris, & Huang, 2009). In order to address the "human" factor, users need to have the appropriate knowledge. This is reiterated by both industry, in form of the aforementioned standards, and in research by numerous authors

Thus, users in organisations are exposed to cyber security education, awareness and training through their respective organisation. Due to the previously mentioned standards, frameworks and best practices users often receive well structure and topical cyber security education, awareness, and training. As such, organisational users benefit from cyber security education, awareness, and training. Thus, enabling them to make use of cyber-driven services in a secure manner. This is in stark contrast to social users outside of organisations. The section to follow will discuss cyber security education, awareness, and training in the social user space.

2.5 Cyber Security Education Awareness, and Training for Social Users

As mentioned earlier, demands are placed on organisations to have sound cyber security and an appropriate level of information security. This should result in users receiving ongoing cyber security education, awareness, and training. This is in stark contrast compared to cyber security education, awareness, and training efforts in the social user space. As mentioned previously, cyberspace plays a significant role in social users' lives. However, compared to users in organisations, social users are not held accountable by higher authorities to ensure they practice

sound cyber security. Due to that fact, there is a lack of enforcement for social users to take part in cyber security, education, awareness, and training events or programs (Kritzinger & Von Solms, 2010). Furthermore, social users also need to be made aware of the value their cyber presence possess, similarly the need to be educated on cyber threats they face.

Approximately 22.5 million South Africans make use of cyberspace, whether that be for communication, entertainment or business purposes (Shapshak, 2017). Therefore, social users can be seen to comprise a large percentage of cyber usage. Social users are increasingly exposed to security threats due to their smartphone and computer use (Furnell, Bryant, & Phippen, 2007). As such, it can be seen that a large percentage of South African citizens are at risk, if they lack an appropriate level of cyber security education, awareness, and training. An appropriate level of cyber security education, awareness and training is imperative in order for social users to use cyber-driven services in a secure manner.

As indicated by Kritzinger and Von Solms (2010), social users are vulnerable due to many factors, one major factor being lack of awareness around using cyberspace. The following statistics support the need for cyber security education, awareness, and training among social users:

- As of 2017 there are approximately 22.5 million South Africans using cyberspace (Shapshak, 2017).
- Due to social users' unfamiliarity with technology, they have a limited ability to recognise threats and understanding the need for protection (Furnell, Tsaganidi, & Phippen, 2008).
- As of 2016 1 in every 1846 e-mail received by social users is an phishing attempt, while the overall e-mail malware rate is 1 in 220 e-mails (Symantec, 2016).
- According to the Symantec Internet Security Threat Report (2016), 78% of scanned websites contain vulnerabilities, which if exploited may allow malicious code to be run without user interaction, potentially resulting in a data breach.

- Unlike organisations, social users do not have their cyberspace usage governed (Furnell et al., 2008).
- Social users financial service companies are being targeted by phishing attacks more than any other industry (APWG, 2017).

As the number of social users accessing cyberspace for social networking, on-line banking and many other cyber services are constantly increasing. The lack of cyber security awareness can be seen as a major problem to social users, potentially exposing themselves to unnecessary or easily avoided risks (Kritzinger & Von Solms, 2010). The amount of cyber security education, awareness, and training programs available to social users is far less compared to organisations. Often, these programs are difficult for social users to find, if available (Kritzinger & Von Solms, 2010). As such, many social users tend to forgo cyber security education, awareness, and training. Thus, exposing themselves to numerous risks.

As stated by Furnell et al. (2007), even advanced social users are vulnerable. This is particularly true for social users, who "believe" they are security aware. Therefore, it is important that all social users are made aware of the risks around their cyberspace usage. Furthermore, they need to be educated in order to be able utilise cyberspace and associated cyber-driven services in a secure manner. As such, cyber security education, awareness, and training as in organisations and governments should be incorporated into social users cyberspace activities. Therefore, social users do not receive adequate cyber security education, awareness, and training. Thus, negatively impacting their cyberspace and cyber service usage.

2.6 Conclusion

As with other security initiatives, cyber security requires teamwork from all parties involved from organisations to social users (WaterISAC, 2015). Cyber security education, awareness and training can be seen as mandatory in any cyber security program (ISO/IEC 27032, 2012; WaterISAC, 2015; Klimburg, 2012). As such, regardless if involved in an organisation or home, users require an appropriate

level of knowledge and the desired attitude to conduct themselves securely in cyberspace. This chapter examined the role cyberspace plays in both organisations and social users day-to-day activities. The concept of cyber security education, awareness, and training was also discussed, showing that organisations require sound cyber security practices. As such, cyber security education, awareness and training is a requirement for all employees exposed to organisational information. It was also highlighted that due to aforementioned standards, organisations have a "road map" in place to develop these cyber security programs. Unlike organisations, social users do not have a set requirement and are thus, not prepared to deal with possible threats in cyberspace. Hence social users are, either through negligence or ignorance, vulnerable to cyberspace threats. As such, the objective of this chapter has been met; contrasting the difference in cyber security education, awareness, and training for organisational and social users as well as highlighting the lack of appealing cyber security education, awareness and training for social users. As indicated by Furnell et al. (2008), social users are limited when it comes to recognising these threats and lack understanding as to why their information needs protection. The chapter to follow, will discuss a particular vulnerable group of social users, those that are conducting cyber-driven financial transactions.

Chapter 3

Education, Awareness, and Training for Users of Cyber-Driven Financial Transactions

Social and organisational users rely on cyberspace for many of their normal everyday operations, including cyber-driven financial transactions. The aim of this chapter is to show how vulnerable users of cyber-driven financial transactions are and that effective cyber security education, awareness, and training are critically important to allowing said users to conduct such cyber-driven financial transactions safely and securely.

3.1 Introduction

From the preceding chapter, it is clear that cyberspace plays an important role in modern organisations and in social cyberspace users day to day operations. Cyberspace and associated cyber-driven services can be seen as core to everyday life. As social cyberspace users are engaged constantly in cyberspace through the internet and their applications (apps) on smartphones and computers, they are

seen to make use of cyberspace even more so than organisations. As such, social cyberspace users constitute a large demographic of cyberspace. Moreover, due to their reliance on cyberspace they need to be able to make use of these cyber-driven services securely and safely. This is particularly true for those social cyberspace users engaged in cyber-driven financial transactions. Cyber-driven financial transactions, for the purposes of this study can be defined as, any financial transaction that involves cyberspace or the internet. Common examples include automated teller machines (ATM) usage, credit card usage, online purchases and debit card usage. Due to the financial nature of these cyber-driven services, any loss of cyber security can be devastating, resulting in a monetary loss.

The issue of effectively educating users of cyber-driven financial transactions to aid in the secure use of the aforementioned services will be addressed in this chapter. As such, this chapter will begin by describing the relationship between banking and cyberspace to illustrate the shift in responsibility from the financial institute to users of cyber-driven financial transactions. The section to follow will discuss the current state of education available to said users. This discussion will also include typical threats users face and mistakes made by users. To conclude, a critical assessment of current educational approaches offered to users of cyber-driven financial transactions will be discussed. Therefore, the aim of this chapter is to highlight the lack of appealing cyber security education, awareness, and training for users of cyber-driven financial transactions.

3.2 Banking and Cyberspace

As mentioned previously, cyberspace plays a significant role in modern organisations. Therefore, cyberspace can be seen to form part of any modern financial institution. Financial institutions or banks can be regarded as one of the oldest formal professions in the world (Gordon, 2003). To understand how banking has evolved overtime, to incorporate cyberspace, a brief history of banking will be provided. The Bank of England, established in 1695, was the first bank to issue banknotes (West, 2015). This moment in history can be seen as the start of

modern banking as it is known today. This also began the trend of banks shifting responsibility to users. By 1745, the standardised printing of notes had begun (West, 2015). Therefore, allowing average users to carry cash and adding an element of risk around their finances. The issuing of bank notes allowed users more financial freedom. However, it shifted more responsibility onto the user, as he/she needed to keep track of physical cash. The 1960's saw the advent of the automated teller machine (ATM), which again can be seen as an attempt from banks to move users out of branches and shifting more responsibility on to said users (Batiz-Lazo, 2013). The advent of the ATM brought along many risks, including the possibility of card swapping or skimming. Therefore, adding an element of risk to users. As such, if users are not aware of the dangers surrounding ATM usage or educated in ways to prevent them falling victim to these dangers, there is a possibility of them being defrauded. Alongside ATM's, banks began investing heavily in computer technology, moreover to automate manual tasks and give users access to more financial services. This was the early signs of banks increasing their cyberspace usage, in order to grow their business and offer cyber-driven services. Towards the early 1970's the first payment systems started developing, leading to electronic payment systems similar to today's systems. In turn, increasing cyberspace usage by banks. The introduction of electronic payment systems, shifted even more responsibility to users as they now needed to manage their own payments. The early 1980's saw the introduction of online banking for the first time in the world. Online banking allowed users', full control of their own financial interests (Cronin, 1998). Online banking brought many advantages to users, including permanent access to banking, ease of use and access anywhere. Online banking brought banking into the 21st century, fully integrating financial services with cyberspace. Consequently, online banking shifted more responsibility onto users of cyber-driven financial transactions. If users are not technologically inclined or well versed with how the Internet works, he/she can be susceptible to may online threats. The smartphone brought with it mobile applications and in turn mobile banking applications. Mobile banking through applications started in the early 2000's, reaching popularity approximately in 2008 (Medne, 2016). As

seen in Figure 3.1, banking applications on smartphones at present is regarded as their latest cyberspace endeavour. No more were users restricted to using online banking by means of a desktop or laptop. Users were free to conduct banking on the go.

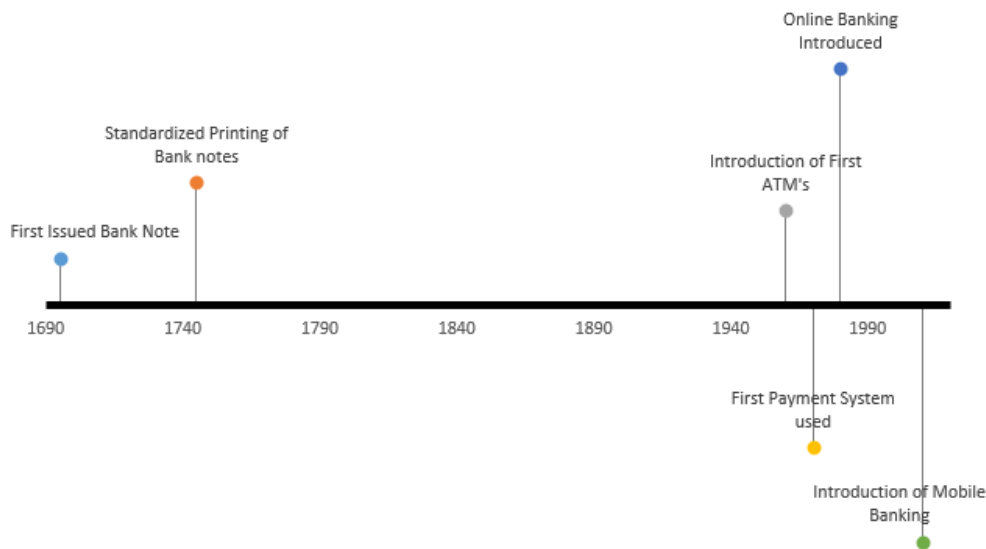


Figure 3.1: Timeline of Major Advances in Banking

As seen in Figure 3.1, banking has evolved over many years. As stated earlier, modern banking began as a simple banknote based system, driven by technology, banking adapted and became very dependent on cyberspace. Overtime, cyber-driven financial transactions are no longer a feature but rather a requirement. In modern times, allowing all users access to cyber-driven financial transactions. Through each major development in banking, users received more responsibility and financial freedom. As such, users need to be fully alert of how they use their cyber-driven financial services and they need to be educated on how to avoid associated threats. Therefore, if users are negligent or ignorant, it could result in a breach of cyber security, leading to financial loss. Thus, users have become a huge vulnerability and it is important that users are educated and made aware of the dangers surrounding their cyber-driven financial usage.

Furthermore, due to banks adapting overtime, offering more cyber-based services, users have taken up more responsibility when it comes to their financial well-being and safety. As such, users' need to be made aware of the role they play in cyber-driven financial transactions and educated appropriately. Cyber security, education, awareness, and training, can be considered a "human" appropriate control (ENISA, 2012), allowing users to make use of cyber-driven financial transactions in a safe and secure manner. Thus, as argued in this section, due to banking evolving over time, more responsibility has been passed onto users. As such, users themselves can be regarded as a vulnerability if negligent or ignorant when conducting cyber-driven financial transactions. The section to follow, will discuss cyber security education, awareness, and training required by users of cyber-driven financial transactions.

3.3 Current Education for Users of Cyber-driven Financial Transactions

As discussed in the previous section, banks have increasingly moved more responsibility on to users. As such, users need to ensure their own financial well-being and security when conducting cyber-driven financial transactions. Due to the nature of cyber-driven financial transactions, users often face more threats than typical users. Due to this fact, banks have attempted to assist users by offering some cyber security education, awareness, and training. The subsection to follow will discuss typical threats faced by banking users involved in cyber-driven financial transactions and related education provided by banks.

3.3.1 Human Error - Typical User Errors and Threats

Users are often described in literature as the weakest link in information security (Frauenstein & Von Solms, 2014). This also holds true for users involved in cyber-driven financial transactions. As stated previously, due to the financial nature of said users' cyberspace usage, they often face numerous threats. Moreover, due to

the vast array of cyber-driven financial services offered to users, it is often difficult for said users to maintain a sound level of appropriate cyber security. Therefore, users themselves become a vulnerability in the cyber-driven financial transaction process. Typical mishaps and threats users of cyber-driven financial transactions face can be broken into two main categories, namely: general cyberspace threats and banking specific threats. These two categories will be discussed in more detail.

General cyberspace threats can be regarded as threats the majority of social cyberspace users face. These threats, common among everyday cyberspace usage are:

- Identity theft: This can be regarded as the fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc (SABRIC, 2018e). Identity theft comes in many forms. The three main forms that affects users of cyber-driven financial transactions are:
 - Phishing: Can be seen as fraudsters pretending to be financial institutions or companies (SABRIC, 2018g). Fraudsters can send spam or pop-up messages to get users to reveal their personal information.
 - Vishing: Vishing is when a fraudster phones their victim imitating a bank official or service provider (SABRIC, 2018i). These fraudsters then use social engineering skills to manipulate their victims into disclosing confidential information.
 - Skimming: This is the process of fraudsters stealing credit/debit card numbers by using a special storage device attached to ATM machines (SABRIC, 2017a).
- Cyber crime: Cyber crime is a broad term used to describe criminal activities carried out by means of computers or the Internet (SABRIC, 2018c). Two major cyber crimes affecting users are:
 - E-mail hacking: Email hacking is the unauthorised access to, or manipulation of, an email account or email correspondence (SABRIC, 2018d).

Fraudsters use this unauthorised access to obtain account information and other sensitive information.

- E-mail spoofing: Can be regarded as the creation of email messages with a forged sender address (SABRIC, 2018d). This allows fraudsters to request information from banks on behalf of a user.

Due to the specific technology involved when conducting cyber-driven financial transactions users face certain threats that regular social cyberspace users are not confronted with. These threats can be regarded as banking specific threats. These banking specific threats can further be sub-divided into: non-internet banking threats, internet banking threats, and credit/debit card banking threats.

Non-internet banking threats can be seen as those threats users face when they are unknowingly connected to the internet. These threats are:

- ATM usage threats: These are threats users' face specifically when making use of ATMs.
 - ATM pin theft: The process of fraudsters attempting to steal users ATM pin's via electronic devices attached to ATM's (SABRIC, 2017a).
 - ATM etiquette: This is can be regarded as fraudsters take advantage of ignorant or negligent ATM users by tricking them into revealing their ATM pin or card details (SABRIC, 2017a).
- Cash and Cheque Usage threats: These are threats users face specifically when making use of cash or cheques.
 - Deposit and refund scams: In such cases, a fraudster orders goods or services from a business or a private seller and then makes a payment into the victims account, generally by means of a fraudulent cheque (SABRIC, 2017c). Proof of payment is then sent to the business or user and goods are delivered to the criminal. When the bank processes the cheque, it is uncovered that the cheque is fraudulent and as a result, no funds are transferred to the victims account.

- Carrying cash etiquette: Users need to ensure they are aware of the correct way to carry cash. Fraudsters can capitalise on ignorant or negligent users (SABRIC, 2018b).
- Cheque fraud: There are various fraud scams that are committed with cheques such as cheque interceptions, the substitution of genuinely issued cheques with fraudulent ones, and cheque washing (SABRIC, 2017b).
- Protection of cash: Some fraudsters wait until users have drawn cash to take advantage. Often fraudsters will loiter around ATM's, waiting for an opportunity (SABRIC, 2018b).

Internet banking threats can be referred to as those threats users face when they knowingly connect to the internet. These threats are:

- Pin/password theft: Fraudsters attempt to steal online banking log-in credentials via social engineering, phishing or other tactics (SABRIC, 2018f).
- Banking details fraud: An innocent user receives an e-mail or letter informing them that a particular supplier of theirs is changing their bank account details (SABRIC, Marcha). The correspondence will almost certainly include the details of the new account. The letter/email will ask said user to update their records. Thus, future payments are made into the fraudulent account.
- Secure connectivity: Fraudsters attempt to access users personal devices via a fraudulent connectivity (SABRIC, Marchb). This can be via fake wireless network.
- SIM swop fraud: SIM swapping is a sophisticated form of fraud and falls under social engineering. Fraudsters will distribute phishing emails, trying to ascertain as much personal information from victims as possible. The aim of which is to trick cellular service providers into giving fraudsters access to said users SIM card.

- Mobile Banking: These are threats present when users conduct banking via mobile devices such as smartphones or laptops (SABRIC, 2018h).
 - Device theft: Act of an individual stealing a users device. This can result in unauthorised use of device.
- Application banking threats: These threats are specific to users making use of banking via mobile applications.
 - Fraudulent applications: Fraudsters create fake banking applications. The aim of which is trick users into making use of it. Gathering banking detail information such as log-in details, passwords and pins.
 - Log-in details theft: Fraudsters attempt to steal log-in details via social engineering tactics (SABRIC, 2018f).
- URL banking threats: These are threats user face when conducting online banking via a banks online website.
 - 419 scam: A letter/fax/e-mail is sent to a selected recipient (but in actual fact is sent to many recipients) making an offer that would result in a large pay off for the recipient (victim) (SABRIC, 2018a). The aim of which is to gather the users banking details.
 - Authentic website usage: Fraudsters create fake banking websites. The aim of which is to fool users into logging in. Once users log-in, their information is captured thus giving fraudsters access to their accounts (SABRIC, 2018f).
 - Sign on/off procedure: Fraudsters take advantage of ignorant or negligent users who do not sign on/off correctly. It may be possible for fraudsters to steal banking details or initiate transactions.
 - Physical PC security: Similar to device theft, physical PC security involves the act of an individual stealing users device (SABRIC, 2018f). This can result in unauthorised use of device.

- PC security (malware): Software which is specifically designed to disrupt, damage, or gain unauthorised access to a computer system. Fraudsters use malware to steal passwords, pins and other sensitive information (SABRIC, 2018f).

Credit/debit card banking threats are those threats specific to card usage whether internet or non-internet based. These threats are:

- Online Purchases (3rd Party) threats: These are threats users face when making use of 3rd party websites for online purchases.
 - Authentic website usage: Fraudsters create fake online shopping websites. The aim of which is to fool users into logging in (SABRIC, 2018f). Once users log-in, their information is captured thus giving fraudsters access to their accounts.
 - Card information theft: Fraudsters attempt to steal card information via phishing or social engineering. Details of information can be card numbers, CVV numbers, and personal information found on banking cards.
- Physical card threats: Threats users face when making use of physical debit/credit cards.
 - PIN theft: The process of fraudsters attempting to steal users debit/credit pins via point of sales or electronic devices attached to ATM's.
 - Lost card fraud: Lost card fraud refers to fraud that results from a fraudulent transaction that is performed on a validly issued card that was stolen from a legitimate user (SABRIC, 2018j).
 - Counterfeit card fraud: Counterfeit card fraud is perpetrated with a card that has been illegally manufactured using information stolen from the magnetic strip of a genuinely issued card (SABRIC, 2018j).
 - Account take over fraud: Account takeover fraud takes place when an existing account is taken over by fraudsters posing as the genuine

account holder, who then uses the account for their own benefit whilst pretending to be the genuine account holder (SABRIC, 2018j).

- Not received issued card fraud: Not Received Issued Card Fraud, relates to the interception of genuinely issued cards before they reach the authentic users (SABRIC, 2018j). Fraudsters then use intercepted cards fraudulently.
- Stolen card fraud: Similar to lost card fraud, stolen card fraud refers to fraud that results from a fraudulent transaction that is performed on a validly issued card that was stolen from a legitimate user (SABRIC, 2018j).

Due to the numerous threats users of cyber-driven financial transactions face, banks have created cyber security education, awareness, and training for said users. The subsection to follow will discuss educational material offered by banks.

3.3.2 Current Educational Material Offered to Users of Cyber-driven Financial Transactions

As seen in the preceding subsection, users of cyber-driven financial transactions face numerous threats. They do not only face the same threats as social cyberspace users, they also face banking specific threats. As such, in order to aid users of cyber-driven financial transactions banks have released cyber security education, awareness, and training for said users. As this research is based in the context of South Africa, this section will discuss educational material provided by South Africa's five major banks. These banks are; Standard Bank, First National Bank (FNB), Amalgamated Banks of South Africa (ABSA), Nedbank, and Capitec Bank. Table 3.1 represents all relevant topics to users of cyber-driven financial transactions and which banks offers educational material on said topic.

Table 3.1: Educational Topics

Educational Topics	Major South African Banks				
	Standard Bank	FNB	ABSA	NedBank	Capitec Bank
General Cyberspace Threats					
Phishing	✓	✓	✓	✓	✓
Vishing	✓	✓	✓	✓	
Skimming	✓	✓	✓		
E-mail Hacking					
E-mail Spoofing					
Non-Internet Banking Threats					
ATM Pin Theft		✓	✓	✓	✓
ATM Secure Etiquette		✓	✓	✓	✓
Deposit and Refund Scams	✓			✓	
Carrying Cash Etiquette				✓	
Cheque Fraud		✓	✓	✓	
Protection of Cash					
Internet Banking Threats					
Pin/Password Theft					
Banking Details Fraud					
Secure Connectivity					
Sim Swap Fraud	✓			✓	
Device Theft					
Fraudulent Applications					
Log-in Details Theft					
419 Scam	✓	✓	✓	✓	
Authentic Website Usage					

Table 3.1: Educational Topics

Educational Topics	Major South African Banks				
	Standard Bank	FNB	ABSA	NedBank	Capitec Bank
Sign On/Off Procedure					
Physical PC Security					
PC Security (malware)					
Credit/Debit Banking Card Threats					
Authentic Website Usage					
Card Information Theft					
Lost Card Fraud		✓			
Counterfeit Card Fraud					
Account Take Over Fraud					
Not Received Issued Card Fraud					
Stolen Card Fraud					

As seen in Table 3.1, each major bank made an effort to provide some educational material on certain topics. However, not all topics are covered in depth nor are topics covered consistently. Therefore, it can be claimed that banks do provide some educational material but the material provided does not cover all topics. Furthermore, banks are not consistent when it comes to topics covered, as not all banks offer the same educational material. The subsection to follow, will discuss how banks go about providing the previously mentioned educational material.

3.3.3 A Critical Assessment of Educational Approaches offered

In the preceding subsection, it was stated that banks do provide some educational material to users of cyber-driven financial transactions. Therefore, banks do make

some effort to aid users in making use of cyber-driven financial transactions safely and securely. This subsection, will assess the educational approaches offered by each major South African bank.

Standard Bank: Standard Bank offers users educational material directly from their main website. Once users access the main Standard Bank website, they can access the "*security centre*". The "*security centre*" contains all educational material provided by Standard Bank. Topics are those found in Table 3.1. Topics are presented in a text format only. Users are required to read through the material themselves. Moreover, there is no mechanism in place to verify if they understand said material.

FNB: Similar to Standard Bank, FNB offers educational material directly from their main website. Once users access their main website, they navigate to the "*security centre*". FNB's "*security centre*", similar to Standard Bank provides text based educational material. Unlike Standard Bank, FNB uses images in their explanations of topics. They also provide a glossary of terms used. As such, users unfamiliar with certain terms can get clarity on said terms. Educational material offered by FNB, can be seen in Table 3.1.

ABSA: Unlike Standard Bank and FNB, ABSA users need to visit the quick links section of the ABSA main website. Once users navigate to the quick links section, they can access the "*security centre*" from there. Similar to Standard Bank, educational material is presented in text-based format . As with the previous banks, topics covered were those in Table 3.1. However, some extra tips are provided to users of cyber-driven financial transactions. These tips include travel and business related information.

Nedbank: Similar to previously mentioned banks, Nedbank makes use of a "*security centre*". However, users need to specifically know they need to visit it, as users need to select it under the navigation section. Therefore, if a user is unaware of how to navigate the website correctly, he/she may struggle to find the educational material. As with the previous banks, Nedbank offers educational material in a text-based format. Topics covered by Nedbank are those seen in Table 3.1.

Capitec Bank: Educational material provided by Capitec Bank can be seen in Table 3.1. Unlike the previous banks, Capitec Bank makes use of a " *Privacy and security*" section. In order for users to access the section, they need to navigate via the help centre. Therefore, unless users know how to access the material they may not be able to find it. Similar to the previous banks, Capitec Bank presents their educational material in a text-based format.

It is thus clear that all five major South African banks provide some educational material. Moreover, all banks follow a similar approach when offering this material, with users accessing the material directly from the website of the bank concerned. Depending on the bank, users either can find the " *security centre*" or equivalent on the main home page otherwise they need to actively search for it. All banks provide their educational material in a text-based format with only some banks using helpful images. Furthermore, none of the banks provide any mechanism for users to test whether or not they have understood the material.

Thus, while it may be concluded from this discussion that banks have made efforts to provide users of cyber-driven financial transactions with educational material, this material is presented in an unattractive or unstimulating way across all banks. Thus, it can thus be argued that this gives rise to the possibility of taking an alternative educational approach, especially in view of the fact that none of the banks have conducted any assessment of the educational material.

3.4 Conclusion

Users of cyber-driven financial transactions are a particularly vulnerable group of users. Due to the financial nature of their cyber usage, they often face more threats than other social cyberspace users. As such, users of cyber-driven financial transactions need an appropriate level of awareness and associated education to make use of their cyber services in a safe and secure manner. As highlighted in this chapter, users of cyber-driven financial transactions need to take a bigger responsibility than ever for their own safety and security. As such, banks provide some educational material in order to aid said users. However, this material

only covers some threats users face. Moreover, the material is not always easily accessible or appealing to users. Therefore, the aim of this chapter to highlight the lack of appealing cyber security education, awareness, and training for users of cyber-driven financial transactions has been met.

As shown in Table 3.1, each bank offers education on various topics, relative to cyber-driven financial transactions. Table 3.1 also shows that there is no standard set of educational topics nor is there a standard method of accessing such educational content.

Even though the educational content is technically correct, the content is challenging to find, users are not required to review the material nor is the presentation necessarily conducive to learning. Therefore, it can be argued that there is a fundamental shortcoming with the approach being taken by banks to educate their users on how to conduct cyber-driven financial transactions in a safe and secure manner.

The proceeding chapter, will discuss the research approach taken in order to create such an alternative educational approach that will enhance current education offered.

Chapter 4

Research Approach

Cyberspace users require an acceptable level of knowledge and awareness in order to make use of cyberspace in a secure manner. This is particularly true for the users of cyber-driven financial transactions. This chapter describes the research approach taken to prove that a social networking approach can be used to make users of cyber-driven financial transactions less vulnerable to related security risks.

4.1 Introduction

From the previous chapter, it was indicated that users of cyber-driven financial transactions are a highly vulnerable group of users and consequently are partly responsible for their own cyber safety. As such, financial institutions have provided these users with some cyber security education, awareness, and training, mostly on their respective website. However, as argued in the previous chapter, this cyber security education, awareness, and training are lacking in both appeal and suitability. Consequently, this research study attempts to provide evidence towards proving a theory that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions, allowing them to conduct said transactions in a more safe and secure manner.

The aim of this chapter is to define the research approach taken to provide evidence towards proving that social networking can be an effective educational

approach to educate users of cyber-driven financial transactions. This chapter will begin by describing the research design followed in order to create said social networking educational approach. Secondly, the design of the research instrument used will be discussed, followed by the criteria influencing the social networking aspect. It will conclude with arguments on how cyber security educational topics were selected.

4.2 Research Design

As previously discussed, all the major financial institutions in South Africa offer cyber security education, awareness, and training to the users of cyber-driven financial transactions. However, these offerings follow a very similar format and generally include text-rich material that requires time and effort on the users part to educate themselves. Furthermore, the material is not always conducive to learning or presented in an attractive manner. Hence, it can be argued that there is a place for more user-friendly and appealing cyber security education, awareness-raising and training to be provided to the users of cyber-driven financial transactions. The aim of this research study is to conduct an experiment to provide evidence towards proving that a social networking approach to cyber security education, awareness, and training can be effective. This could ultimately qualify users of cyber-driven financial transactions to conduct said transactions in a more safe and secure manner.

According to Olivier (2009), experimentation is utilised in order to achieve one of three goals; firstly, to see if one can find anything interesting, secondly, to "test" a theory and lastly to prove a theory. The first goal, to see if one can find anything interesting, can be regarded as an exploratory experiment. Exploratory experiments typically have very little structure (Olivier, 2009). An example of this would be seeing how far you can drive with a single tank of petrol. This experiment is very unstructured and one is simply doing it to observe the distance. The second goal, to "test" a theory is performed in order to "feel" if the theory is correct or more commonly to refine the proposed theory (Olivier, 2009). Again,

the example of driving on a single tank of petrol can be used. However, in this instance, the researcher believes they might be able to drive 250 kilometres on a single tank. The experiment is done in order to test if the theory holds true or not. The last goal, conducting an experiment to prove a theory is performed in order to remove any doubts (Olivier, 2009). Once again, the example of driving on a single tank of petrol can be used. In this case, the research has the official mileage of the vehicle and conducts the experiment in order to verify its accuracy. As such, this research study can be considered experimental in nature seeing as the aim of the research is to provide evidence, proving that a social networking approach to cyber security education, awareness, and training can be effective. Thus, according to Olivier (2009) the third goal, to prove a theory, is the most relevant for this research study. Thus, the research approach followed was that of an experiment, specifically to prove a theory that a social networking approach to cyber security education, awareness, and training can be used to make users of cyber-driven financial transactions less vulnerable to related security risks.

Similar to an experiment, there are various ways to categorise theories. Theory building research can be classified under two major classifications namely: empirical and analytical research (Wacker, 1998).). When building a theory using empirical research, inductive methods are applied to arrive to the theory at hand, while when building a theory using analytical research, deductive methods are used. In the context of this research study, the aforementioned theory, that of a social networking approach to cybersecurity education, awareness and training to make users of cyber-driven financial transactions less vulnerable to related security risks, may be classified as building a theory using analytical research. Moreover, analytical research can be subdivided into three categories: analytical conceptual, analytical mathematical and analytical statistical research (Wacker, 1998). Furthermore, this research study will be using argumentation theory. Argumentation theory, is the process of drawing conclusions from logical reasoning in order to prove a theory (Van Eemeren & Grootendorst, 2003). The Handbook of Argumentation Theory contains numerous examples of where sound argumentation has been applied in order to prove a theory (Haaften, 2016). According to Haaften

(2016), argumentation can be considered a sound approach in order to prove a theory developed using analytical research. Therefore, in this research study in order to prove the aforementioned theory of analytical conceptual nature, argumentation has been used alongside data captured from the research instrument.

Owing to the experimental nature of this research two groups of cyber security experts were utilised. The aim of selecting these groups of cyber security experts was to lead the experiment by making use of their expertise in order to create an alternative educational approach. The first group of cyber security experts comprised academic professionals from the Nelson Mandela University while the second consisted of industry professionals from the South African Banking Risk Information Centre (SABRIC). SABRIC is a non-profit company formed by the four major South African Banks to assist banking organisations and cash-in-transit companies in combating organised bank-related crimes, including cyber crime. The section that follows will discuss the design of the research instrument used in this research.

4.3 Research Instrument Design

As mentioned previously, the research approach followed is that of an experiment utilising two groups of cyber security experts to lead the experiment. The decision for this approach was motivated due to the high level of expertise afforded by these groups of cyber security experts. These groups of cyber security experts also allowed for the practical utilisation of the research instrument at a national level. The experiment made use of a research instrument within the social media domain, to gather data. The research instrument in this context is the cyber security education tool utilising a social media quiz and video combination. These were created in order to raise awareness and to educate users of cyber-driven financial transactions.

The research instrument was targeted at the majority of South African banking clients of which the majority make use of cyber-driven financial services. Therefore, considerations in the design of the research instrument include the following:

audience-appropriate content, the delivery mechanism, ease of use and understanding. Due to the research instrument target audience being the majority of South African banking users, content needed to cater for varying knowledge and education levels. As such, content was kept to the most prevalent cyber security topics. Furthermore, the delivery mechanism had to be easily accessible by many, as such, social networking being of such popularity was deemed appropriate. While existing educational instruments used by South African banks were considered as a basis for the research instrument, the current state of awareness and education, as the previous chapter showed, is lacking and unappealing. During an initial discussion with cyber security experts from SABRIC, a two-fold approach was decided upon, which comprised of a combination of an awareness raising game-type quiz Facebook and an accompanying educational video on YouTube. Users would firstly take part in the quiz, raising awareness and subsequently be prompted to watch the accompanying video, educating themselves. This approach served as the basis for the research instrument for two major reasons. Firstly, social networking, particularly Facebook and YouTube, are growing rapidly in South Africa and both allow for a far wider audience to be reached. Secondly, an approach where a social networking game and video are utilised, would lower the preconceived notions of typical education, which can be seen as dull and unappealing. This would make the research instrument more appealing to the majority of South African users.

The subsections to follow will discuss the criteria considered in order to decide upon the approach taken, the selection process for educational topics.

4.3.1 Criteria Influencing a Social Networking Approach

Cyber security is a topic often addressed in today's modern age of internet connected devices. This is particularly true in the South African banking industry, where cyber usage and cyber security are often matters of great concern. As expressed in literature, software and hardware security mechanisms are often used to strengthen information systems (IS) against attacks. However, these systems are still vulnerable as a result of user negligence or ignorance (Öütçü, Testik, & Chouseinoglou, 2016). Unfortunately, the majority of cyber security efforts in

South African banking can be regarded as technical in nature, consequently users of cyber-driven financial transactions are required to seek out their own cyber security education, awareness, and training. This research was conducted at a national level, using social networking platforms as an educational tool. A "fun" social networking quiz (to raise awareness and gain interest) and a related informative video (to educate) were therefore created. This two-fold approach, using social networking, form the basis of the research instrument.

This subsection will address the criteria that influenced the design of the research instrument, with the final result being a social networking game quiz and video combination, which resulted in a suitable research instrument to raise awareness and educate users of cyber-driven financial services.

Three primary criteria influenced the design of the final research instrument. The South African Risk Information Centre (SABRIC) expertise was consulted in each criteria, determining the final research instrument. These criteria included, firstly, catering to a wide audience; secondly, ensuring that education, awareness, and training can be deemed appealing and; lastly, offering an alternative to text-based education.

Firstly, due to the target audience being the majority of South African cyber-driven financial transactions users, the research instrument had to cater to a wide audience. Furthermore, the group of cyber security experts from SABRIC allowed the research instrument to be used at a national level. Disseminating the research instrument on a national level was made possible through the use of social networking, in particular Facebook and YouTube, as the platforms on which users could interact with the research instrument. At the time of conducting this research, Facebook has two billion active users each month, with a large portion being South African (Constine, 2017). Hence, the utilisation of popular social media platforms would allow the research instrument to be reached by the majority of cyber-driven financial transaction users.

Secondly, as highlighted in the previous chapter, current cyber security education, awareness, and training provided by financial intuitions can be deemed as unappealing or difficult to understand. Therefore, the research instrument had to

be designed to allow users to be made aware in an alternative method. The concept of a "fun" and interactive game-type quiz was introduced. This allowed for users awareness levels to be raised in an alternative manner compared to existing means, while lowering the preconceived notions of traditional learning. This was ultimately achieved by a high score quiz, accessed by Facebook. The quiz served to raise awareness and gain interest amongst users. Using the quiz type approach, allowed for the research instrument to be interactive and have a certain "fun" factor.

Lastly, the research instrument needed to engage users, allowing them to be educated in an alternative manner. This was done by introducing short videos. These videos allowed users to educate themselves with very little effort from themselves. The videos produced were short, which allowed for users to keep focus throughout the video. Videos that were produced followed a similar theme and were consistent in design.

Thus, as this discussion indicates, the research instrument design was carefully considered using input from the group of cyber security experts and addressing each of the three primary criteria. SABRIC cyber security experts were involved throughout the entire design process, guiding the design and allowing for the final research instrument to be created in a professional manner. Thus, based on the criteria and the input from the cyber security experts, a two-fold approach, using a "fun" Facebook quizzes and a YouTube educational videos was decided upon.

In order for users' to benefit, the content of the quiz and video had to ensure that focused and relevant learning takes place. The content found in both the video and quiz is of particular importance. The following subsection will discuss the process taken in order to identify relevant topics to be incorporated in the cyber security quizzes and educated on in the educational videos.

4.3.2 The Process to Identify Relevant Cyber Security Educational Topics

As mentioned previously in order for users to benefit from cyber security education, awareness, and training the material has to be presented in an appealing manner.

Moreover, the content needs to be audience appropriate and relevant to the problem space. As such, this subsection will discuss the process followed to identify relevant cyber security educational topics to create the research instrument.

The process to identify relevant cyber security educational topics followed four phases. Input from two groups of cyber security experts were core during these four phases. These groups comprised of cyber security experts from academia (Nelson Mandela University) and cyber security experts from industry (SABRIC). The aim of was to identify the most prominent educational topics that users of cyber-driven financial transactions required to be made aware of and educated on. These phases will be discussed individually.

- Phase One:

The initial phase in identify relevant cyber security educational topics was conducted using literature. Firstly, all of the major South African banks (Standard Bank, FNB, ABSA, NedBank, Capitec Bank) have websites that provide some awareness and educational material. A critical assessment of the cyber security educational material on their websites was conducted, assessing the aforementioned banks educational offerings. This was done in order to identify what they deem relevant cyber security educational topics that users should be educated on. These cyber security educational topics can be found in Table 3.1. This allowed for the creation of a version 1 topic map. A topic map is a representation of knowledge (ISO/IEC, 2015). A topic map was selected as the method of knowledge representation for this research study due to the being an ISO/IEC 13250 standard describing the topic map creation process.

Cyber security educational topics that formed the basis of the initial topic map are those found in Table 3.1. Figure 4.1 below represents the initial version of the topic map, based on information gathered and presented in Table 3.1.

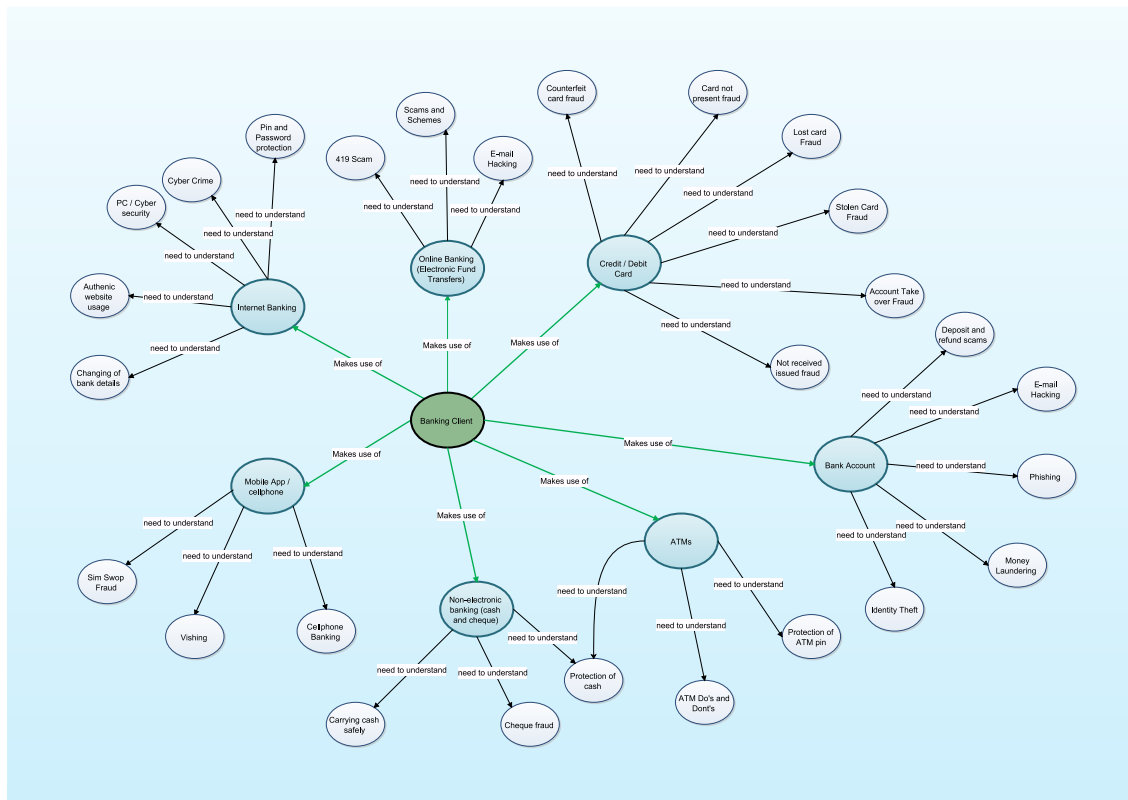


Figure 4.1: Topic Map Version 1

As seen in Figure 4.1, the initial topic map was certainly not complete, but it did serve as the basis for future revisions.

- Phase Two:

The second phase of the process to identify relevant cyber security educational topics was conducted internally at the Nelson Mandela University. A group of academic cyber security experts provided input on the initial topic. The group of cyber security experts comprised of three well-established professors and a junior researcher. The aim of the second phase was to refine the topic map further. During a group discussion with the academic cyber security experts, various new cyber security educational topics were added. Some educational topics were combined while some were removed from the

initial version of the topic map. A significant change was made to the topic map by shifting the core of the topic map from the financial user to the financial users’ bank account.

Further feedback from the group of cyber security experts included, the layout of certain areas of the topic map, and connections between cyber security educational topics. Figure 4.2 below represents the revised version of the topic map, after all feedback from the academic cyber security experts were incorporated.

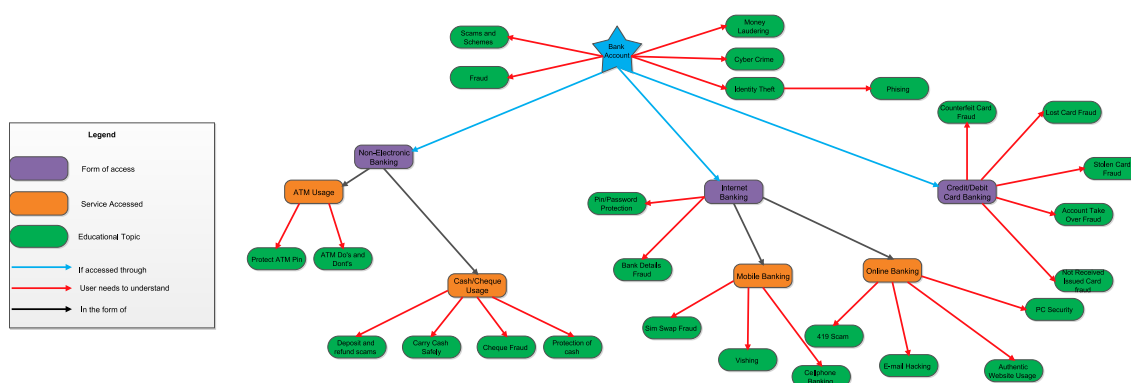


Figure 4.2: Topic Map Version 2

As seen in Figure 4.2, the revised topic map has evolved to centre around the users’ bank accounts rather than the users themselves. This allowed further relevant educational topics to be added linking them to banking services utilised.

- Phase Three:

The third phase of the process to identify relevant cyber security educational topics was conducted with cyber security experts from SABRIC. The group of cyber security experts comprised of two experts in consumer awareness creation, an expert in online banking, a technical cyber security expert and finally a communications expert. The group of experts are all involved in the banking industry with a focus on cyber security in some form. The subse-

quent, discussion resulted in previously overlooked cyber security educational topics to be added. Having incorporated the feedback from the SABRIC cyber security experts, the revised topic map now represents the majority of cyber security educational topics relevant to users of cyber-driven financial transactions. Figure 4.3 represents the final version (version 3) of the topic map.

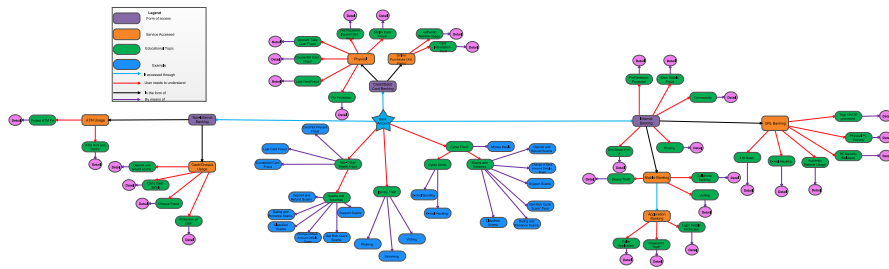


Figure 4.3: Topic Map Version 3

After this phase, the topic map of cyber security educational topics, that users of cyber-driven financial transactions need to be aware of and educated on has been finalised. Thus, all relevant cyber security educational topics have been identified and put in relation to one another. To view the various topic maps in a larger format, please refer to Appendix A.3.

- Phase Four:

The final phase of the process, as with phase three, was conducted with cyber security experts from SABRIC. The group of cyber security experts comprised of a communications expert and an information expert. This final phase distilled the final version of the topic map into the most prevalent educational topic areas to users of cyber-driven financial transactions. Five main educational topic areas were identified to be most relevant. These five topic areas can be considered to be the areas where users are the most negatively impacted by cyber crime. Whether that be due to ignorance or negligence, users' are most prone to experiencing cyber crime when attempting to make

use of these topic areas or associated devices. These five educational topic areas are:

1. Online Shopping
2. Card Fraud
3. Mobile Banking
4. Cyber Hygiene
5. Malware

These five educational topic areas played a major role in the main research instrument.

As discussed in this subsection, the identification of relevant cyber security educational topics involved an iterative process utilising input from cyber security experts from both academia and industry (SABRIC). This resulted in the creation of a topic map. During each phase of the topic identification process the topic map became more detailed, showing the majority of educational topics that users of cyber-driven financial transactions need to be educated on. The final phase culminated in the five most important educational topic areas being selected. Accordingly, the process to identify relevant cybersecurity educational topics comprised four phases: the initial phase resulted in the creation of a basic topic map, the following two phases incorporated feedback from cyber security experts resulting the refinement of the map into one that represented the majority of topics the users of cyber-driven financial transactions need to be educated on. The final phase again incorporated feedback from cyber security experts, which assisted in grouping the identified topics into cyber security topic areas. Each of the five educational topic areas will be discussed in detail in the chapter to follow.

4.4 Conclusion

In this chapter, it was highlighted that the research approach followed of this research study is that of an experiment. The aim of this research is to provide

evidence towards proving that social networking can be an effective educational approach to educate users of cyber-driven financial transactions. This was conducted by means of an experiment as per Olivier (2009), who states that an experiment can have the goal of proving a theory. The addition of the group of cyber security experts allowed the experiment access to resources and expertise outside traditional academic avenues. The objective of this chapter was to define the research approach taken in order to prove that social networking can be an effective educational approach to educate users of cyber-driven financial transactions. This was first done by discussing the research approach, which is that of an experiment. Moreover, the design of the research instrument was also discussed. The research instrument in the context of this research is the cyber security education tool utilising a social media quiz and video combination. The criteria influencing the social networking approach were also discussed, followed by the process to identify relevant cyber security educational topics. Thus, the aim of this chapter is completed.

The following chapter discusses the research instrument in more detail and the methods used to gather the requisite data.

Chapter 5

Social Networking Instrument

Users of cyber-driven financial transactions are a particularly vulnerable group. Appropriate cyber security education, awareness, and training can be seen as lacking or unappealing. This chapter serves to provide detail on the social networking instrument and data gathering aspect used in this research study

5.1 Introduction

From the preceding chapter, it was understood that the research approach followed in this research study is that of an experiment. The aim of the study being to provide evidence, towards proving that an educational approach, utilising social networking, can educate users of cyber-driven financial transactions. In turn, allowing them to conduct said transactions in a more safe and secure manner. The experiment made use of a research instrument within the social media domain to gather data. The research instrument in this context is the cyber security education tool utilising a social media quiz and video combination. This was created in order to raise awareness and to educate users of cyber-driven financial transactions. Incorporated into the research instrument is the data gathering aspect or data gathering mechanism, of which the results will be discussed in the following chapter. Thus, the aim of this chapter is to discuss the social networking instrument in detail and the data gathering aspect used.

This chapter begins by describing the research instrument in detail. Firstly, discussing the awareness-raising quizzes, followed by the accompanying educational videos. To conclude the data gathering aspect or data gathering mechanism will be discussed.

5.2 Research Instrument Details

As previously stated, the research instrument is targeted at the majority of South African banking clients, the majority of which make use of cyber-driven financial transactions. Therefore, as previously discussed, considerations in the design of the instrument include: audience-appropriate content, the delivery mechanism, ease of use and understanding.

Due to the aforementioned considerations, using a social networking cyber security education, awareness and training was determined to be as the most appropriate approach. Users are free to access the quizzes or videos via Facebook or YouTube respectively. Moreover, this training is offered free and the quizzes and videos may be accessed via compatible device. However, users that follow the quizzes or videos are prompted to attempt their corresponding counterpart. Regardless, a two-fold approach is followed, comprising of completing the awareness raising game-type quiz followed by the educational video or alternatively by viewing of the educational video and then attempting the awareness raising game-type quiz. The subsection to follow will discuss the cyber security quizzes.

5.2.1 Cyber Security Quizzes

As discussed in the previous chapter, five main topic areas were identified to be most relevant in both how users are negatively affected and how lacking cyber security education, awareness, and training are. These topic areas are: online shopping, mobile banking, card fraud, malware and computer hygiene. As such, five cyber security quizzes with five relating educational videos have been created. All cyber security quizzes comprise of six, close-ended questions and are linked to an educational video. After a user selects an answer, regardless if it is a correct

or incorrect answer, an educational message is displayed. Each question is a close-ended, multiple-choice questions. The user, in the majority of questions, has a choice of four answers with only one being correct. Once the user answers a question, he/she is prompted with a short text message adding an element of educational reinforcement to the quiz. All of the questions and answers, as well as the educational messages that follow each question, were approved by the group of SABRIC cyber security experts.

Each cyber security quiz will briefly be discussed.

Quiz 1: Online Shopping Cyber Security Quiz

Questions found in the online shopping cyber security quiz focus on making use of secure websites, identify theft, passwords and unsafe online shopping behaviour. The aim of the online shopping quiz is to raise user awareness around the dangers of online shopping specifically, via web browsers. Table 5.1 below represents a sample question from the online shopping quiz.

Table 5.1: Online Shopping Sample Question

Which of the following contributes to unsafe online shopping?	
Answer A:	Saving of payment information in web browsers
Answer B:	Using a well-known online merchant
Answer C:	Making use of 3-D secure payment
Answer D:	Looking for closed padlock symbol

As seen in Table 5.1, the user is required to distinguish between what is safe and unsafe online shopping behaviour. In that specific question, the correct answer is Answer A. If the user answers correctly, the following message is displayed: *Right answer! Never save payment information in your web browser as it may be used if someone gets a hold of your device or can be obtained via malicious software..* However, if the user answers incorrectly, the following message is displayed: *Wrong answer! Some sites (as well as all browsers) offer to remember your payment information (e.g. password) for your convenience upon subsequent*

purchases. Never accept to have your "financial information" stored on any website/web browser.

Refer to Appendix B.1 to view the full set of online shopping questions. To access the online shopping cyber security quiz, please follow the *link* <https://qz.app.do/online-shopping>.

Quiz 2: Mobile Banking Cyber Security Quiz

Questions in the mobile banking cyber security focuses on securing the users mobile device, how often to update mobile applications and how to protect information stored on mobile devices. The aim of the mobile banking quiz is to raise user awareness around the dangers of mobile banking. Table 5.2 is a sample question from the mobile banking cyber security quiz.

Table 5.2: Mobile Banking Sample Question

What do financial institutions provide free of charge to assist in keeping your mobile device secure?	
Answer A:	VPN
Answer B:	Anti-virus application
Answer C:	Airtime
Answer D:	Music

As seen in Table 5.2, the user is asked to identify what security mechanism financial institutes provide free of charge. The correct answer, Answer B has been highlighted. If the user answers correctly the following message is displayed: *Right answer! Install an up-to-date anti-virus application on your mobile device. Most financial institutions provide this to their customers free of charge.* However, if the user answers incorrectly the following message is displayed: *Wrong answer! Install an up-to-date anti-virus application on your mobile device. Most financial institutions provide this to their customers free of charge.*

Refer to Appendix B.1 to view the full set of mobile banking questions. To access the mobile banking cyber security quiz, follow the *link* <https://qz.app.do/mobile-banking>.

Quiz 3: Card Fraud Cyber Security Quiz

Questions in the card fraud cyber security quiz centre around card usage at ATMs and point of sales, for example, how can a user identify that he/she may be a victim of card fraud at an ATM. The aim of the card fraud quiz is to raise user awareness around the dangers of card usage. Table 5.3 is a sample question from the card fraud cyber security quiz.

Table 5.3: Card Fraud Sample Question

Which of the following indicates that you may be a target of card fraud?	
Answer A:	The area around the ATM you are using is quiet
Answer B:	A stranger offers to assist you at the ATM
Answer C:	The ATM is out of order
Answer D:	There is a security guard on duty at the ATM

As seen in Table 5.3, the user needs to identify in which scenario he/she might be a target of card fraud. In this specific question, the correct answer is Answer B. If the user answers correctly the following message is displayed: *Right answer! Be cautious of strangers offering to help at the ATM as they could be trying to distract you in order to get hold of your card or your PIN.* However, if the user answers incorrectly the following message is displayed: *Wrong answer! Be cautious of strangers offering to help at the ATM as they could be trying to distract you in order to get hold of your card or your PIN. Also, ensure that you feel safe. If something bothers you, rather use another ATM*

Refer to Appendix B.1 to view the full set of card fraud questions. To access the card fraud cyber security quiz, follow the *link* <https://qz.app.do/card-fraud>.

Quiz 4: Malware Cyber Security Quiz

The malware cyber security quiz includes topics such as; the correct action to take when inserting a flash drive in a computer and what actions to take if you

receive a suspicious e-mail. The aim of the malware quiz is to raise user awareness around the dangers of malware on electronic devices and to prevent said devices from becoming infected. Table 5.4 is a sample question from the malware cyber security quiz.

Table 5.4: Malware Sample Question

If you receive an email from unknown or suspicious origins, what action should be taken?	
Answer A:	Respond to the email appropriately
Answer B:	Ignore the email, but check the attachment for further details
Answer C:	Delete the email
Answer D:	Download the attachment to your computer

Table 5.4 poses the question regarding what should a user do if he/she receives a suspicious e-mail or an e-mail from unknown origins. The correct answer, Answer C has been highlighted. If the user answers correctly the following message is displayed: *Right answer! Never open emails from unknown or suspicious origins. Cyber-criminals use attachments which could be disguised as, for example, tax refunds, package deliveries and invoices to install malware on your device.* However, if the user answers incorrectly the following message is displayed: *Wrong answer! Never open emails from unknown or suspicious origins. Cyber-criminals use attachments which could be disguised as, for example, tax refunds, package deliveries and invoices to install malware on your device. It would be best to delete the email as it will prevent you from opening it accidentally.*

Refer to Appendix B.1 to view the full set of malware quiz questions. To access the malware cyber security quiz, follow the *link* <https://qz.app.do/malware>.

Quiz 5: Computer Hygiene Cyber Security Quiz

The computer hygiene quiz as with the previous quizzes, is a set of 6 questions. The aim of the computer hygiene quiz is to raise user awareness around good

computer hygiene which is about being proactive and preventing any incidents from occurring in the first place. Table 5.5, represents a sample question from the computer hygiene cyber security quiz.

Table 5.5: Computer Hygiene Sample Question

The main aim of good computer hygiene is to?	
Answer A:	Think reactively about security
Answer B:	Protect our physical security
Answer C:	Ensure safe and secure Facebook usage
Answer D:	Train ourselves to think proactively about our cyber security

As seen in Table 5.5, the user is prompted to define what the main aim of computer hygiene is. Answer D, has been highlighted, as it is the correct answer. If the user answers correctly the following message is displayed: *Right answer! Good computer hygiene is about being proactive and preventing any incidents from occurring in the first place.* However, if the user answers incorrectly the following message is displayed: *Wrong answer! The main aim of good computer hygiene is to be proactive and prevent any incidents from occurring in the first place. Possible good computer hygiene tips include; having an up-to-date anti-virus application installed.*

Refer to Appendix B.1 to view the full set of computer hygiene quiz questions. To access the computer hygiene cyber security quiz, please follow the *link* <https://qz.app.do/computer-hygiene>.

This section discussed the five cyber security quizzes, one quiz per topic area. Each quiz comprised of six questions. Each question is a close-ended, multiple-choice questions. The user in majority of questions has a choice of four answers with only one being correct. Once the user answers a question he/she is prompted with a short text message adding an element of educational reinforcement to the quiz. The subsection to follow will discuss the details of the accompanying educational videos.

5.2.2 Educational Video Details

As discussed previously, five main topic areas were identified and formulated with group of SABRIC cyber security experts to be most relevant in both how users are negatively affected and how lacking cyber security education, awareness, and training are. As such, five corresponding educational videos have been created. Each educational video relates to the respective cyber security quiz and is approximately 1 minute long. As mentioned previously, the videos were kept short in order to keep the users' attention, allowing them to concentrate throughout the duration of the video.

The scripts utilised in the educational videos were developed in collaboration with the group of cyber security experts from SABRIC. The aim of each video is to aid users in making use of the specific cyber service in a more secure and safe manner. The educational videos were created by a professional video creation company, allowing them to be of a high quality. All videos have a similar aesthetic; an animated production, with a look and feel that appeals to users from various backgrounds. The subsection to follow will briefly discuss the educational videos in more detail.

Video 1: Online Shopping

The main message behind the online shopping educational video is to educate users to allow them to perform online shopping in a more safe and secure manner. The video comprises of five pointers for safe and secure online shopping. The script for the online shopping video is as follows:

Cyber-crime is a reality. Ensure your anti-virus software is installed, activated and updated regularly. Cybersecurity habits can reduce your risk of becoming a victim.

Check out these top five pointers for safe and secure online shopping.

1. Look out for the padlock followed by HTTPS next to the URL when transacting online the S shows that you are connected to a secure and encrypted website.
2. When registering on a secure site, choose a strong password and do not save your log-in details on any computer or mobile device. Never re-use the same password on multiple domains.
3. Avoid sharing your personal information, online merchants dont need your ID number or date of birth to process your order, but cyber criminals can use this to steal your identity.
4. Check your bank balance after making any online shopping payments. Report any fraudulent transactions to your bank.
5. For added online shopping verification, register your bank card with 3D secure.

Be smart, be secure. A message brought to you by SABRIC and the Nelson Mandela University.

The aim of the video is to educate users on simple, yet effective security techniques to conduct online shopping in a safe and secure manner. Due to targeting a wide demographic, the video is simple and addresses basic cyber security issues surrounding online shopping.

To view the actual video, follow the *link* <https://www.youtube.com/watch?v=W18VHuzbD8E>.

Video 2: Mobile Banking

The main message behind the mobile banking video is to educate users ensuring they can conduct mobile banking in a more safe and secure manner. The video comprises of five pointers for safe and secure mobile banking. The script used for the mobile banking video is as follows:

Cyber-crime is a reality. Ensure your anti virus software is installed, activated and updated regularly. Cybersecurity habits can reduce your risk of becoming a victim.

Check out these top five pointers for safe and secure Mobile Banking.

1. Memorise your Mobile banking PIN and change it regularly. Never share your PIN with anyone.
2. Ensure that you connect to a trusted source of internet, for example your mobile service provider or secure home WiFi.
3. Install an up-to-date anti-virus application to your cell phone. Most banks provide this free of charge to their customers.
4. When your Mobile banking session is complete, do not simply press the Home button. You have to log out from your banking application before closing the app.
5. If you unexpectedly lose connectivity, do not automatically assume that there is a problem with the network or handset. A SIM swop may have occurred. Never ignore an SMS message alerting you to a pending SIM swop request on your account.

Be smart, be secure. A message brought to you by SABRIC and the Nelson Mandela University.

The aim of the video is to educate users on various aspects of mobile banking

including, pin usage and physical device security.

To view the actual video, follow the *link* <https://www.youtube.com/watch?v=1FYVA3MRmgk>.

Video 3: Card Fraud

The main message behind the card fraud video is to educate users on how to make use of banking cards in a safe and secure manner. The video comprises of five pointers for safe and secure card usage. The script for the card fraud video is as follows:

Card fraud is a reality. Reduce your risk of becoming a victim.

Check out these top five pointers and stay card wise.

1. Create a random PIN number that cannot be easily guessed and never share your PIN with anyone.
2. Be cautious of strangers offering to help at the ATM, they could be trying to distract you in order to get your card or your PIN.
3. When withdrawing cash or swiping your card in-store, always ensure that you cover the hand typing your PIN number into the keypad to prevent criminals from stealing your PIN number.
4. Pay attention to notifications from your bank when paying with your card and report any suspicious transactions immediately.
5. Keep your card with you at all times. Should your bank card go missing, inform the bank immediately and cancel your card.

Be smart, be secure. A message brought to you by SABRIC and the Nelson Mandela University.

The video focuses on card usage at: ATMs, point of sales stations and pin usage. The video is simple and addresses basic cyber security issues surrounding

card usage.

To view the actual video, follow the *link* <https://www.youtube.com/watch?v=GQ8s5Tnfcyc>.

Video 4: Malware

The main message behind the malware video is to educate users on how to protect themselves from malware. As with previous videos, this video comprises of five pointers to prevent malware from infecting your device. The aim of the video is to educate users on simple yet effective security techniques. This will prevent users unintentionally installing malware on their devices in turn, compromising its security. The script for the malware video is as follows:

Cyber-crime is a reality. Ensure your anti-virus software is installed, activated and updated regularly. Malicious software can cause damage and give cyber criminals authorised access to your network, computer or mobile device.

Check out these top five pointers to prevent malware from infecting your devices.

1. Always scan hard drives and flash drives with your updated anti-virus software before use.
2. Never open suspicious emails, cyber criminals use attachments which could be disguised as tax refunds, package deliveries and invoices to install malware on your device.
3. Make sure that your firewall is active and set to maximum security and use a strong network password to prevent cyber criminals from accessing your devices.
4. Set your computer or mobile device to run regular virus scans.
5. Ensure that your operating system is updated with the most recent security patches.

Be smart, be secure. A message brought to you by SABRIC and the Nelson Mandela University.

To view the actual video, follow the *link* <https://www.youtube.com/watch?v=4HnrWInq-z8> or alternatively, search for SABRIC's YouTube channel.

Video 5: Computer Hygiene

The main message behind the computer hygiene video is to educate users on how to have good computer hygiene. This video also comprises of five pointers about training ourselves to think proactively about our computer hygiene. The script for

the computer hygiene video is as follows:

Cyber-crime is a reality. Ensure your anti-virus software is installed, activated and updated regularly.

Computer hygiene is about training ourselves to think proactively about our cyber security.

1. Use a strong password to unlock your computer and never share your password with anyone.
2. Always ensure that your operating system, browser and anti-virus program are updated with the most recent security patches.
3. Never click on links or attachments from suspicious e-mails; this can prevent a phishing attack or harmful software such as viruses, spy ware & Trojans being installed and infecting your PC.
4. Do not access internet banking from public computers, malicious software can capture your log-in details and give cyber criminals access to your bank account.
5. Terminate your banking session safely by clicking on the Log Out button before closing the browser window.

Be smart, be secure. A Message brought to you by SABRIC and the Nelson Mandela University.

The aim of the video is to educate users what good computer hygiene is. Allowing users to prevent cyber security incidents from occurring initially. To view the actual video, follow the *link* <https://www.youtube.com/watch?v=xeDegx1stb0>. This section described the five cyber security educational videos, one per topic area. The average length of each educational video is approximately 1 minute long to ensure viewers keep focus throughout the duration of the video. Each educational video has a corresponding cyber security quiz.

The effectiveness of the research instrument as a cyber security educational tool was determined by the data gathering aspect or data gathering mechanism, to be discussed in the section to follow.

5.3 Data Gathering Aspect

As mentioned earlier, the research approach followed is that of experiment. The aim being to provide evidence towards proving that an educational approach, utilising social networking, can be effective. In the context of this research data gathering is conducted via the data gathering mechanism. The data gathered will be used in order to argue that towards the effectiveness of an educational approach, utilising social networking. Results gathered will be analysed and discussed in the chapter to follow.

The data gathering mechanism consists of two parts. The initial part of the data gathering mechanism forms part of the quiz. While the second part consists of a poll held at the end of the educational video. The quiz, alongside raising user awareness, has been used to capture statistical data about the level of awareness and knowledge that users of cyber-driven financial transactions possess.

The quiz questions are close-ended, multiple-choice answer questions which relate to the most prominent threat situations users face concerning cyber-driven financial transactions. This allows for some approximation of user's awareness levels and knowledge to be rated per quiz. The primary data gathered from the quiz includes;

- Correct answers
- Incorrect answers
- Average score
- Number of participants
- Participant origin

- Participant device
- Average elapsed time

The ratio of correct and incorrect answers gives some indication of the users level of awareness and knowledge on the specific topic. Incorrect answers indicate that users might lack awareness and knowledge to conduct these cyber services in a safe and secure manner.

The second part of the data gathering mechanism consists of a poll asked at the end of each video. The poll attempts to determine if the user feels more positive and assured of the level of knowledge on the subject matter acquired. Users are only polled at the end of the video, only if they complete the associated cyber security quiz. In the context of this research study, the poll at the end of educational video is the most vital data gathered. Due to the theory, that an educational approach, utilising social networking, can educate users of cyber-driven financial transactions. As results from the aforementioned poll determines if indeed users did benefit from an educational approach, utilising social networking.

Both parts of the data gathering mechanism, therefore, form part of the research instrument and is applied in the context of this research study. The combination of both parts of the data gathering mechanism, indicates the level of awareness and education before and after the research instrument has been used. All five cyber security quizzes and related educational videos follow the data gathering mechanism outlined in this section. The results from the research instruments implementation will be presented in the chapter to follow.

5.4 Conclusion

Users of cyber-driven financial transactions are required to take a bigger responsibility than ever for their own cyber safety and security. Therefore, they need an appropriate level of awareness and associated education to make use of their cyber services in a safe and secure manner. As such, this research study attempts to aid users in achieving this by utilising social networking. As discussed in this

chapter, the research instrument within the social media domain has been detailed, alongside the data gathering mechanism which has been used to collect relevant primary data. Thus, fulfilling the aim of this chapter.

The chapter to follow will discuss, the implementation of the research instrument and the results obtained from the data gathering mechanism. In turn, providing evidence, towards proving the theory that an educational approach, utilising social networking, can be effective in educating users of cyber-driven financial transactions.

Chapter 6

Results and Analysis

This research study attempts to provide evidence towards proving a theory that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions, allowing them to conduct said transactions in a more safe and secure manner. This chapter serves to present said evidence from the social networking instrument.

6.1 Introduction

From the previous chapter, it was understood that the research instrument used a two-fold approach. Firstly, five cyber security quizzes and secondly, five accompanying educational videos. The cyber security quizzes and educational videos focus on five main topic areas that were identified to be most relevant in both how users are negatively affected and how lacking cyber security education, awareness, and training is. These topic areas are: online shopping, mobile banking, card fraud, malware and computer hygiene. Furthermore, the data gathering aspect used in this research study comprises of two parts. The initial part of the data gathering forms part of the quiz. While the second part consists of a poll held at the end of the educational video. The first part allows for the approximation of awareness of users before the educational video while also gaining interest. The second part enables the researcher to gauge if users did indeed benefit from an educational

approach, utilising social networking. Thus, providing evidence towards proving that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions and therefore allowing them to conduct said transactions in a more safe and secure manner.

The aim of this chapter is to discuss the results from the aforementioned research instrument. The objective being to provide evidence towards proving that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions. The chapter will begin by describing the implementation process of the experiment. This will be followed by discussing the results from each cyber security quiz and educational video. The chapter will be concluded by providing sound argumentation to prove that aforementioned theory holds true.

6.2 Implementation and Results of Experiments

The research instrument was distributed through social media channels (Facebook, YouTube, Twitter and Instagram). The distribution took place primarily through a Facebook campaign which took place in partnership with the South African Banking Risk Information centre (SABRIC). This allowed for a wider audience to be reached, as SABRIC is an authority in the local banking environment. The initial campaign began on the 27th of March 2018. SABRIC released a media statement alongside the aforementioned sponsored Facebook campaign. The media release can be viewed via the following *link*, <https://bit.ly/2I7rrSR>.

The sponsorship consisted of promoting the cyber security quizzes via sponsored adverts on Facebook directly and promoting the educational videos individually through paid adverts on YouTube. This sponsorship allowed for a greater target audience to be reached. While the campaign was being run, the quizzes were also shared from other sources. These sources included, the researchers own Facebook account and any participants that opted to share the quizzes themselves. The social networking instrument was also distributed through the Nelson Mandela University' Facebook page and through internal e-mail communication. This

allowed the quizzes and videos to be shared beyond just the social media campaign. As of the 1st November 2018 the social media campaign is still ongoing, as such participants are still taking part in quizzes and viewing the educational videos. The findings presented in this chapter are statistics gathered up to the 1st of November 2018 from the initial distribution date 27Th March 2018.

As mentioned previously, a total of five cyber security quizzes and five accompanying educational videos have been created and distributed. They form part of the research instrument. The sections to follow will discuss the results from the aforementioned cyber security quizzes and educational videos.

6.2.1 Online Shopping Results

As seen in Figure 6.1, as of the 1st November 2018 the online shopping quiz has been visited 940 times. Furthermore, the quiz saw 817 attempts by participants.

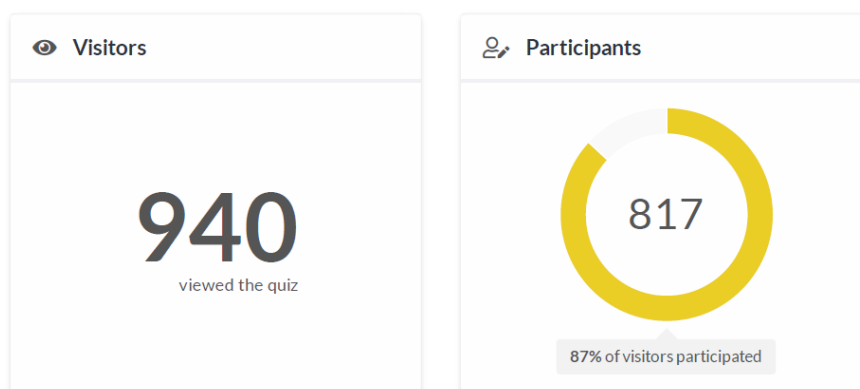


Figure 6.1: Online Shopping Visitors and Participants

As a result has shown in Figure 6.1, 87% of visitors became participants by actually answering the cyber security quiz. The online shopping quiz has been completed as shown in Figure 6.2, 832 times, this indicates that certain participants attempted the quiz more than once. However, not all forms were completed fully, 832 equates to only 91% of forms being fully completed.

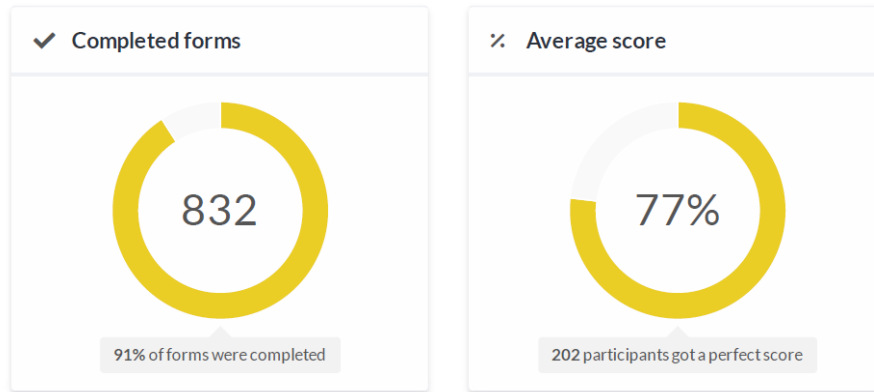


Figure 6.2: Online Shopping Completed Forms and Average Score

Moreover, Figure 6.2 shows that the average score of participants was 77%, while 202 participants received a perfect score. Due to the nature of social networking not all participants were from South Africa. It can be seen that, 97.8% of participants were South African while the remainder come from other countries (Figure 6.3).

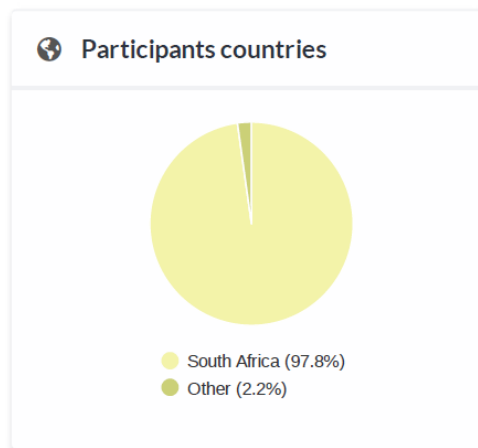


Figure 6.3: Online Shopping Participant Origin

As shown in Figure 6.4, 76% of users accessed the online shopping quiz via a

computer and 24% of participants accessed it via a mobile device.

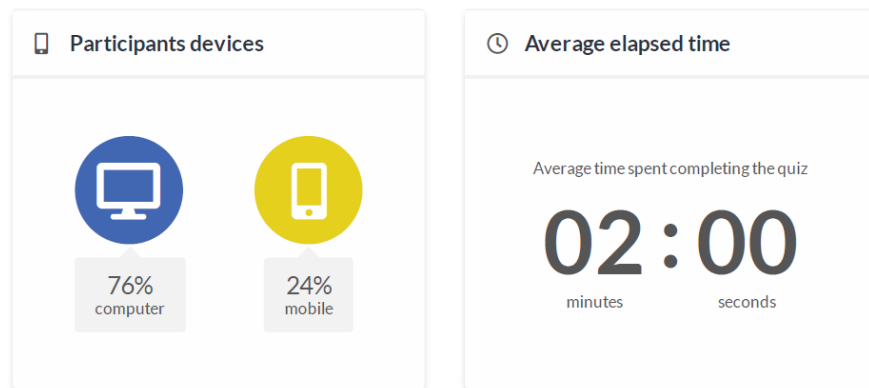


Figure 6.4: Online Shopping Participant Device and Average Time

Moreover, as shown in Figure 6.4, the average time taken to complete the online shopping quiz was 2 minutes and 0 seconds. The average time indicates that users did not spend a significant amount of time on these quizzes, as envisaged.

Due to the educational videos being promoted separately from the cyber security quizzes, the online shopping video was viewed up to the 1st November 2018, 38 141 times, as shown in Figure 6.5.



Sabric Survey Online Shopping (Lifetime)	
Title	Analytic
Watch Time	37,057 (minutes)
Average View Duration	0:58
Views	38,141
Impressions	92,279
Average % Viewed	92%
Highest watch time by device	Computer - 67%
Male	60%
Female	40%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

Figure 6.5: Online Shopping Video Statistics

The majority of viewers being male at 60% while females viewers accounted for 40% (Figure 6.5). From the poll held at the end of the online shopping educational video, asking viewers whether the educational experience was useful, 100% of participants agreed that they did feel the experience was worthwhile and they learnt something.

6.2.2 Mobile Banking Results

As compared to the online shopping cyber security quiz, the mobile banking cyber security quiz as indicated by Figure 6.6, was viewed 918 times.

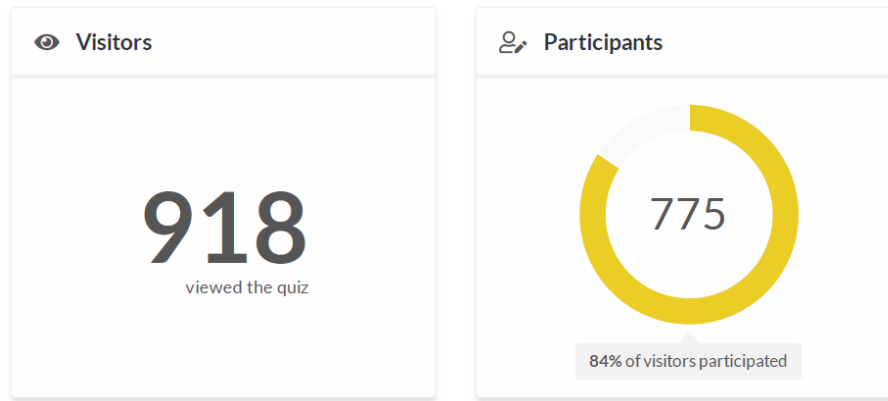


Figure 6.6: Mobile Banking Visitors and Participants

Figure 6.6 shows, that 918 users that viewed the quiz and 775 participated by completing the quiz. This equates to 77% of visitors becoming participants. Furthermore Figure 6.7 shows, that the mobile banking cyber security quiz was completed 951 times.

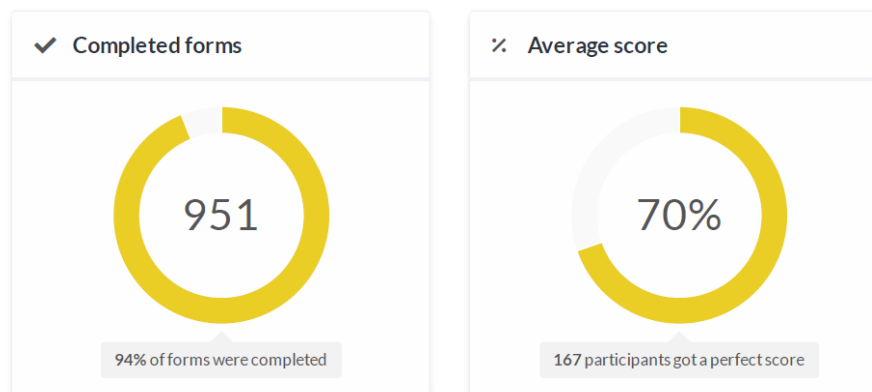


Figure 6.7: Mobile Banking Completed Forms and Average Score

Subsequently, Figure 6.7 shows, the average score for the mobile banking cyber quiz on the 1st November 2018 is 70%, while 167 participants achieved a perfect score. As with the previous quiz, not all participants were South African as shown in Figure 6.8.

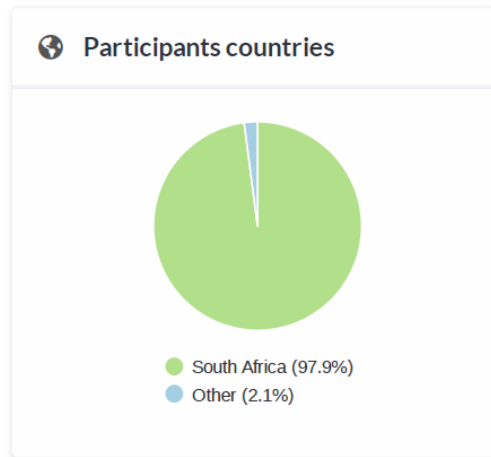


Figure 6.8: Mobile Banking Participant Origin

As seen in Figure 6.8, 97.9% of participants are South African while 2.1% are from other countries. Figure 6.9 below, shows the split between devices used and average time taken to complete the mobile banking cyber security quiz.

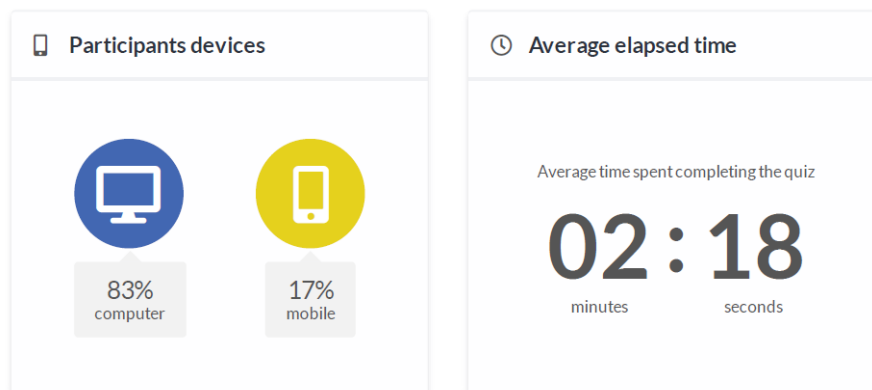


Figure 6.9: Mobile Banking Participant Device and Average Time

As seen in Figure 6.9, 83% of participants accessed the quiz via computers while 17% preferred mobile devices, while the average time taken to complete the quiz was 2 minutes 18 seconds. As with the online shopping educational video, the mobile banking video was prompted separately.



Sabric Survey Mobile Banking (Lifetime)	
Title	Analytic
Watch Time	43,311 (minutes)
Average View Duration	1:02
Views	41,616
Impressions	91,994
Average % Viewed	91%
Highest watch time by device	Computer - 66%
Male	58%
Female	42%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

Figure 6.10: Mobile Banking Video Statistics

The video was viewed 41 616 times up to the 1st November 2018 with 58% of viewers being male and 42% female (Figure 6.10). Furthermore, 66% of viewers agreed that the experience gained from the social networking approach was indeed beneficial to their mobile banking safety and security. As a result, the majority confirming that they indeed did learn something.

6.2.3 Card Fraud Results

On the 1st November 2018 the card fraud cyber security quiz, as shown in Figure 6.11, has been visited the most, with 1200 visitors while 985 became participants by successfully completing the quiz.

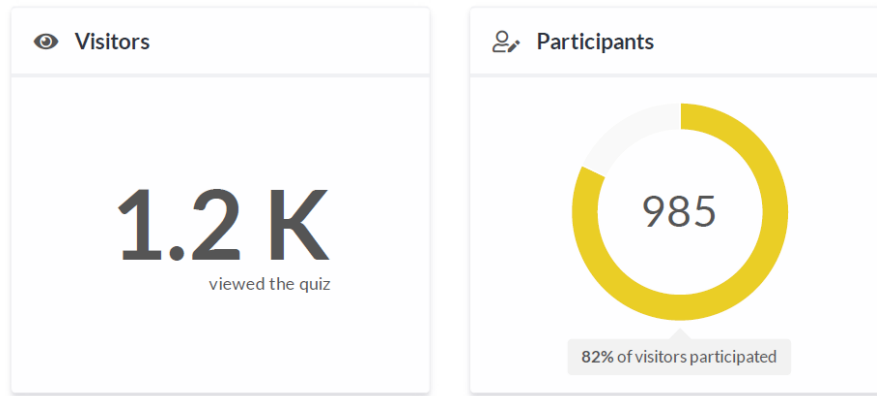


Figure 6.11: Card Fraud Visitors and Participants

It can be seen from Figure 6.11, that 985 participants equates to 82% of visitors becoming participants. Furthermore, as shown in figure 6.12, the quiz has been successfully completed 926 times.

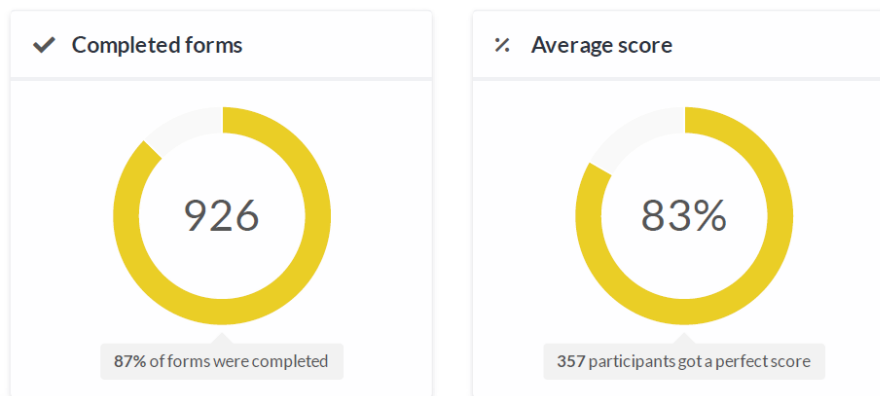


Figure 6.12: Card Fraud Completed Forms and Average Score

From the completed forms, as shown in Figure 6.12, the average score is 83% while 357 participants had a perfect score. Similar to the previous quizzes, not all participants are from South Africa (Figure 6.13).

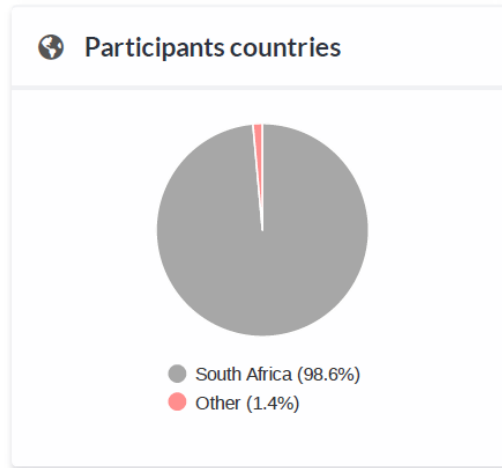


Figure 6.13: Card Fraud Participant Origin

It can be seen from Figure 6.13, that 98.6% of participants were South African while the remainder being from different countries. Figure 6.14 shows that 64% of participants preferred to access the quiz via a computer while 36% preferred to access it via a mobile device.

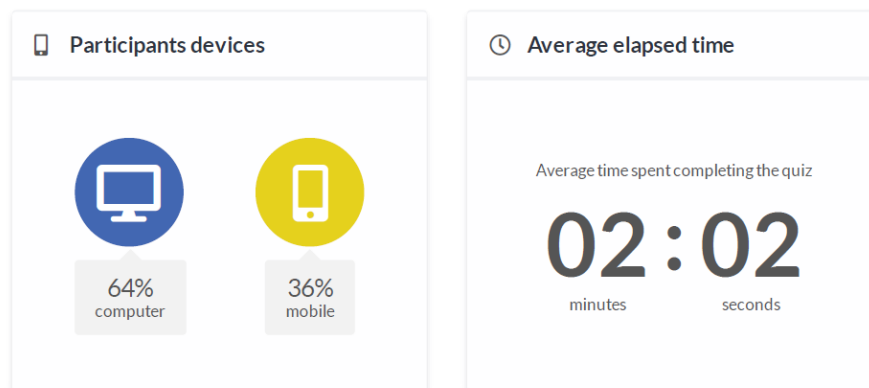



Figure 6.14: Card Fraud Participant Device and Average Time

Moreover, Figure 6.14 shows that the average time taken to complete the card fraud cyber security quiz is 2 minutes and 02 seconds. Alongside the card fraud

cyber security quiz, the accompanying educational video was viewed 74 414 times up to 1st November 2018 (Figure 6.15).



Sabric Survey Card Fraud (Lifetime)	
Title	Analytic
Watch Time	63,736 (minutes)
Average View Duration	0:51
Views	74,414
Impressions	260,786
Average % Viewed	92%
Highest watch time by device	Computer - 61%
Male	56%
Female	44%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

Figure 6.15: Card Fraud Video Statistics

Furthermore, Figure 6.15 shows, 56% of viewers are male while the remainder 44% are female. The results from the poll at the end of the educational video showed that 68% of viewers agreed that they did indeed benefit from the educational approach using social networking.

6.2.4 Malware Results

The malware cyber security quiz as shown in Figure 6.16, received the third highest visitors, namely 1000. However, from the 1000 visitors only 803 became participants.

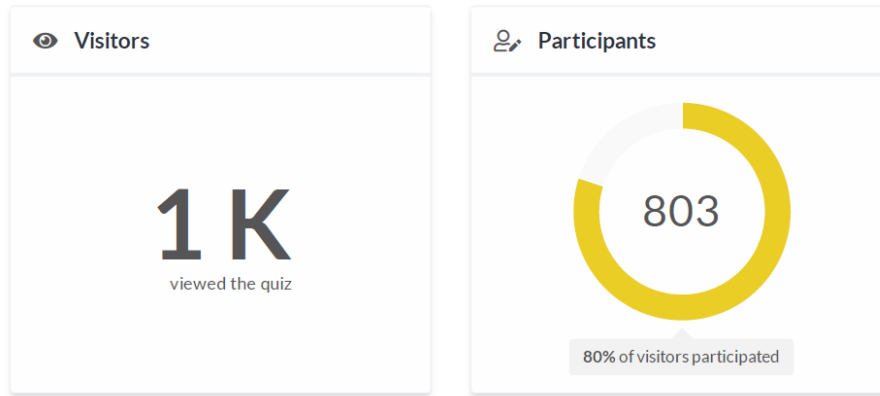


Figure 6.16: Malware Visitors and Participants

Figure 6.16 shows, 803 participants equates to 80% of all visitors becoming participants. Subsequently, as shown in Figure 6.17, 90% of the total number of forms have been completed which equates to 897 fully completed quizzes.

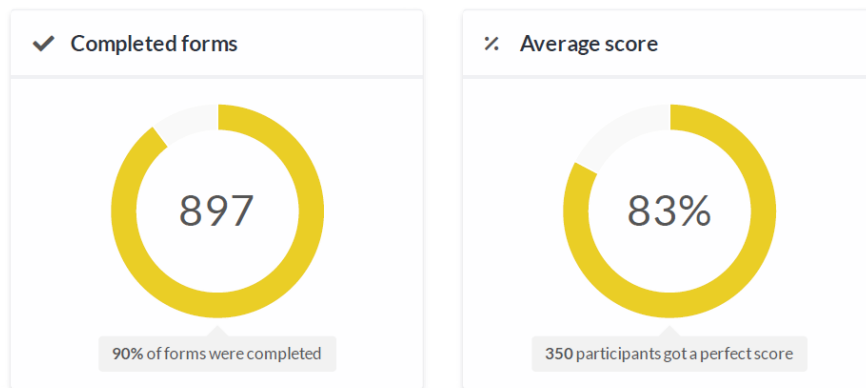


Figure 6.17: Malware Completed Forms and Average Score

Figure 6.17 indicates, that the average score for the malware quiz was 83%, while 350 participants got a perfect score. Due to the nature of social networking not all participants were from South Africa. As shown in Figure 6.18, 98.5% of participants were South African while the remainder participated from other countries.

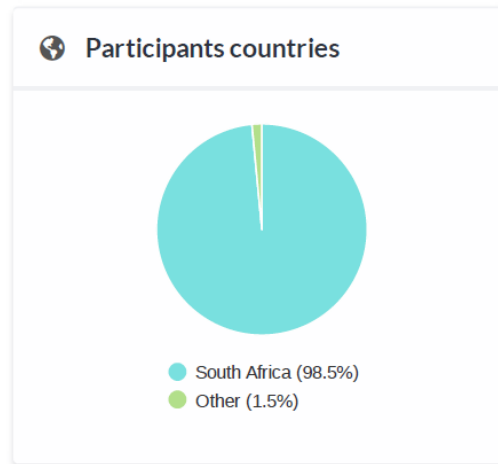


Figure 6.18: Malware Participant Origin

As shown in Figure 6.19, participants preferred to access the malware cyber security quiz via computers (83%) while the remainder accessed it via a mobile device.

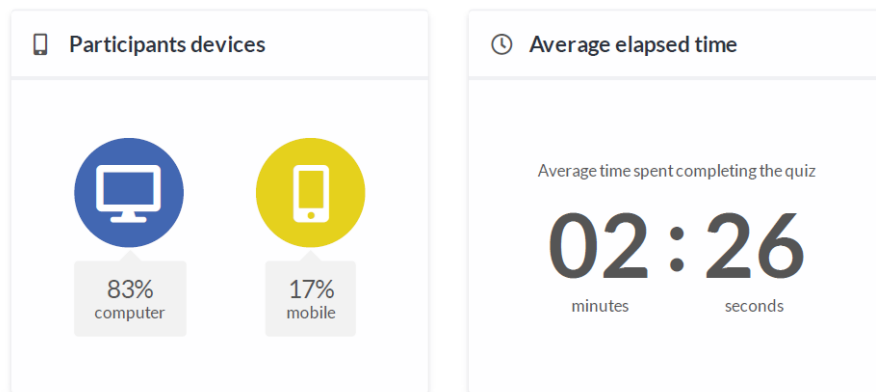



Figure 6.19: Malware Participant Device and Average Time

Moreover, as shown in Figure 6.19, the average time taken to complete the malware quiz was 2 minutes and 26 seconds. Up to the 1st November 2018, this is the longest average time out of any of the cyber security quizzes.

The malware educational video has been viewed 40 731 times as of the 1st November 2018 (Figure 6.20).



Sabric Survey Malware Protection (Lifetime)	
Title	Analytic
Watch Time	38,613 (minutes)
Average View Duration	0:56
Views	40,731
Impressions	104,038
Average % Viewed	92%
Highest watch time by device	Computer - 66%
Male	58%
Female	42%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

Figure 6.20: Malware Video Statistics

Figure 6.20 shows, viewers are split between 58% male and 42% female. The poll at the end of malware educational video, attempted to determine if users did indeed benefit from the educational approach utilising social networking, of which 83% of viewers did agree that they benefited from the approach in some manner.

6.2.5 Computer Hygiene Results

The computer hygiene cyber security quiz received the second highest number of visitors namely 1040, as indicated in Figure 6.21. Furthermore, 84% of visitors become participants (Figure 6.21).

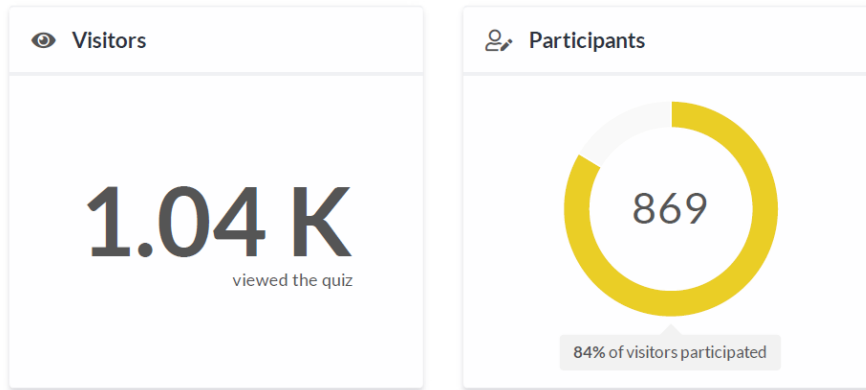


Figure 6.21: Computer Hygiene Visitors and Participants

As shown in Figure 6.21, that results in 869 participants. From Figure 6.22, it can be seen that 848 forms were fully completed.

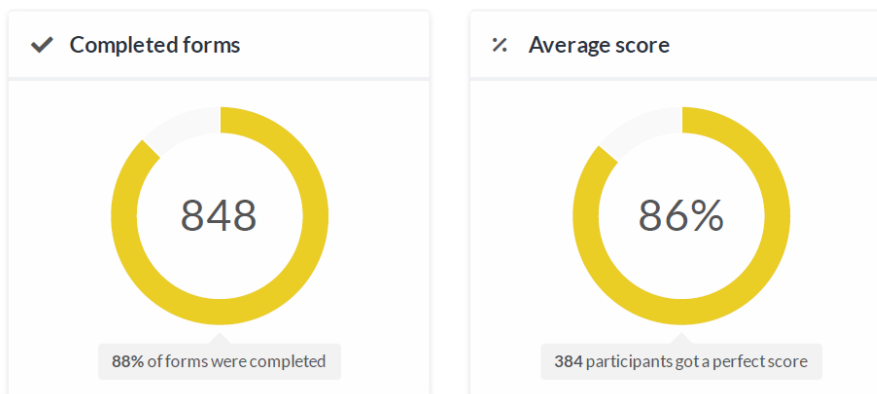


Figure 6.22: Computer Hygiene Completed Forms and Average Score

This, as shown in Figure 6.22, equates to 88% of all quiz forms attempted becoming successfully completed. Similarly to the previous cyber security quizzes, Figure 6.23 shows not all participants are South African.

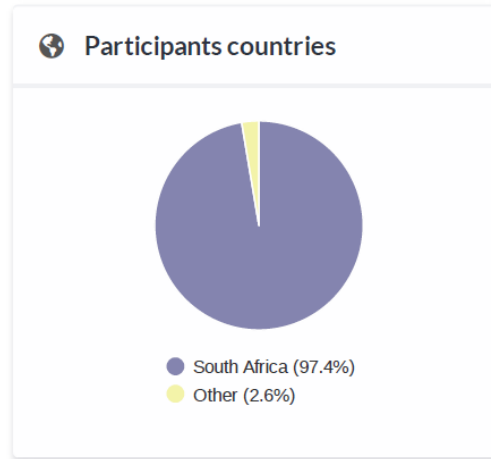


Figure 6.23: Computer Hygiene Participant Origin

Figure 6.23, shows that 97.4% of participants are local to South Africa while remainder being from foreign countries. Participants taking part in the computer hygiene cyber security quiz as shown in Figure 6.24 preferred to access the quiz via computers rather than mobile devices.

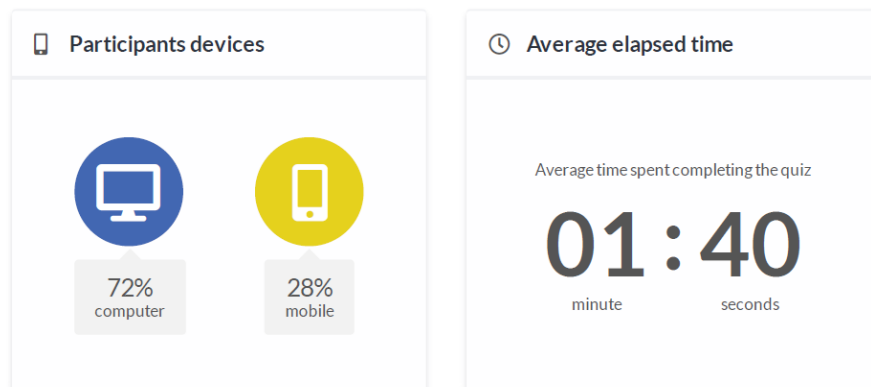



Figure 6.24: Computer Hygiene Participant Device and Average Time

Furthermore, the average time taken to complete the computer hygiene cyber security quiz as shown in Figure 6.24 was 1 minute and 40 seconds. The fastest average time from all the cyber security quizzes. Currently, the computer hygiene

educational video has received the lowest viewership as of the 1st November 2018 at 20 258 viewers as seen in Figure 6.25.



Sabric Survey Computer Hygiene (Lifetime)	
Title	Analytic
Watch Time	20,615 (minutes)
Average View Duration	1:00
Views	20,258
Impressions	50,393
Average % Viewed	91%
Highest watch time by device	Computer - 60%
Male	65%
Female	35%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

Figure 6.25: Computer Hygiene Video Statistics

As of the 1st November 2018, viewers comprise of 65% male and 35% female (Figure 6.25). Moreover, the poll results show that 75% of viewers indeed did benefit from the educational approach utilising social networking. To view an extended set of results, including how participants answered each question, please refer to Appendix C.1.

Thus, it can be seen from the forgone section that the initial experiment began on the 27th of March 2018. The research instrument in the form of the five cyber security quizzes and accompanying educational videos were shared across multiple social networking platforms in order to gain participants. Furthermore, a Facebook campaign was launched in association with SABRIC to garner more interest as well.

The section to follow will present the results of the experiment.

6.3 Analysis of Results

It can be seen from the forgone section, that both the cyber security quizzes and educational videos were popular among cyberspace users. All cyber security quizzes received more than 800 participants while the five educational videos were viewed more than 20 000 times each. As discussed in the previous section, a poll asking whether the cyber security quizzes and educational videos was helpful and whether the participants did benefit educationally, took place at the end of every video. These results were captured and is presented in Table 6.1.

Table 6.1: Educational Video Poll Results

	Percentage of Yes Responses	Percentage of No Responses
Online Shopping Poll	100%	0%
Mobile Banking Poll	66%	34%
Card Fraud Poll	68%	32%
Malware Poll	83%	17%
Computer Hygiene Poll	75%	25%

Table 6.1, shows that the majority of participants, that took part in the experiment, did indeed benefit from the educational approach utilising social networking. Thus, it can be argued that an educational approach utilising social networking can be an effective alternative to traditional approaches as those seen in Chapter 3 of this research study.

Moreover, it can be seen from the number of views recorded that users preferred to go directly to the educational videos rather than following the cyber security quiz educational video route. This might be interpreted that a large number of users are already aware they lack proper knowledge to deal with the cyber threats they face. Irrespective of the standalone YouTube video views, results show that a combination of both the quiz and video can be a successful educational combination. In general, this study argues that participants gained relevant knowledge

and confidence on how to conduct their cyber-driven services safely and securely in cyberspace through a social networking educational approach.

This research study gathered adequate data to argue that the theory that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions, allowing them to conduct said transactions in a more safe and secure manner.

6.3.1 Lessons Learnt from Results

This study has shown that if implemented correctly and made appealing, social media can be used to educate and raise awareness in users, thus allowing them to conduct their cyber-driven financial transactions in a safer and more secure manner. It can, therefore, be argued that that social networking and social media in general, and specifically in the format used in this study, can be used as a possible option for the education of users of cyber-driven financial transactions.

However, from the results discussed in this chapter the following lessons can be learnt:

- Participants did not often share the quizzes.
- Participants preferred to go directly to the educational videos.
- Participants often preferred to access the educational content via computers rather than mobile devices.

6.4 Conclusion

The use of cyberspace, as previously mentioned, has become an essential part of most industries, as well as playing an important roles in the daily lives of social users. This is particularly true in the banking sector, where users make use of ATMs, internet, mobile banking and the like. These users of cyber-driven financial transactions pose a great risk to themselves through negligent or ignorant behaviour. Therefore, relevant cyber security education and awareness is a must

to empower these users to protect themselves. As shown in Chapter 3, while financial institutions do offer some cybersecurity education, awareness-raising and training, these offerings are similar in nature and often follow a traditional learning approach. Therefore, the aim of this chapter, to provide evidence towards proving the theory that an educational approach, utilising social networking, can indeed be used as an educational tool towards effective cyber security education has been conducted satisfactorily. As may be seen from the results of the data gathered, such an approach had a positive effect on the majority of users.

The chapter to follow will conclude this research study.

Chapter 7

Conclusion

As the discussion thus far has shown, the study has produced evidence to assist in proving the theory that an educational approach, utilising social networking, can be used to educate the users of cyber-driven financial transactions. Accordingly, this will support the users of cyber-driven financial transactions in conducting such transactions in a safer and more secure manner.

7.1 Introduction

It can be argued that a social networking approach to cyber security education, awareness, and training can be an effective alternative to traditional cyber security, education, awareness, and training. The effectiveness of said approach can be seen in the penultimate chapter, that provided evidence towards proving the theory that such an approach is indeed effective.

This chapter will firstly, discuss the findings made throughout this research study. Secondly, it is important to confirm that all research objectives were met. Thirdly, through meeting the research objectives various research contributions have been produced and will be highlighted. Lastly, to conclude the potential for future research will be discussed.

7.2 Summary of Findings

It is clear that cyberspace plays a crucial role in the day to day lives of organisations and social users. Moreover, social users can be seen to contribute the majority of cyberspace usage. As such, social users need to ensure that they can adequately make use of cyberspace, including protecting themselves from associated cyberspace threats.

From the discussion in Chapter 2, it is clear that cyberspace is of crucial importance to all users. Furthermore, cyberspace has evolved overtime to offer modern services including cyber-driven financial transactions. In turn creating a social users dependent on cyberspace, this users forming a cyberculture (Horn, 2010). It can also be seen from Chapter 2, that information security forms part of cyber security in the greater context of information technology. As such, similar to information security, the human factor still plays a key role in securing cyberspace. As such, organisations have various best practices and international standards that aid in the creation of cyber security education, awareness, and training programs (ISO/IEC 27032, National Cyber Security Framework). This allows for organisational users to become a strength rather than a weakness in the cyber security process. These cyber security education, awareness, and training programs, as discussed in Chapter 2, can be delivered through various mediums. Moreover, it was argued that organisations recognise their employees as potential weaknesses. Chapter 2, also served to highlight how vulnerable social users are. Unlike users in organisations, social users do not have cyber security education, awareness, and training readily and easily available.

Subsequently, Chapter 3 discussed a particular group of social users, namely users of cyber-driven financial transactions. Cyber-driven financial transactions, for the purposes of this study were defined as, any financial transaction that involves cyberspace or the internet. Chapter 3, argued that there has been a shift in responsibility from financial institutions to users of cyber-driven financial transactions. Moreover, Chapter 3, served to highlight various typical user errors and threats. A critical assessment of current educational offerings from financial institutions was also conducted and the findings were also discussed in Chapter 3.

As a result, it was argued in Chapter 3, that there is a fundamental shortcoming with the approach being taken by banks to educate their users on how to conduct cyber-driven financial transactions in a safe and secure manner. In turn confirming that there is a need for an alternative educational approach.

To address this need of an alternative educational approach the theory that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions was proposed. Chapter 4, highlighted the research approach of this research study, namely experimentation, to prove a theory using sound argumentation and data gathered. Furthermore, Chapter 4, discussed the research approach taken in order to create the research instrument used in this research study. Chapter 4, further discussed the research design instrument design including criteria influencing a social networking approach and the process to identify relevant cyber security educational topics. Ultimately, the research approach followed gave way to the social networking instrument.

By using the research approach detailed in Chapter 4, the research instrument was created. Chapter 5, discussed the details of the research instrument how it was used. Each cyber security quiz was detailed and the accompanying educational video. How data was gathered was also discussed in said chapter.

Upon the completion of the research instrument, it was distributed on 27th March 2018. Chapter 6, discussed the findings derived from data gathered by the research instrument. Results discussed were collected from the initial distribution date until the 1st of November 2018. Chapter 6, argued that an social networking approach can be a viable alternative to traditional cyber security education, awareness, and training. Results in Table 6.1 indicates that the majority of participants agreed that the approach utilising social networking was indeed useful and beneficial to there cyber security. Consequently, providing evidence towards proving the theory that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions.

The subsequent section will discuss the how the objectives of this research study were met.

7.3 Meeting the Objectives

This research study aimed to address cyber security education, awareness, and training for users of cyber-driven financial transactions. In light of that, Chapter 1 stated that the primary objective of this research study is to provide evidence towards proving the theory that an educational approach, utilising social networking, can be used to educate users of cyber-driven financial transactions. In turn, allowing these users to conduct said transactions in a more safe and secure manner.

To achieve the primary objective, Chapter 1 identified various secondary objectives that aided in that addressed the aim of this research collectively. These secondary objectives are:

1. Critically assess material currently offered to users of cyber-driven financial transactions.
2. Determine an alternative educational approach, to educate users of the aforementioned audience.
3. Determine which social networking approaches can be used.
4. Identify typical topics and aspects that need to be educated to the audience at hand.

In order to *"critically assess material currently offered to users of cyber-driven financial transactions"*, Chapter 3 led with a discussion on typical user errors and threats. This was done through a literature study. This was followed by an assessment of current cyber security education, awareness, and training provided by financial institutions. This was done by assessing financial institutions' websites. In doing so, it was clear that an alternative educational approach was required.

After addressing the first secondary objective, it was necessary to *"determine an alternative educational approach, to educate users of the aforementioned audience"*, as such allowing for the creation of the research instrument. Due to the involvement of cyber security experts from the South African Banking Risk

Information Centre (SABRIC), the approach followed needed to meet set requirements. In turn, these requirements dictated the approach followed. As such, a two-fold approach was decided upon, which comprised of a combination of an awareness raising game-type quiz and an accompanying educational video.

As such, this led to the third secondary objective, "*determine which social networking approaches can be used*", in turn allowing for the creation of the research instrument. The following criteria influenced the approach followed:

- The target audience being the majority of South African cyber-driven financial transactions users.
- The research instrument had to be designed to allow users to be made aware in an alternative method.
- The research instrument needed to engage users, allowing them to be educated in an alternative manner.

As such, this criteria in combination with the approach followed resulted in the research instrument. A two-fold approach was decided upon for the research instrument, which comprised of a combination of an awareness raising game-type quiz on Facebook and an accompanying educational video on YouTube.

Nonetheless, this led to the fourth secondary objective to "*identify typical topics and aspects that need to be educated to the audience at hand*", in order to ensure that users were educated on the most crucial threats. This was done initially, through a literature study and resulted in a topic map. Moreover, further revisions to the topic map were done via two rounds of discussions led by cyber security experts (SABRIC and Nelson Mandela University). These identified topics were then grouped into five topic areas. These five topic areas were subsequently used in the research instrument. Thus, utilising the research approach outlined in Chapter 4 and outputs from the secondary objectives, the research instrument was created.

As a result of the above, the achievement of the four secondary objectives addressed the primary objective of providing evidence towards proving the theory that an educational approach, utilising social networking, can be used to educate

users of cyber-driven financial transactions. In turn, allowing them to conduct said transactions in a more safe and secure manner. Thus, it can be argued that all the stated objectives were met.

During the length of this research study various research outputs were produced. The section to follow will discuss said outputs.

7.4 Summary of Contributions

This research study produced two research outputs that collectively represent the entire research contribution.

Research Contribution: The Research Instrument

The research instrument was created, as a means to provide evidence can be considered the first research output. This research instrument was discussed extensively in Chapter 5. The first part of the research instrument is the cyber security quizzes, found on Facebook. The second part of the research instrument are the accompany educational videos hosted on YouTube. The results of the research instrument were detailed in Chapter 6.

Research Contribution: Publication

The final research contribution was in the form of an academic publication. A peer-reviewed research paper was published in the proceedings of the 2018 International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018), that took place in Dundee, Scotland.

7.5 Future Research

The research instrument was created, as a means to provide evidence can be considered the primary output of this research. This research instrument was discussed extensively in Chapter 5. The instrument was created with input from two groups of cyber security experts. Due to the involvement of these cyber security experts,

limitations to the study exist. Firstly, due to the study taking place in South Africa and cyber security experts being South African topics users are made aware of and educated on are those primarily affecting South African citizens. Secondly, due to the close involvement from the group of cyber security experts from SABRIC the research is aligned with specific outcomes set by them such as ensuring a high standard of work and marketability. Furthermore, the study only focuses on results obtained directly after the quiz and video have been completed. Possible additional research includes assessing users for knowledge retention to verify if the approach used can be a long term solution.

However, with the limitations in context this study has shown that, if implemented correctly and made appealing, social media can be used to educate and make the users of cyber-driven financial transactions more aware of the risks involved in cyberspace, thus allowing these users to conduct their cyber-driven financial transactions in a safer and more secure manner. It can therefore, be seen that, social networking and social media in general and specifically in the format used in this study, can be a possible option for the education of users of cyber-driven financial transactions. However, further research should be done to improve the process.

7.6 Epilogue

Cyberspace and cyber-driven services are utilised in most industries and are a part of the lives of many social users. This is particularly true in the banking sector, where users make use of ATMs, and internet and mobile banking. These users of cyber-driven financial transactions pose a great risk to themselves through their negligent or ignorant behaviour. Therefore, relevant cybersecurity education and awareness is a necessity for these users. Social media and social networking can indeed be used as an educational tool in effective cyber security education, under the following conditions: firstly, that the material can be accessed with ease, secondly, that the material is appealing to users and, thirdly, that the material is not too data or time-consuming.

This study has shown that if implemented correctly and made appealing, social media can be used to educate and raise awareness in users, thus allowing them to conduct their cyber-driven financial transactions in a safer and more secure manner. It is therefore concluded that sufficient evidence has been provided to show that social networking and social media in general, and specifically in the format used in this study, can be used as a possible option for the education of users of cyber-driven financial transactions.

References

- Agnes, M. E. (2004). *Webster's New World College Dictionary, Fourth Edition*.
- APWG. (2017). Phishing Activity Trends Report Q4 2017. (December), 11.
- Batiz-Lazo, B. (2013). *How the ATM Revolutionized the Banking Business*.
- Bawazir, M. A., Mahmud, M., Molok, N. N. A., & Ibrahim, J. (2016). Persuasive Technology for Improving Information Security Awareness and Behavior : Literature Review.
- Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers and Security, 75*, 24–35.
- Carole Déglise, L Suzanne Suggs, P. O. (2012). Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use. *Journal of Telemedicine and Telecare, 18*(5), 273–281.
- Constine, J. (2017). *Facebook now has 2 billion monthly users and responsibility — techcrunch*. <https://techcrunch.com/2017/06/27/facebook-2-billion-users/>. ((Accessed on 10/02/2018))
- Cronin, M. J. (1998). *Banking and finance on the internet*. John Wiley & Sons.
- Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management. *04*, 92-100.

- Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *computers & security*, 26(1), 73–80.
- ENISA. (2012). Collaborative Solutions For Network Information Security in Education.
- Farn, K.-J., Lin, S.-K., & Fung, A. R.-W. (2004). A study on information security management system evaluation assets, threat and vulnerability. *Computer Standards & Interfaces*, 26(6), 501–513.
- Florentine, S. (2015). *Security best practices for users is your first line of defense — CIO*.
- Frauenstein, E. D., & Von Solms, R. (2014). Combatting phishing: A holistic human approach. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*.
- Furnell, S., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal internet users. *Computers & Security*, 26(5), 410–417.
- Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice internet users. *Computers & Security*, 27(7-8), 235–240.
- Gerber, M., & Solms, R. von. (2005). Management of risk in the information age. *Computers & Security*, 24(1), 16–30.
- Gordon, A. (2003). *A modern history of japan: from tokugawa times to the present*. Oxford University Press New York.
- Gubbi, J., Buyya, R., & Marusic, S. (2013). 1207.0203. (1), 1–19.
- Haaften, T. van. (2016). Frans H. van Eemeren, Bart Garssen, Erik C.W. Krabbe, A. Francisca Snoeck Henkemans, Bart Verheij and Jean H.M. Wagemans: Handbook of Argumentation Theory. *Argumentation*, 30(3), 345–351.
- Hansche, S. (2001). *Designing a Security Awareness Program: Part I* (No. 6).

- Horn, S. (2010). *Cyberville: Clicks, Culture, and the Creation of an Online Town*. Grand Central Publishing.
- ISO/IEC. (2013). *ISO/IEC 27002:2013(E) Information technology Security techniques Code of practice for information security controls*.
- ISO/IEC, . (2015). Information technology - Topic Maps ISO/IEC 13250:2015 . *ISO/IEC 13250*.
- ISO/IEC 27032. (2012). INTERNATIONAL STANDARD ISO / IEC: Information technology Security techniques Guidelines for cybersecurity. *2012*, 58.
- Jardine, E. (2015). Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime. *Paper Series(16)*.
- Kakihara, M. (2014). Grasping a global view of smartphone diffusion : An analysis from a global smartphone study. *International Conference on Mobile Business*, 11.
- Kearl, M. (2016). *99 Need-to-Know Stats on the Mobile Customer — Appboy*.
- Klimburg, A. (2012). *National Cyber Security Framework Manual*.
- Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers and Security*, *29(8)*, 840–847.
- Madeline. (2016). *Different Types Of Apps and Their Functions - Mynt Productions*.
- Medne, E. (2016). *Mapa Research - A third of banks have mobile detection*.
- Olivier, M. S. (2009). *Information technology research: A practical guide for computer science and informatics*. Van Schaik.
- Ombudsman Annual Report for Banking Services. (2016). Ombudsman Annual Report 2016 for Banking Services.

- Oxford. (2016). *cyberspace - definition of cyberspace in English — Oxford Dictionaries*.
- Öütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83–93.
- Polański, P. P. (2017). Cyberspace: A new branch of international customary law? *Computer Law and Security Review, 33*(3), 371–381.
- Portal, S. (2018a). *Mobile internet usage worldwide - Statistics & Facts — Statista*.
- Portal, S. (2018b). *Number of social media users worldwide 2010-2021 — Statista*.
- Portal, S. (2018c). *Smartphone users worldwide 2014-2020 — Statistic*.
- Posthumus, S., Solms, R. von, & King, M. (2010). The board and IT governance : The what , who and how. *Framework, 41*(3), 23–33.
- SABRIC. (2017a, December). *Atm safety*. <https://www.sabric.co.za/stay-safe/atm/>. (Accessed on 08/17/2018)
- SABRIC. (2017b, December). *Cheque fraud*. <https://www.sabric.co.za/stay-safe/cheque-fraud/>. (Accessed on 08/17/2018)
- SABRIC. (2017c, March). <https://www.sabric.co.za/stay-safe/deposit-and-refund-scams/>. <https://www.sabric.co.za/stay-safe/deposit-and-refund-scams/>. (Accessed on 08/17/2018)
- SABRIC. (2018a, February). *419 scam*. <https://www.sabric.co.za/stay-safe/419-scam/>. (Accessed on 08/17/2018)
- SABRIC. (2018b, January). *Carrying cash safely*. <https://www.sabric.co.za/stay-safe/carrying-cash-safely/>. (Accessed on 08/17/2018)
- SABRIC. (2018c, January). *Cyber crime*. <https://www.sabric.co.za/stay-safe/cyber-crime/>. (Accessed on 08/17/2018)

- SABRIC. (2018d, January). *E-mail hacking and spoofing*. <https://www.sabric.co.za/stay-safe/e-mail-hacking/>. (Accessed on 08/17/2018)
- SABRIC. (2018e, January). *Identity theft*. <https://www.sabric.co.za/stay-safe/identity-theft/>. (Accessed on 08/17/2018)
- SABRIC. (2018f, February). *Internet banking*. <https://www.sabric.co.za/stay-safe/internet-banking/>. (Accessed on 08/17/2018)
- SABRIC. (2018g, January). *Phishing*. <https://www.sabric.co.za/stay-safe/phishing/>. (Accessed on 08/17/2018)
- SABRIC. (2018h, February). *Safe banking awareness*. <https://www.sabric.co.za/stay-safe/safe-banking-awareness/>. (Accessed on 08/17/2018)
- SABRIC. (2018i, January). *Vishing*. <https://www.sabric.co.za/stay-safe/vishing/>. (Accessed on 08/17/2018)
- SABRIC. (2018j, April). <https://www.sabric.co.za/stay-safe/card-fraud/>. <https://www.sabric.co.za/stay-safe/card-fraud/>. (Accessed on 08/17/2018)
- SABRIC. (Marcha, 2018). <https://www.sabric.co.za/stay-safe/changing-bank-details-scam/>. <https://www.sabric.co.za/stay-safe/changing-bank-details-scam/>. (Accessed on 08/17/2018)
- SABRIC. (Marchb, 2018). <https://www.sabric.co.za/stay-safe/cyber-security/>. <https://www.sabric.co.za/stay-safe/cyber-security/>. (Accessed on 08/17/2018)
- SANS Institute. (2015). SANS Securing The Human - 2015 Security Awareness Report. *SANS AInstitute InfoSec Reading Room*, 12.
- Shapshak, T. (2017). *South Africa Has 21 Million Internet Users*.
- Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92–100.

- Simone, M. P. (2009). NS Ins titu Au tho r r eta ins l rig. *Sans Institute*, 27.
- Staff Writer. (2017). *The biggest banks in South Africa by customers*.
- Statista. (2016). *App stores: number of apps in leading app stores 2016* — Statista.
- Symantec. (2016). Internet Security Threat Report Internet Report. *Network Security*, 21, 81.
- Van Eemeren, F. H., & Grootendorst, R. (2003). A systematic theory of argumentation: The pragma-dialectical approach. *A Systematic Theory of Argumentation: The Pragma-Dialectical Approach*, 25(1), 1–216.
- Verizon. (2017). 2017 Data Breach Investigations Report Tips on Getting the Most from This Report. *Verizon Business Journal*(1), 1–48.
- Von Solms, R., Thomson, K. L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, 38, 97–102.
- Von Solms, R. (1998). Information security management (3): the code of practice for information security management (bs 7799). *Information Management & Computer Security*, 6(5), 224–225.
- Von Solms, S. H., & Solms, R. v. (2008). *Information security governance*. Springer Publishing Company, Incorporated.
- Wacker, J. (1998). A definition of theory: research guidelines for different theory-building research methods in operations management. *Journal of Operations Management*, 16(4), 361–385.
- WaterISAC. (2015). 10 Basic Cybersecurity Measures: Best Practices To Reduce Exploitable Weaknesses And Attacks. (June), 9.

West, P. (2015). *History of British Banknotes*.

Whittman, M. E., & Mattord, H. J. (2013). *Management of Information Security*
Fourth Edition. 545.

Appendix A

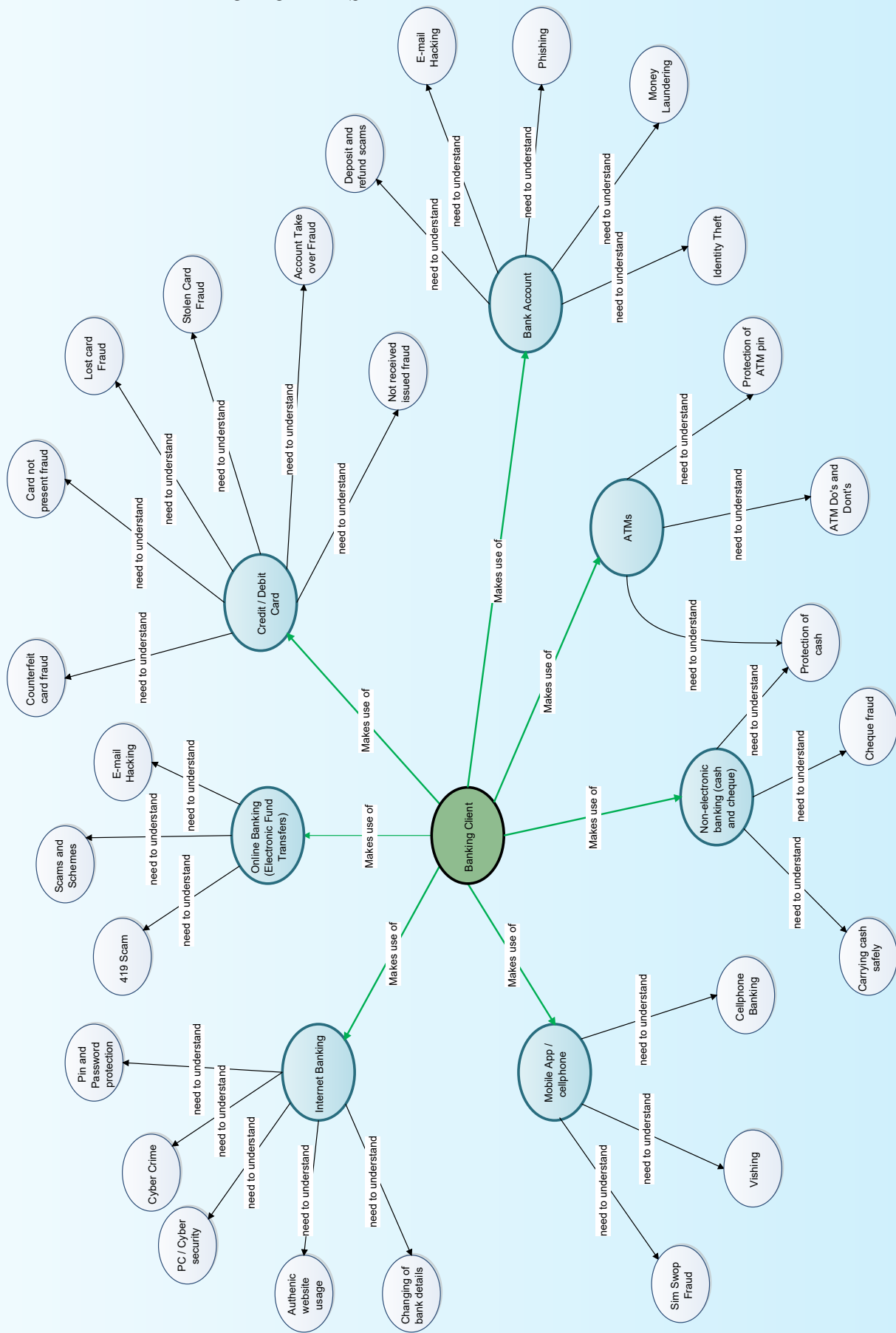
Topic Maps

Appendix A includes the various topic maps discussed in 4 that were created throughout the duration of the study:

1. Phase One Topic Map
2. Phase Two Topic Map
3. Phase Three Topic Map

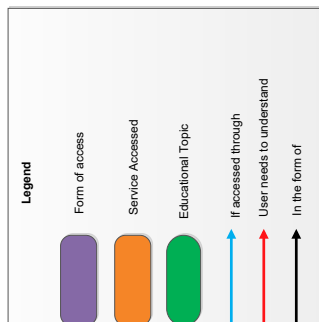
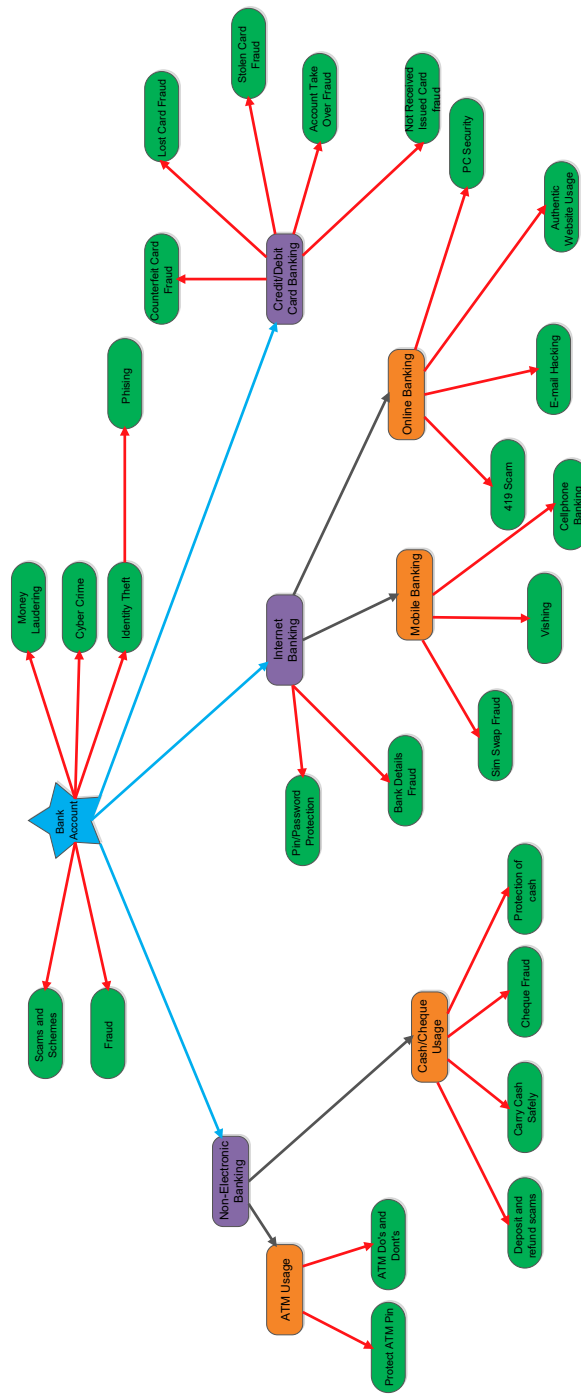
A.1 Phase One Topic Map

The initial phase of the process to select relevant cyber security educational topics was conducted using literature. The image below represents the initial topic map (version 1).



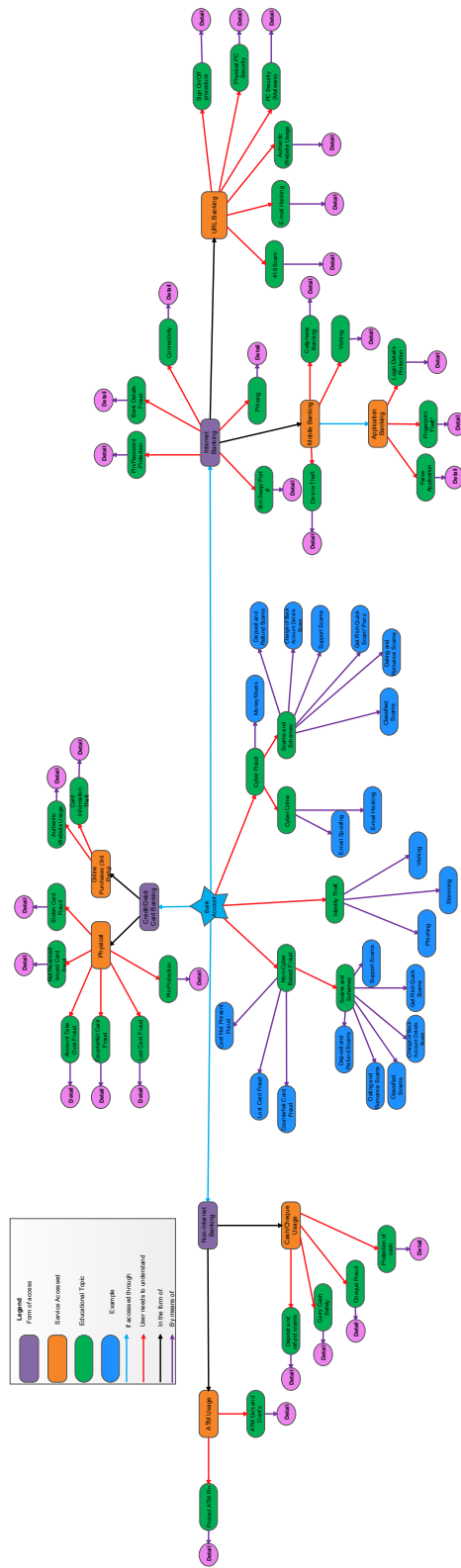
A.2 Phase Two Topic Map

The second phase of the process to select relevant cyber security educational topics was conducted internally at the Nelson Mandela University. A group of academic cyber security experts provided input on the initial topic. The image below represents a revised topic map (version 2).



A.3 Phase Three Topic Map

The third phase of the process to select relevant cyber security educational topics was conducted with cyber security experts from SABRIC. The image below represents the finalised topic map (version 3).



Appendix B

Quiz Questions

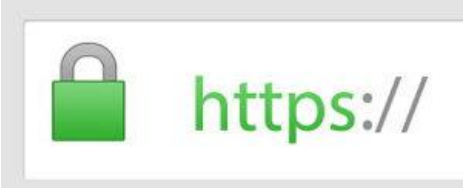
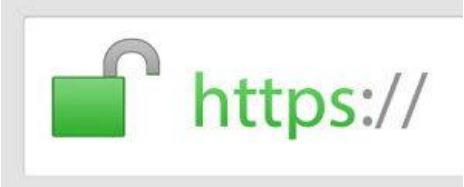
Appendix B includes the quiz questions utilised in the research instrument:

1. Online Shopping
2. Mobile Banking
3. Card Fraud
4. Malware
5. Computer Hygiene

B.1 Cyber Security Quizzes

The below list of tables represents all quiz questions used in the research instrument of this research study.

ONLINE SHOPPING

Question 1: Which of the following provides an indication that you are communicating securely with a website?	
Answer A:	
Answer B:	
Correct Answer Text: Right answer! Always look for the padlock symbol and <i>https</i> in the address bar of your web browser as it is safer and more secure.	Incorrect Answer Text: Wrong answer! Always ensure that you are using an <i>https</i> website as it is safer and more secure. Look for the closed padlock symbol and <i>https</i> in web browser address bar.

Question 2: Which of the following personal details should be given to an online merchant when requested during registration?	
Answer A:	Name
Answer B:	ID number
Answer C:	Birth date
Answer D:	CVV number
Correct Answer Text: Right answer! An online merchant should never ask for personal details beyond your name.	Incorrect Answer Text: Wrong answer! No website needs your ID number or your birth date to process your order. This information is of no use to online merchants, but it is of great use to someone who wants to steal your identity.

ONLINE SHOPPING

Question 3: Which of the following is an example of a strong password?	
Answer A:	12345
Answer B:	john1993
Answer C:	ABC123
Answer D:	A3\$6b3
Correct Answer Text: Right answer! Always ensure that your password is at least 8 characters long, with a mix of symbols, lower and capital letters and includes numbers.	Incorrect Answer Text: Wrong answer! Always ensure that your password is at least 8 characters long, with a mix of symbols, lower and capital letters and includes numbers.

Question 4: Which of the following contributes to unsafe online shopping?	
Answer A:	Saving of payment information in web browsers
Answer B:	Using a well-known online merchant
Answer C:	Making use of 3-D secure payment
Answer D:	Looking for closed padlock symbol
Correct Answer Text: Right answer! Never save payment information in your web browser as it may be used if someone gets a hold of your device or can be obtained via malicious software.	Incorrect Answer Text: Wrong answer! Some sites (as well as all browsers) offer to "remember" your payment information (e.g. password) for your convenience upon subsequent purchases. Never accept to have your "financial information" stored on any website/web browser.

ONLINE SHOPPING

Question 5: Which method of accessing online shopping is the most secure?	
Answer A:	Virtual Private Network (VPN)
Answer B:	Home Wi-Fi
Answer C:	Mobile service provider
Answer D:	Free Wi-Fi access point
Correct Answer Text: Right answer! A VPN is the most secure method of accessing online shopping. Mobile service providers can be considered second most secure, followed by home Wi-Fi. Never use public Wi-Fi to conduct online shopping as it may have been tampered with.	Incorrect Answer Text: Wrong answer! A VPN is considered the most secure method of accessing online shopping. Mobile service providers can be considered second most secure, followed by home Wi-Fi. Never use public Wi-Fi to conduct online shopping as it may have been tampered with.

Question 6: If you suspect online fraud or you have lost your credit card, do you have your financial institution's contact details saved on your mobile phone?	
Answer A:	Yes
Answer B:	No
Correct Answer Text: Right answer! Ensure that you save your financial institution's contact details in case of emergency.	Incorrect Answer Text: Wrong answer! Ensure that you save your financial institution's contact details in case of emergency.

MOBILE BANKING

Question 1: What is the easiest way to protect your personal information stored on your mobile device?	
Answer A:	Password protect your device
Answer B:	Third-party malware protection
Answer C:	Store information on an SD card or cloud
Answer D:	Install an anti-virus application
<p>Correct Answer Text: Right answer! Using a password or fingerprint is the easiest method of protecting your device. However, encrypting information is seen as the most secure method.</p>	<p>Incorrect Answer Text: Wrong answer! Using a password or fingerprint is the easiest method and should always be used. However, encrypting information is seen as the most secure method.</p>

Question 2: If you "click" on an unknown link in a text message. What might happen?	
Answer A:	Your mobile device could be infected with ransomware
Answer B:	Your mobile device could be infected with malware
Answer C:	You could accidentally download a virus
Answer D:	All three of these could happen
<p>Correct Answer Text: Right answer! Unknown links in messages can lead to your mobile device being infected and/or hacked. For example, your mobile banking app might be hijacked by fraudsters.</p>	<p>Incorrect Answer Text: Wrong answer! Your selection is possible. However, depending on the situation any of the choices could occur. It is best to avoid clicking on any links. Unknown links in messages can lead to your mobile device being infected and/or hacked. For example, your mobile banking app might be hijacked by fraudsters.</p>

MOBILE BANKING

Question 3: How often should you update your mobile banking application?	
Answer A:	When you have a chance to
Answer B:	As soon as an update is available
Answer C:	Never. Updates cost data
Answer D:	After friends try it first
Correct Answer Text: Right answer! Application updates are critical and should be done as soon as possible. Remember, they are designed to fix any potential problems.	Incorrect Answer Text: Wrong answer! Application updates are critical and should be done as soon as possible. Remember, they are designed to fix potential problems.

Question 4: Your mobile device starts acting strangely. Apps open by themselves and the device reboots. What might be occurring?	
Answer A:	Your mobile device's battery is low
Answer B:	Your mobile device is conducting an update
Answer C:	Your mobile device's storage is full
Answer D:	Someone might be attempting to do a SIM-swap
Correct Answer Text: Right answer! If you suspect someone is attempting to do a SIM-swap, contact your financial institution and mobile service provider immediately.	Incorrect Answer Text: Wrong answer! A criminal may be attempting to perform a SIM-swap. If you suspect someone is attempting to do a SIM-swap, contact your financial institution and mobile service provider immediately.

MOBILE BANKING

Question 5: If you ever lose or suspect your mobile device has been stolen, what should you first do?	
Answer A:	Use a preinstalled app to track your mobile device
Answer B:	Attempt to dial it
Answer C:	Call your service provider and report it stolen
Answer D:	Contact your insurance provider and inform them it has been stolen
Correct Answer Text: Right answer! Informing your mobile service provider of your mobile device being stolen will allow them to block the device and prevent any further use of it.	Incorrect Answer Text: Wrong answer! Informing mobile service provider should be your priority as they will disable the device and block its usage

Question 6: What do financial institutions provide free of charge to assist in keeping your mobile device secure?	
Answer A:	VPN
Answer B:	Anti-virus application
Answer C:	Airtime
Answer D:	Music
Correct Answer Text: Right answer! Install an up-to-date anti-virus application on your mobile device. Most financial institutions provide this to their customers free of charge.	Incorrect Answer Text: Wrong answer! Install an up-to-date anti-virus application on your mobile device. Most financial institutions provide this to their customers free of charge.

CARD FRAUD

Question 1: Which of the following is an example of a strong pin?	
Answer A:	My birthdate
Answer B:	12345
Answer C:	0000
Answer D:	4987
Correct Answer Text: Right answer! Always create a random PIN number that cannot be guessed easily and never share your PIN with anyone.	Incorrect Answer Text: Wrong answer! Always create a random PIN number that cannot be guessed easily and never share your PIN with anyone.

Question 2: Which of the following indicates that you may be a target of card fraud?	
Answer A:	The area around the ATM you are using is quiet
Answer B:	A stranger offers to assist you at the ATM
Answer C:	The ATM is out of order
Answer D:	There is a security guard on duty at the ATM
Correct Answer Text: Right answer! Be cautious of strangers offering to help at the ATM as they could be trying to distract you in order to get hold of your card or your PIN.	Incorrect Answer Text: Wrong answer! Be cautious of strangers offering to help at the ATM as they could be trying to distract you in order to get hold of your card or your PIN. Also, ensure that you feel safe. If something bothers you, rather use another ATM

CARD FRAUD

Question 3: Which of the following assists in protecting your PIN when swiping your card at shops or using ATM's?	
Answer A:	Entering your PIN as normal
Answer B:	Covering the keypad while entering your PIN
Answer C:	Entering your bank card PIN as quickly as you can
Answer D:	Turning the card machine away from the cashier
Correct Answer Text: Right answer! When withdrawing cash or swiping your card in-store, always ensure that you cover the hand typing your PIN number to prevent criminals from seeing your PIN number.	Incorrect Answer Text: Wrong answer! When withdrawing cash or swiping your card in-store, always ensure that you cover the hand typing your PIN number to prevent criminals from seeing your PIN number.

Question 4: What can be considered as credit card fraud?	
Answer A:	Unauthorized usage of credit cards
Answer B:	Online purchases conducted by myself
Answer C:	An authorized debit order
Answer D:	None of the options
Correct Answer Text: Right answer! If you suspect unauthorized usage of your credit card, immediately report it to your financial institution.	Incorrect Answer Text: Wrong answer! Always ensure that you are in control of your card usage. If you suspect unauthorized usage of your credit card, immediately report it to your financial institution.

CARD FRAUD

Question 5: What should you do if someone calls you, claiming to be from your banking institution, and asks to provide your banking card details over the phone?	
Answer A:	Give it to them. What's the big deal?
Answer B:	Ask to speak to a supervisor or person in charge
Answer C:	Hang up and ignore the call
Answer D:	After complying with instructions find the phone number of the claimed institution and verify the request
Correct Answer Text: Right answer! Financial institutions will never ask you to provide details over the phone or via email.	Incorrect Answer Text: Wrong answer! Someone maybe attempting to steal your bank card information. Financial institutions will never ask you to provide details over the phone or via email.

Question 6: If you suspect card fraud or you have lost your credit card, do you have your financial institution's contact details saved on your mobile phone in order to report the matter?	
Answer A:	Yes
Answer B:	No
Correct Answer Text: Right answer! Ensure that you save your financial institution's contact details on your phone, ready to use in case of emergency.	Incorrect Answer Text: Wrong answer! Ensure that you save your financial institution's contact details on your phone, ready to use in case of emergency. The sooner you report a suspected crime or stolen card, the better.

MALWARE

Question 1: When inserting a flash or hard drive into your computer, what action should be done first?	
Answer A:	Formatting the flash drive or hard drive
Answer B:	Accessing the files on the flash drive or hard drive
Answer C:	Scanning the flash or hard drive with an anti-virus program
Answer D:	No action should be taken
Correct Answer Text: Right answer! It is recommended to always scan a flash or hard drive with an up-to-date anti-virus program to prevent your computer being infected.	Incorrect Answer Text: Wrong answer! It is recommended to always scan a flash or hard drive with an up-to-date anti-virus program to prevent your computer being infected.

Question 2: If you receive an email from unknown or suspicious origins, what action should be taken?	
Answer A:	Respond to the email appropriately
Answer B:	Ignore the email, but check the attachment for further details
Answer C:	Delete the email
Answer D:	Download the attachment to your computer
Correct Answer Text: Right answer! Never open emails from unknown or suspicious origins. Cyber-criminals use attachments which could be disguised as, for example, tax refunds, package deliveries and invoices to install malware on your device.	Incorrect Answer Text: Wrong answer! Never open emails from unknown or suspicious origins. Cyber-criminals use attachments which could be disguised as, for example, tax refunds, package deliveries and invoices to install malware on your device. It would be best to delete the email as it will prevent you from opening it accidentally.

MALWARE

Question 3: Computers have many built-in security features. Which of the following security features should always be activated?	
Answer A:	Microsoft Office
Answer B:	Firewall
Answer C:	Internet browser
Answer D:	Windows Explorer
Correct Answer Text: Right answer! Make sure that your firewall is active and set to maximum security and use a strong network password to prevent cyber-criminals from accessing your devices.	Incorrect Answer Text: Wrong answer! A firewall is a network security device that monitors incoming and outgoing network traffic. Firewalls are the first line of defence. They establish a barrier between you and untrusted outside networks, such as the internet.

Question 4: Which of the following are good cyber security habits?	
Answer A:	Setting your anti-virus to automatically scan your computer
Answer B:	Conducting manual anti-virus scans
Answer C:	Ensuring your computer is public and visible on your network
Answer D:	Ignoring notifications and alerts
Correct Answer Text: Right answer! Set your computer or mobile device to run regular virus scans automatically and ensure that your operating system is updated with the most recent security patches.	Incorrect Answer Text: Wrong answer! Setting your anti-virus to scan automatically at least once a day is recommended as it will ensure that a virus scan is always conducted, regardless if it's necessary or not. Better to be safe than sorry.

MALWARE

Question 5: Which option below is a sign that suggests the email you received from your bank is possibly forged and an attempt at phishing?	
Answer A:	URL of the bank provided in the email is a perfect match to authenticated emails previously received
Answer B:	The email contains spelling and grammar mistakes
Answer C:	The email asks you to visit your nearest branch to complete a form
Answer D:	The domain name of the email sender corresponds to the bank name. (e.g. AHZ bank: ...@AHZ.com)
<p>Correct Answer Text: Right answer! Banks typically ensure that any emails sent are free from errors, such as spelling mistakes. If you notice any spelling or grammar errors, it is best to contact your bank and confirm whether they did indeed send the email.</p>	<p>Incorrect Answer Text: Wrong answer! Banks typically ensure that any emails sent are free from errors such as spelling mistakes. If you notice any spelling or grammar errors, it is best to contact your bank and confirm whether they did indeed send the email.</p>

Question 6: Which of the following is most likely to make your computer stop functioning correctly?	
Answer A:	Trojan
Answer B:	Worm
Answer C:	Virus
Answer D:	Spyware
<p>Correct Answer Text: Right answer! Viruses are usually created by hackers who just want to influence as many computers as possible. It is recommended to run anti-virus scans regularly or even better is setting your anti-virus program to scan your computer automatically.</p>	<p>Incorrect Answer Text: Wrong answer! Trojans, worms and spyware all depend on your computer functioning correctly. They use your computer's resources to complete whatever their designer intended, such as sending emails, stealing information from your computer, etc.</p>

COMPUTER HYGIENE

Question 1: Which of the following is an example of a strong password?	
Answer A:	12345
Answer B:	john1993
Answer C:	ABC123
Answer D:	A3\$6x3
Correct Answer Text: Right answer! Always ensure that your password is at least 8 characters long, with a mixture of lower and capital letters, numbers and special characters.	Incorrect Answer Text: Wrong answer! Always ensure that your password is at least 8 characters long, with a mixture of lower and capital letters, numbers and special characters.

Question 2: Which of the following devices is the most unsafe to use for internet banking?	
Answer A:	Public Computer
Answer B:	Private Mobile Device
Answer C:	Home Computer
Answer D:	Office Computer
Correct Answer Text: Right answer! Do not conduct internet banking from public computers. Malicious software can capture your login details and give cyber-criminals access to your bank account.	Incorrect Answer Text: Wrong answer! Do not conduct internet banking from public computers. Malicious software can capture your login details and give cyber-criminals access to your bank account.

COMPUTER HYGIENE

Question 3: You receive an email from your bank asking you to complete an online form. You notice in the email address your bank's name is spelt incorrectly. What cyber-attack maybe occurring?	
Answer A:	Phishing Attack
Answer B:	E-mail Hacking
Answer C:	Cross-site Scripting
Answer D:	None
<p>Correct Answer Text: Right answer! Phishing is the fraudulent practice of sending emails pretending to be from a reputable company to trick you into revealing personal information, such as passwords and credit card numbers.</p>	<p>Incorrect Answer Text: Wrong answer! Phishing is the fraudulent practice of sending emails pretending to be from a reputable company to trick you into revealing personal information, such as passwords and credit card numbers.</p>

Question 4: How often should you update your anti-virus application?	
Answer A:	When you have a chance to
Answer B:	As soon as an update is available
Answer C:	Never. Updates use costly data
Answer D:	After friends tried it first
<p>Correct Answer Text: Right answer! Anti-virus application updates are critical and should be done as soon as possible. Remember, they are designed to ensure your anti-virus can detect new threats.</p>	<p>Incorrect Answer Text: Wrong answer! Anti-virus application updates are critical and should be done as soon as possible. Remember, they are designed to ensure your anti-virus can detect new threats.</p>

COMPUTER HYGIENE

Question 5: The main aim of good computer hygiene is to?	
Answer A:	Think reactively about security
Answer B:	Protect our physical security
Answer C:	Ensure safe and secure Facebook usage
Answer D:	Train ourselves to think proactively about our cyber security
Correct Answer Text: Right answer! Good computer hygiene is about being proactive and preventing any incidents from occurring in the first place.	Incorrect Answer Text: Wrong answer! The main aim of good computer hygiene is to be proactive and prevent any incidents from occurring in the first place. Possible good computer hygiene tips include; having an up-to-date anti-virus application installed.

Question 6: Online fraud is one of the most widespread forms of cybercrime. In case you suspect you have been affected by online fraud, do you have your bank’s contact details readily available?	
Answer A:	Yes
Answer B:	No
Correct Answer Text: Right answer! As more and more people use their computers for banking and online shopping, they become more attractive to cyber criminals, who use email messages, website and social networks to get access to your personal information. It is best to have your bank’s contact details at hand in case you are defrauded and need to report it.	Incorrect Answer Text: Wrong answer! As more and more people use their computers for banking and online shopping, they become more attractive to cyber criminals, who use email messages, website and social networks to get access to your personal information. It is best to have your banks contact details at hand in case you are defrauded and need to report.

Appendix C

Results

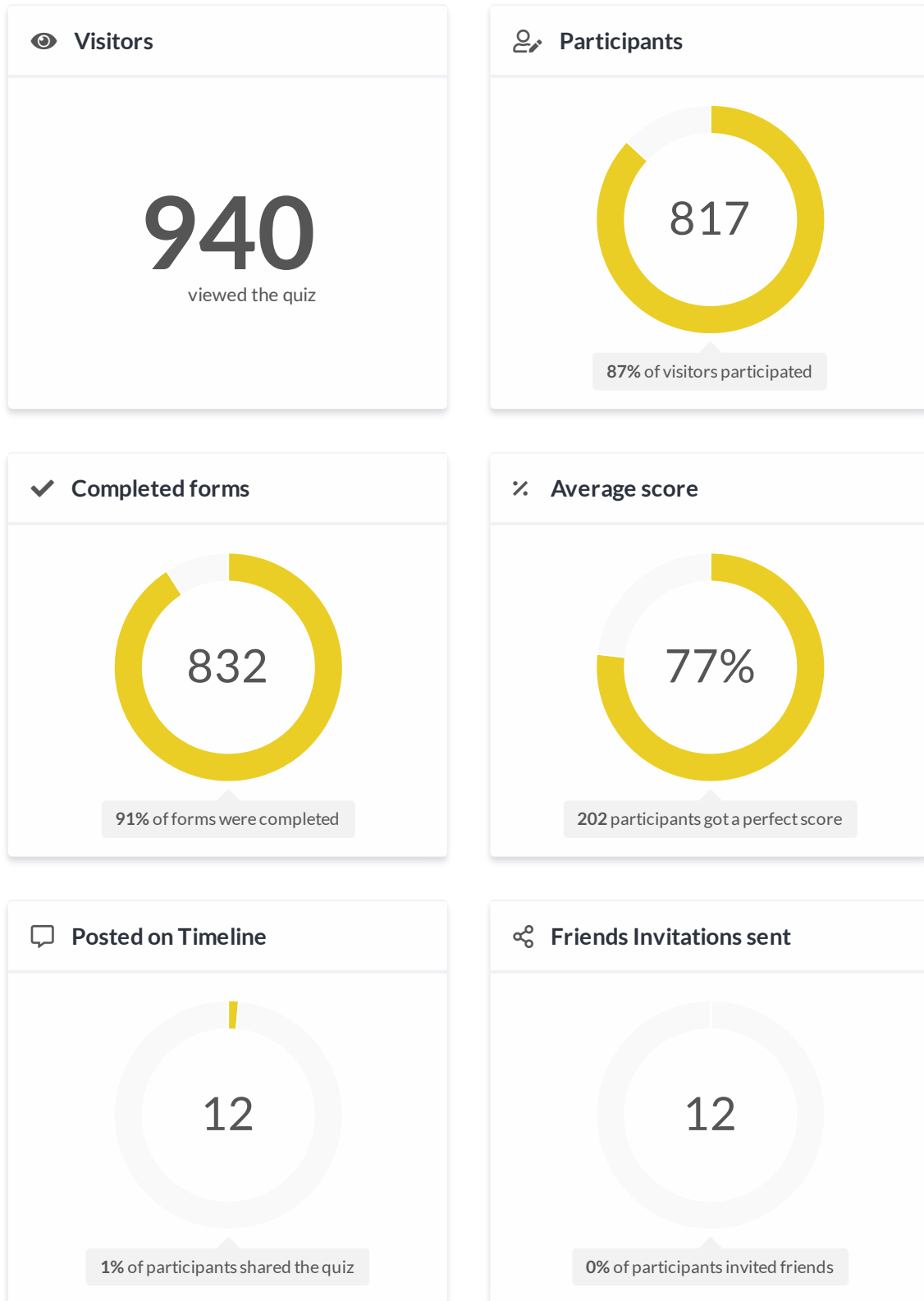
Appendix C includes all results and statistics from the research instrument used in this study:

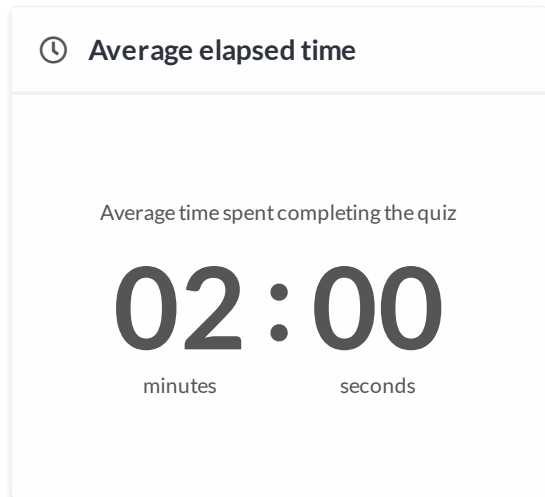
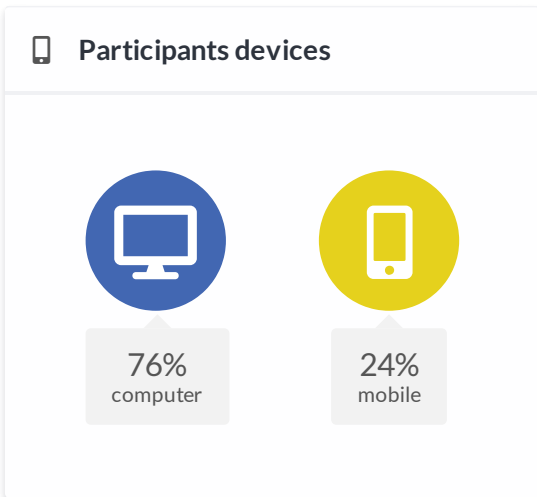
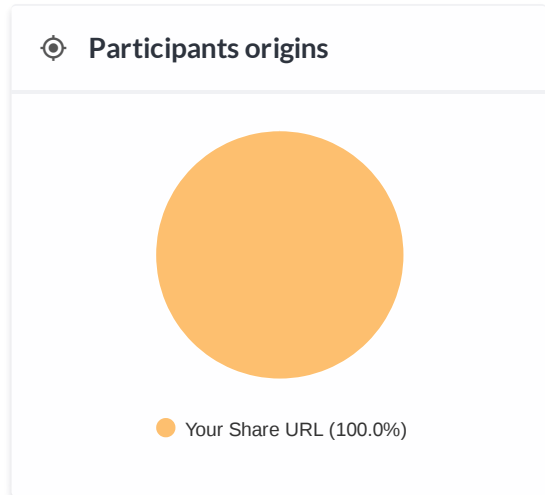
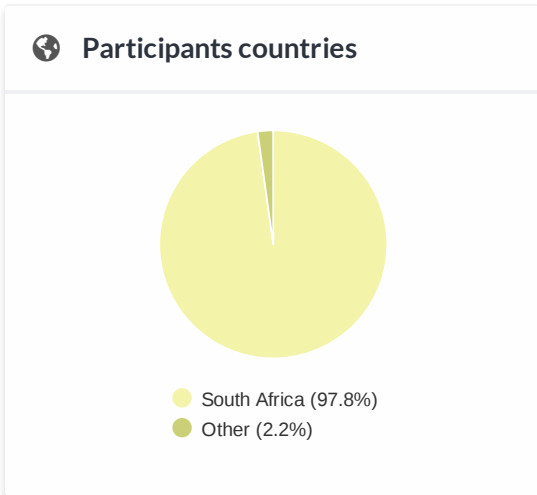
1. Online Shopping Cyber Security Quiz Results and Video Statistics
2. Mobile Banking Cyber Security Quiz Results and Video Statistics
3. Card Fraud Cyber Security Quiz Results and Video Statistics
4. Malware Cyber Security Quiz Results and Video Statistics
5. Computer Hygiene Cyber Security Quiz Results and Video Statistics

C.1 Online Shopping Cyber Security Quiz Results and Video Statistics

Online Shopping

Created on December 01, 2017 by Rahul Maharaj



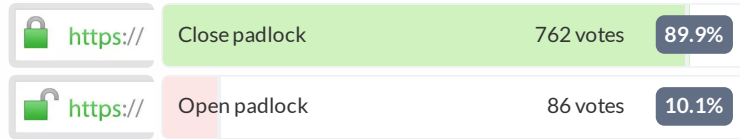


Online Shopping

Created on December 01, 2017 by Rahul Maharaj

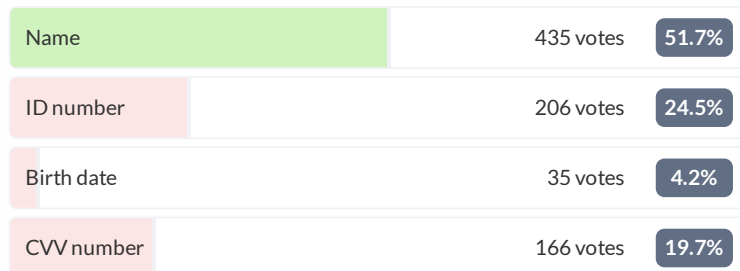
Which of the following provides an indication that you are communicating securely with a website?

848 answers



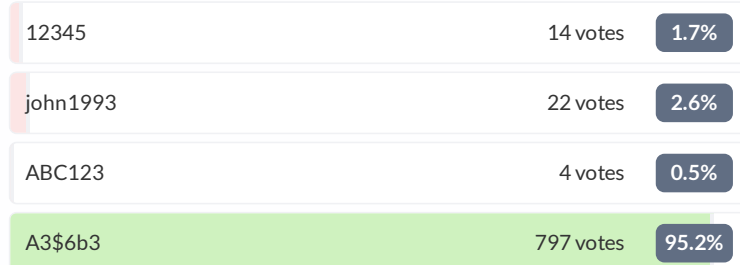
Which of the following personal details should be given to an online merchant when requested during registration?

842 answers



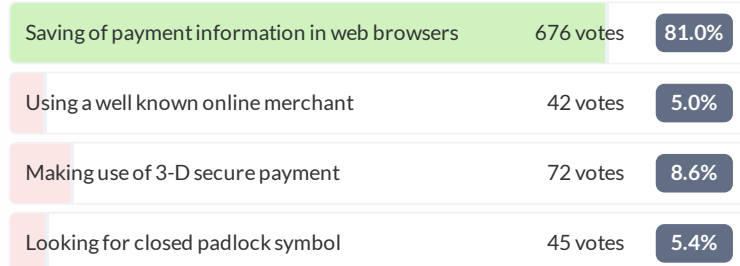
Which of the following is an example of a strong password?

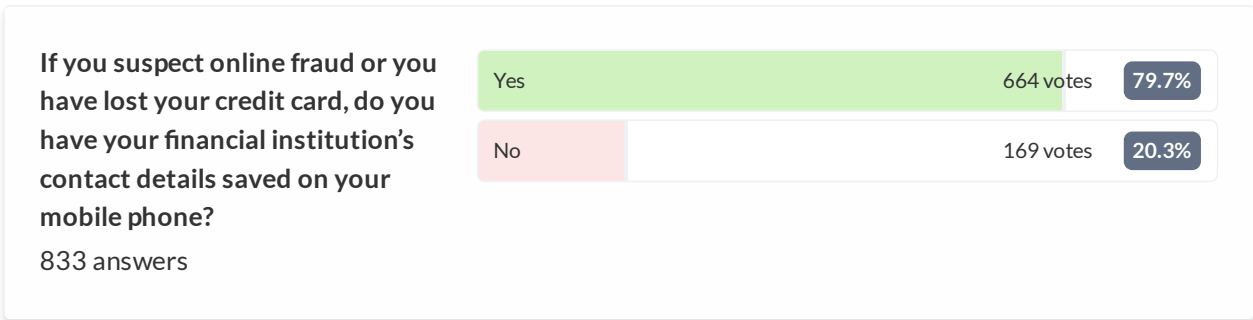
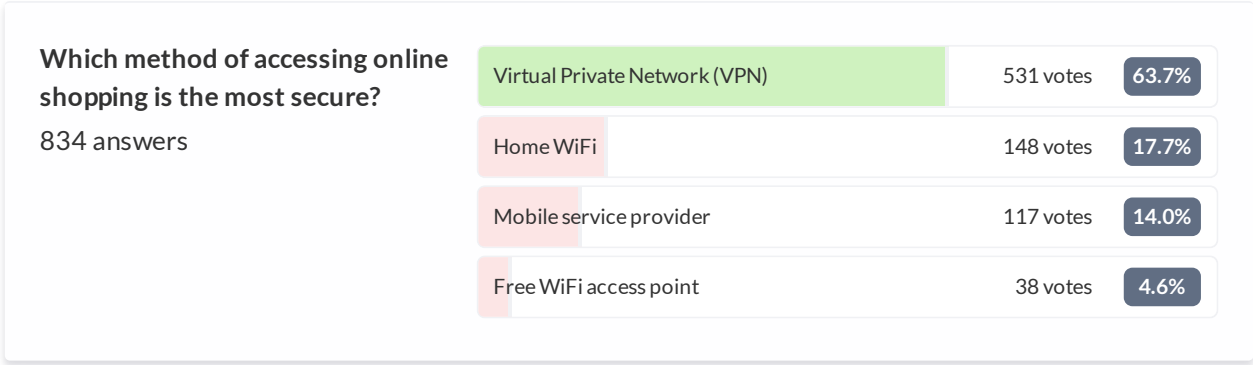
837 answers



Which of the following contributes to unsafe online shopping?

835 answers





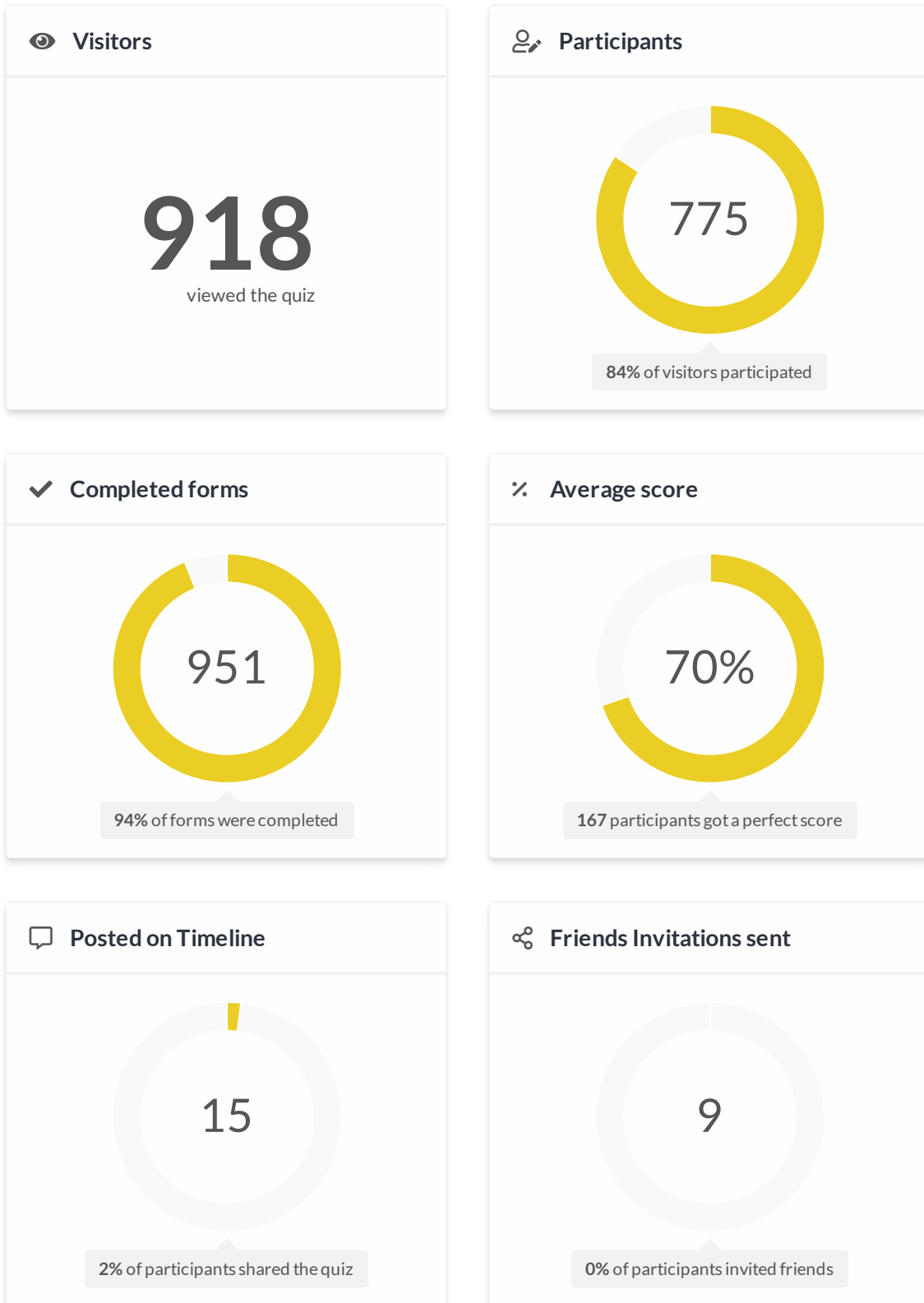


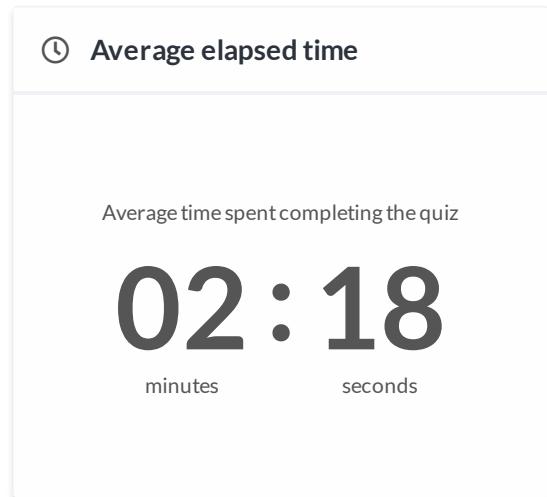
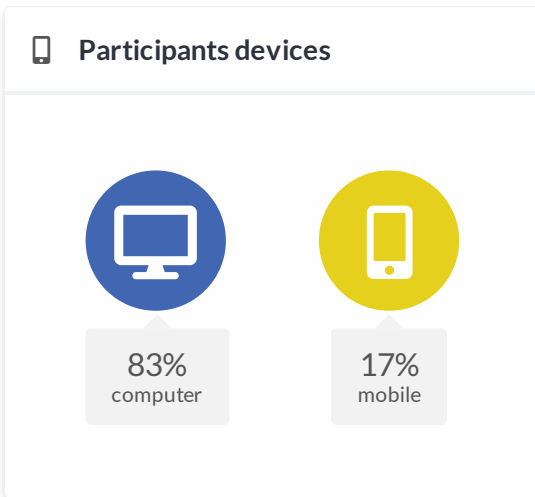
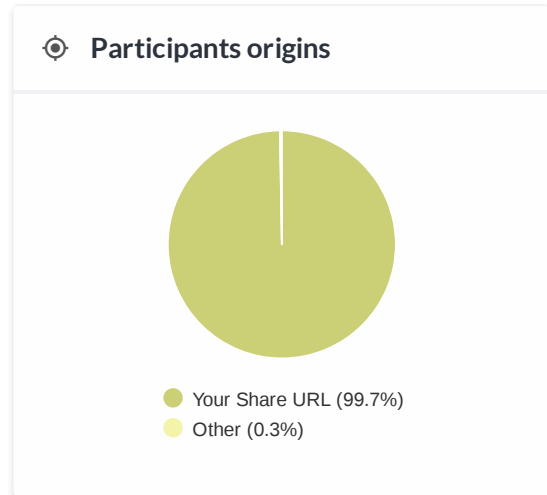
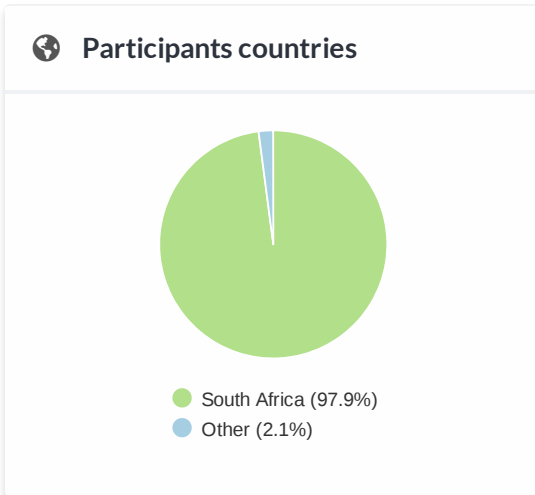
Sabric Survey Online Shopping (Lifetime)	
Title	Analytic
Watch Time	37,057 (minutes)
Average View Duration	0:58
Views	38,141
Impressions	92,279
Average % Viewed	92%
Highest watch time by device	Computer - 67%
Male	60%
Female	40%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

C.2 Mobile Banking Cyber Security Quiz Results and Video Statistics

Mobile Banking

Created on February 12, 2018 by Rahul Maharaj





Mobile Banking

Created on February 12, 2018 by Rahul Maharaj

What is the easiest way to protect your personal information stored on your mobile device?

967 answers

Password protect your device	719 votes	74.4%
Third-party malware protection	59 votes	6.1%
Store information on an SD card or cloud	89 votes	9.2%
Install an anti-virus application	100 votes	10.3%

If you "click" on an unknown link in a text message. What might happen?

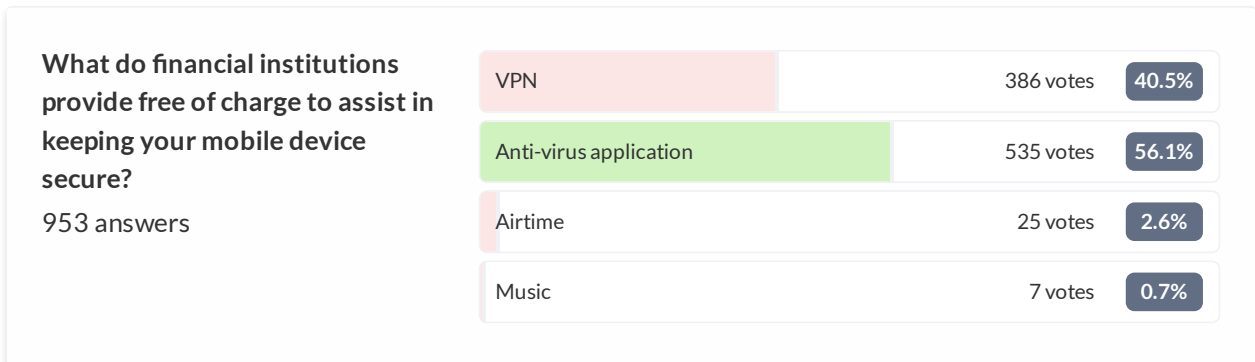
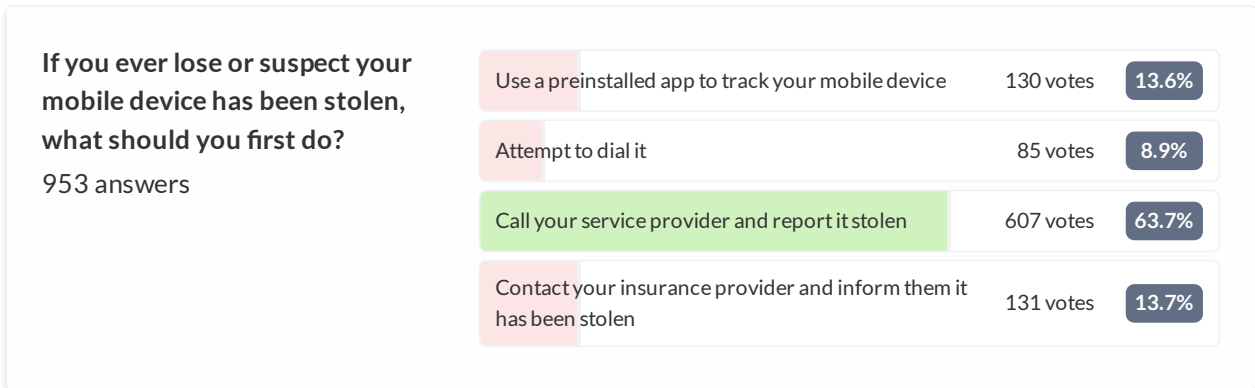
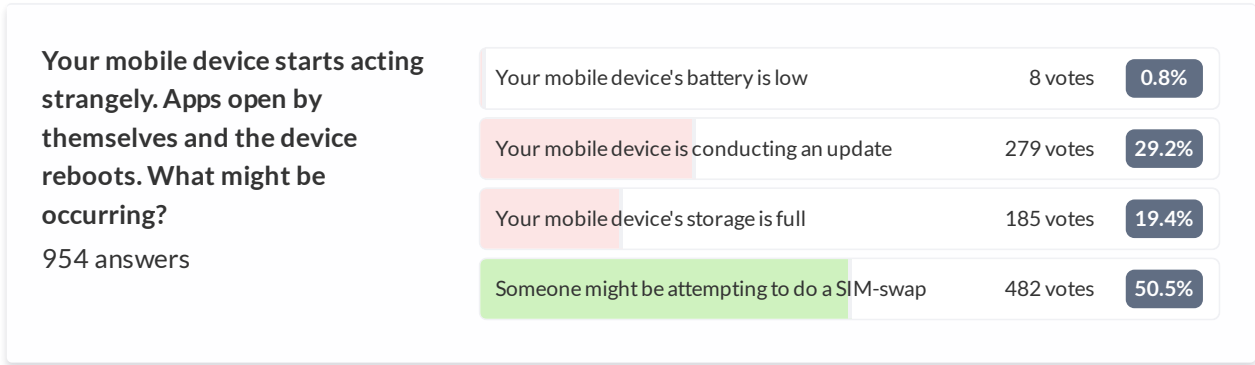
958 answers

Your mobile device could be infected with ransomware	24 votes	2.5%
Your mobile device could be infected with malware	44 votes	4.6%
You could accidentally download a virus	146 votes	15.2%
All three of these could happen	744 votes	77.7%

How often should you update your mobile banking application?

956 answers

When you have a chance to	27 votes	2.8%
As soon as an update is available	910 votes	95.2%
Never. Updates cost data	15 votes	1.6%
After friends try it first	4 votes	0.4%



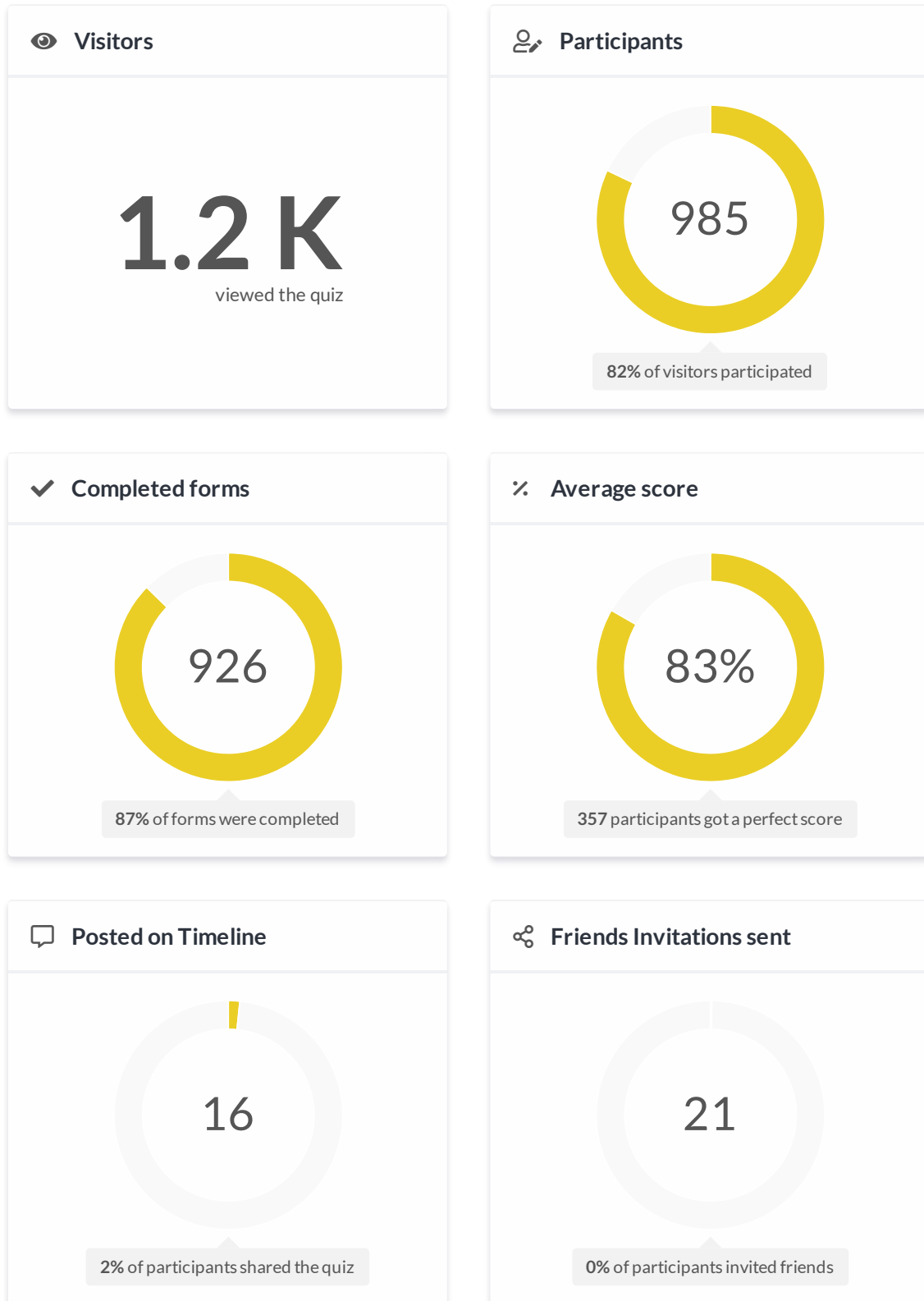


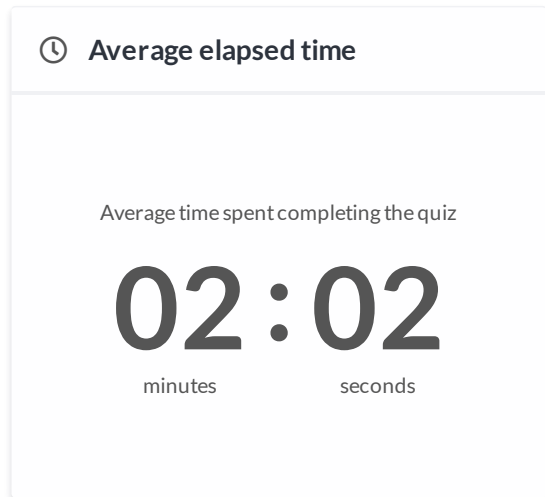
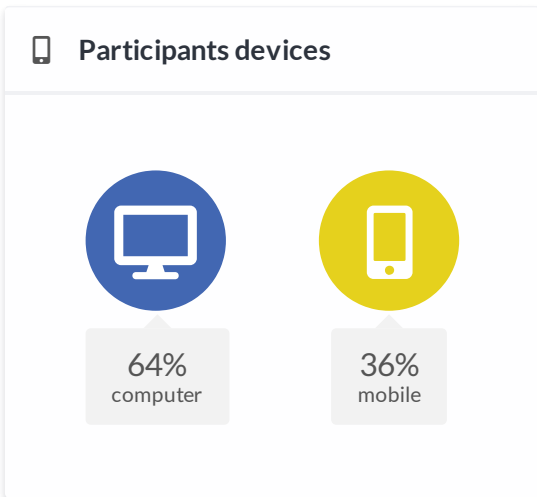
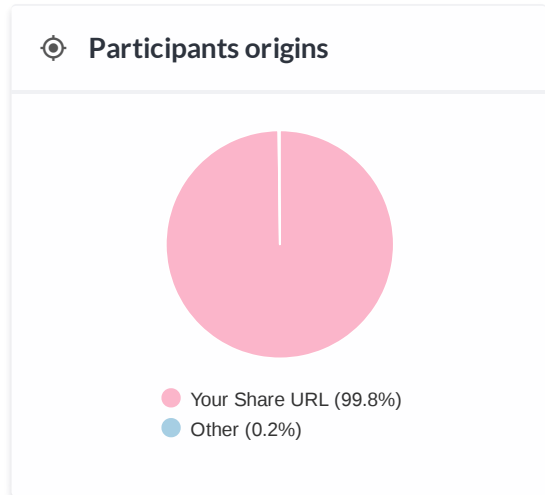
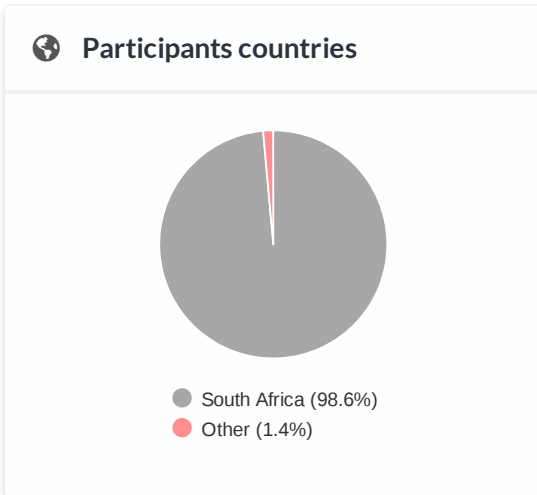
Sabric Survey Mobile Banking (Lifetime)	
Title	Analytic
Watch Time	43,311 (minutes)
Average View Duration	1:02
Views	41,616
Impressions	91,994
Average % Viewed	91%
Highest watch time by device	Computer - 66%
Male	58%
Female	42%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

C.3 Card Fraud Cyber Security Quiz Results and Video Statistics

Card Fraud

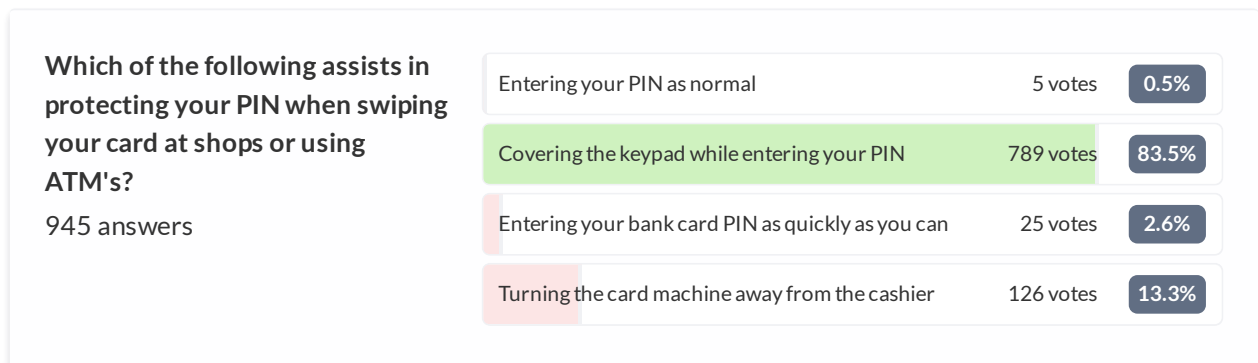
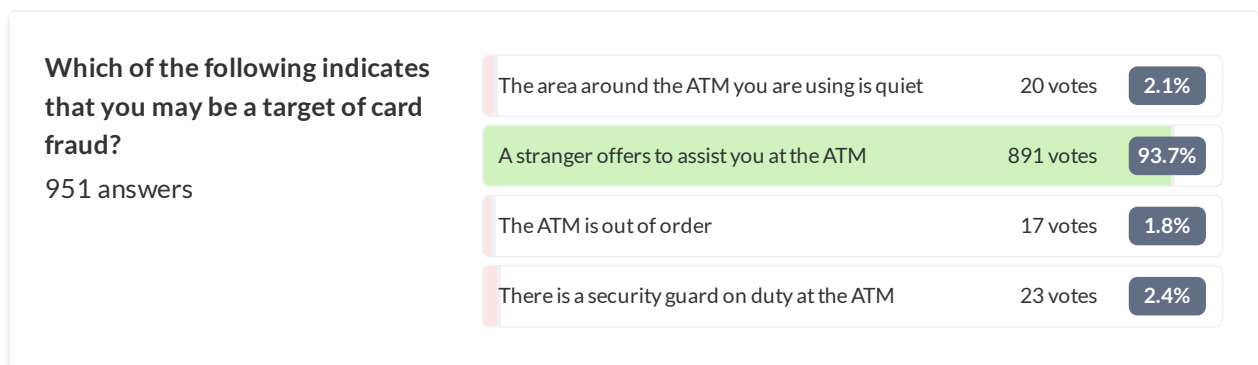
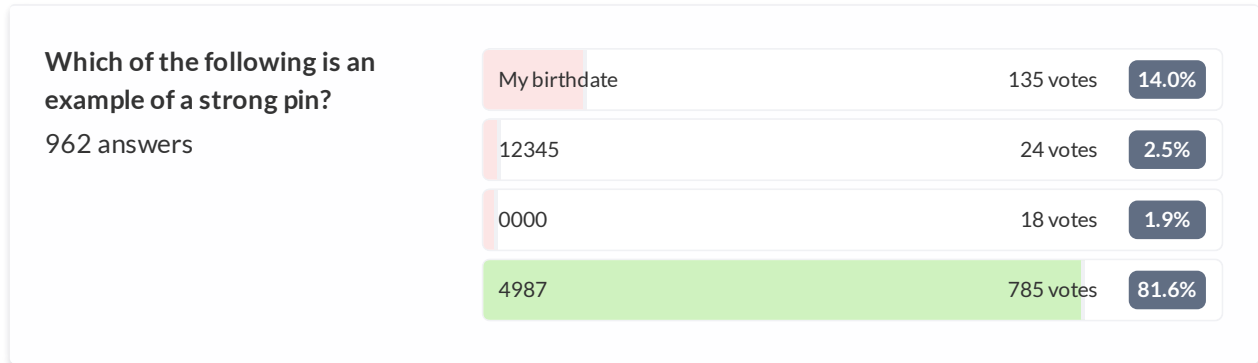
Created on March 16, 2018 by Rahul Maharaj

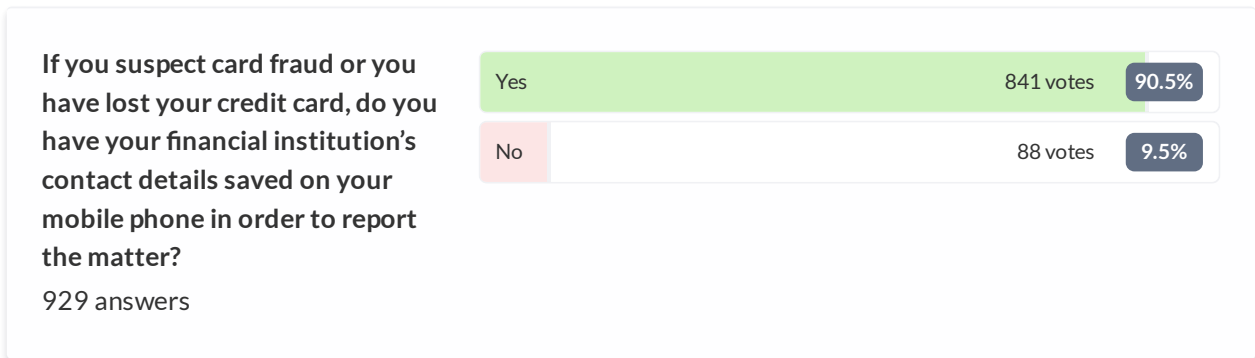
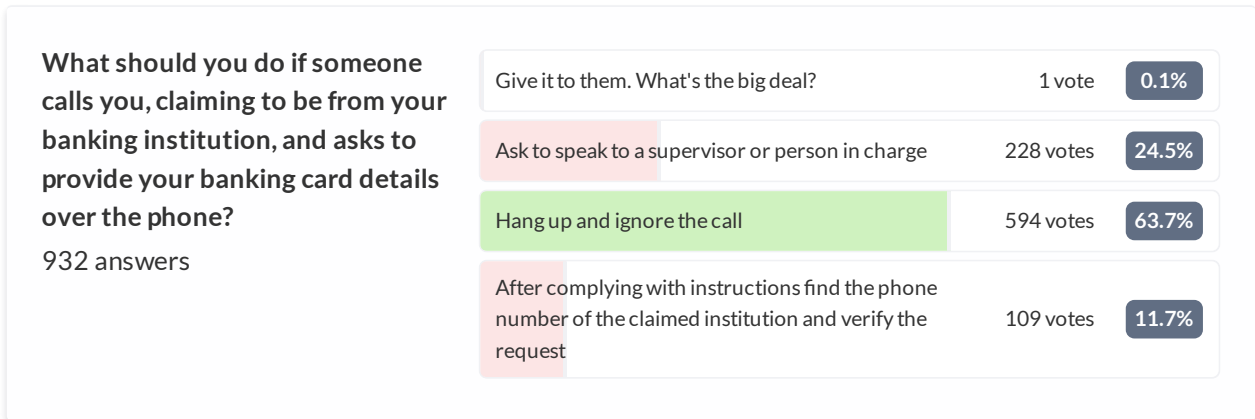
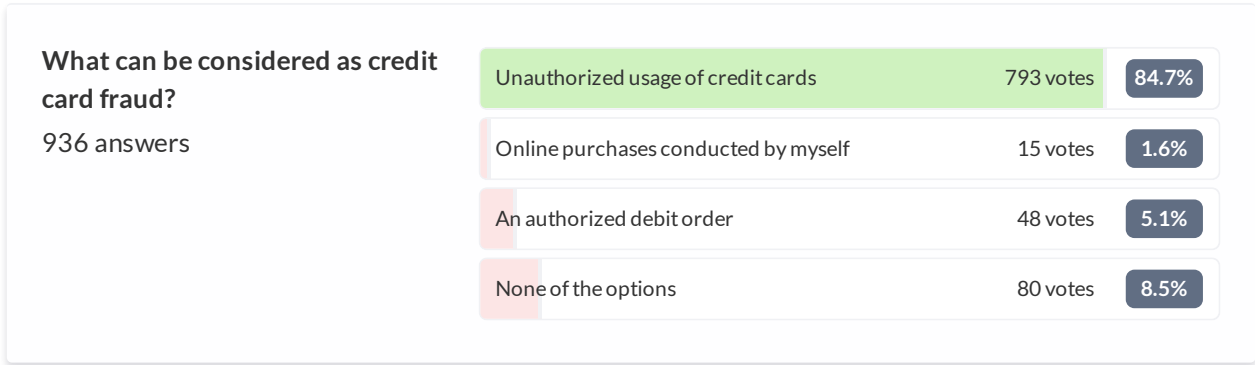




Card Fraud

Created on March 16, 2018 by Rahul Maharaj





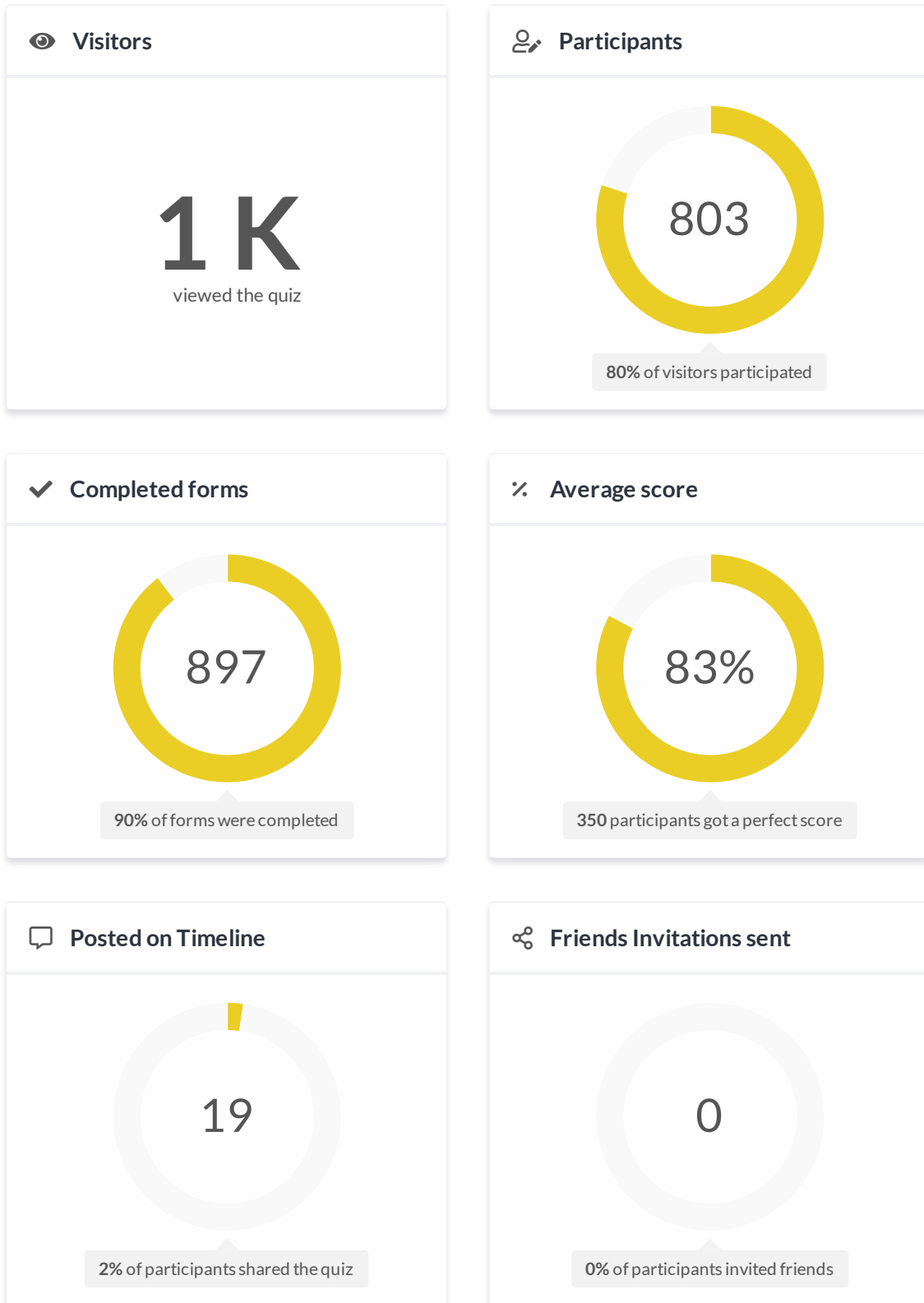


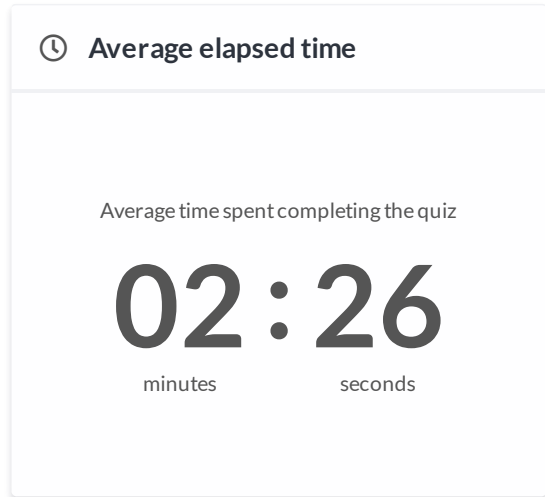
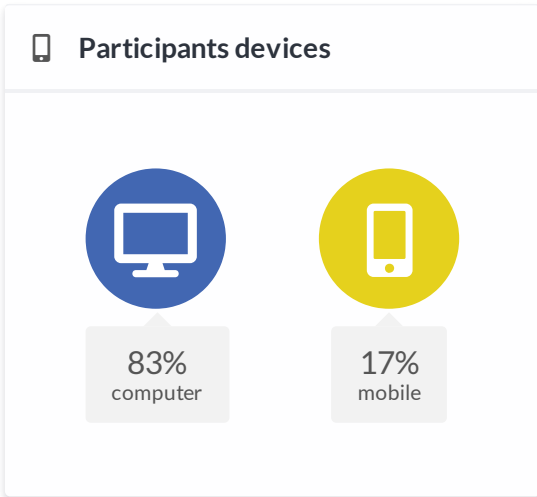
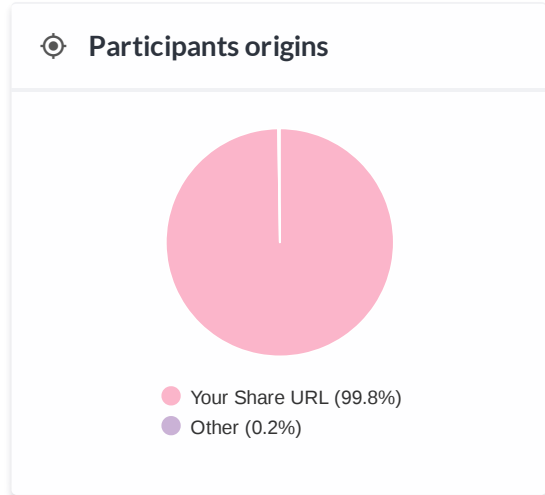
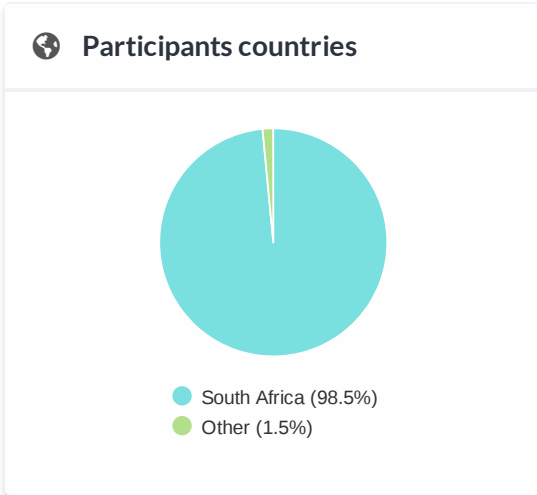
Sabric Survey Card Fraud (Lifetime)	
Title	Analytic
Watch Time	63,736 (minutes)
Average View Duration	0:51
Views	74,414
Impressions	260,786
Average % Viewed	92%
Highest watch time by device	Computer - 61%
Male	56%
Female	44%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

C.4 Malware Cyber Security Quiz Results and Video Statistics

Malware

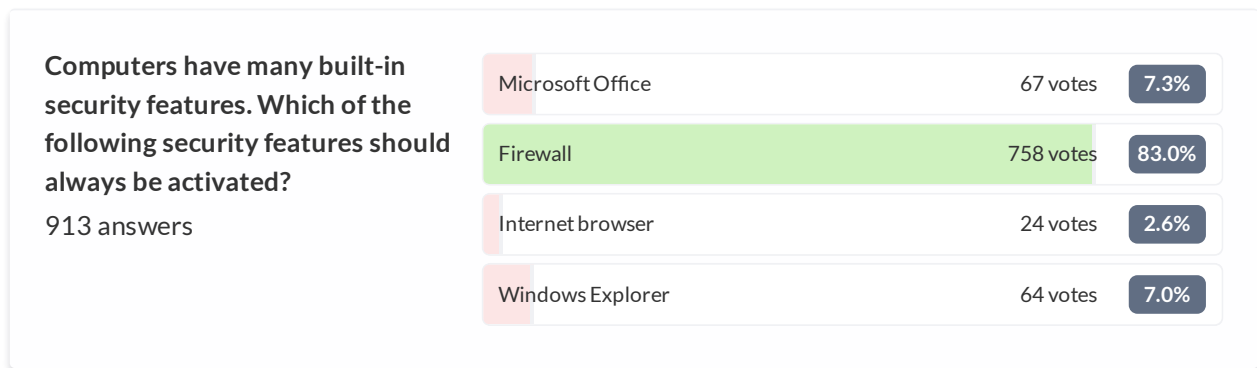
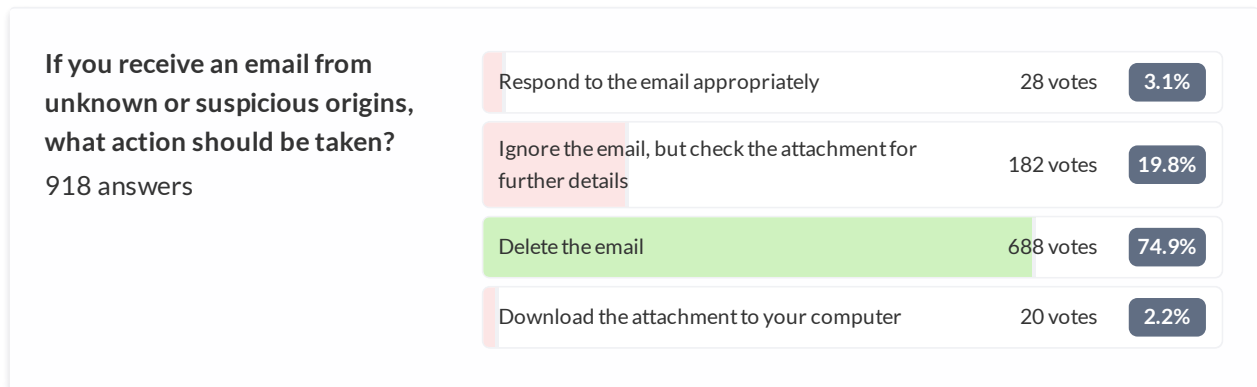
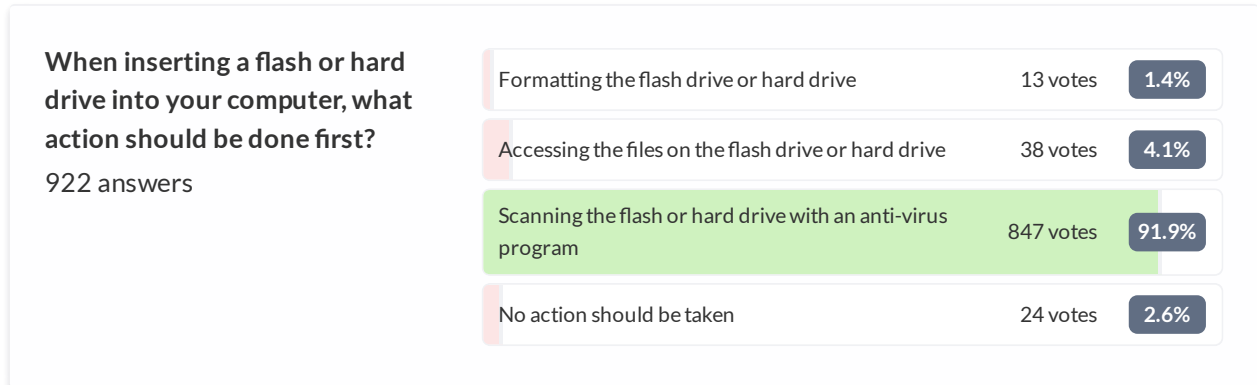
Created on February 21, 2018 by Rahul Maharaj

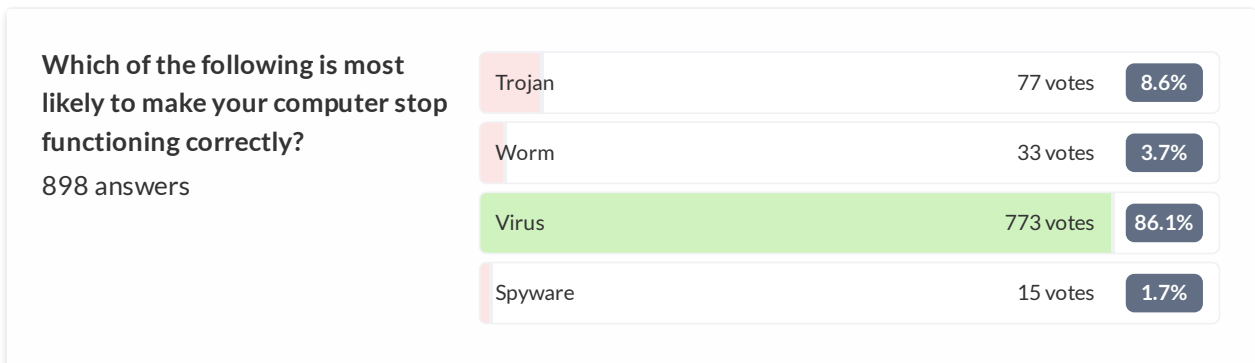
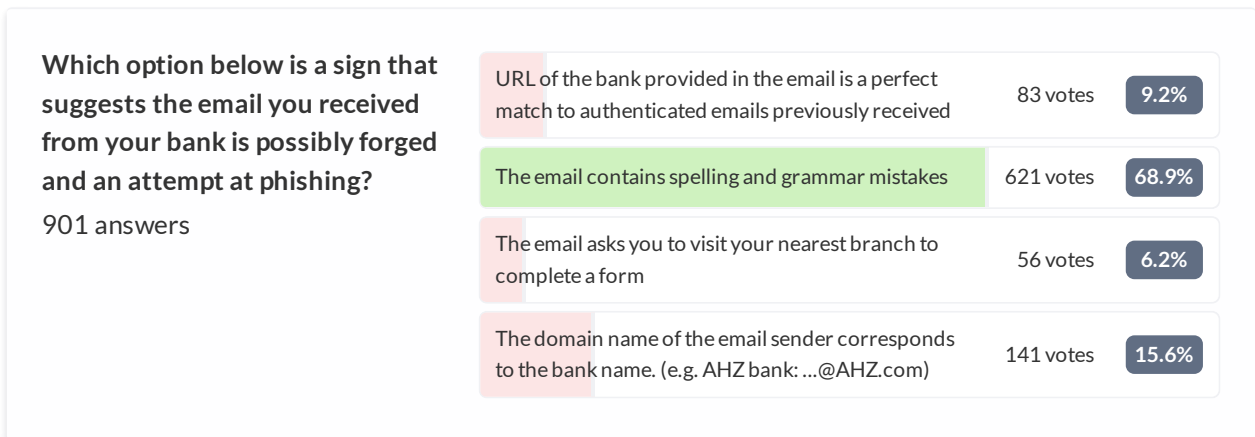
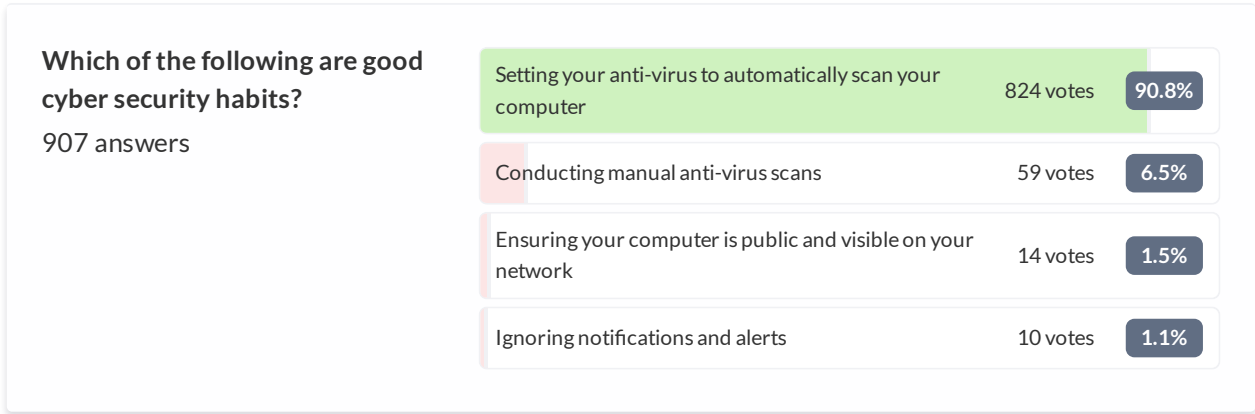




Malware

Created on February 21, 2018 by Rahul Maharaj





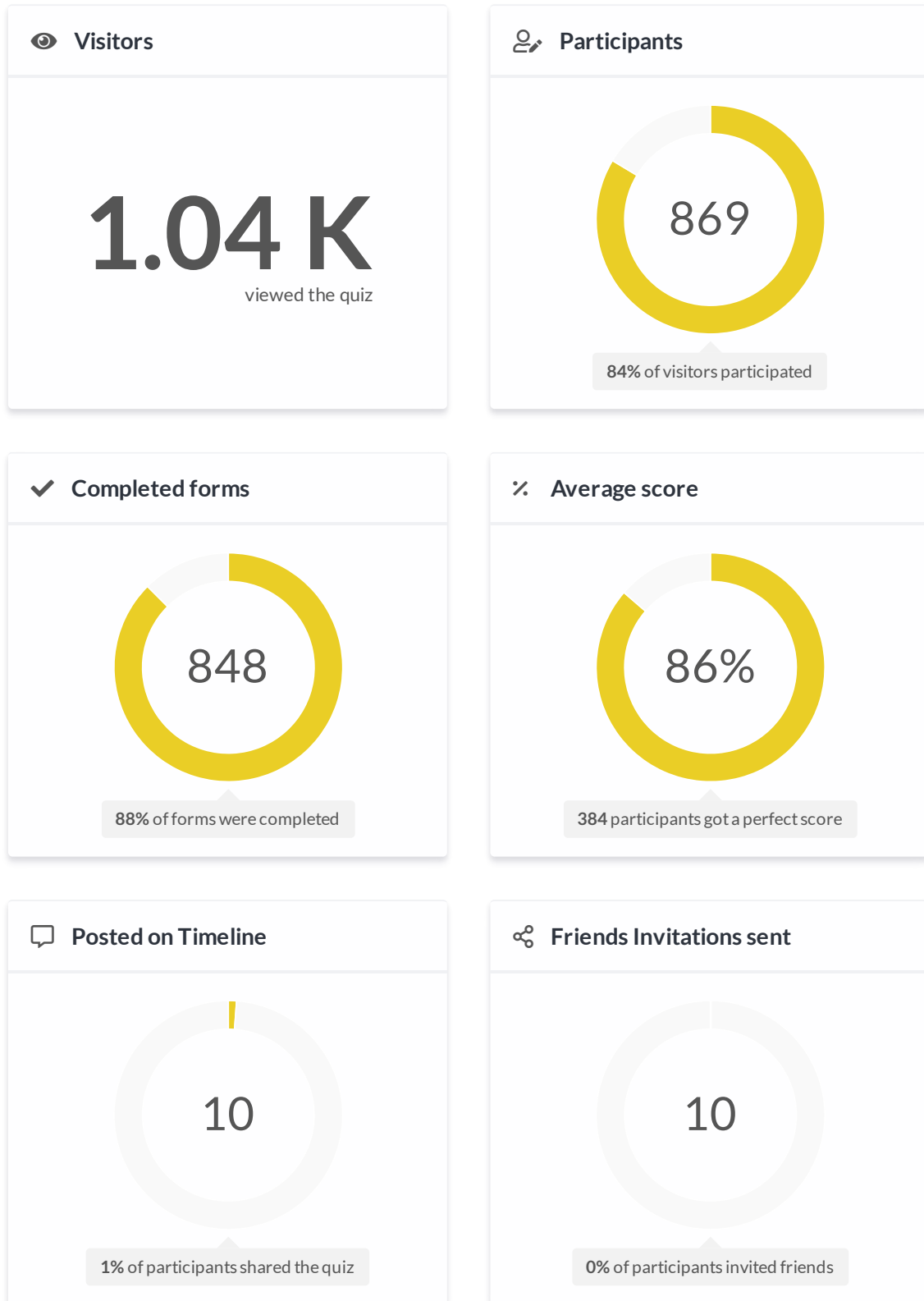


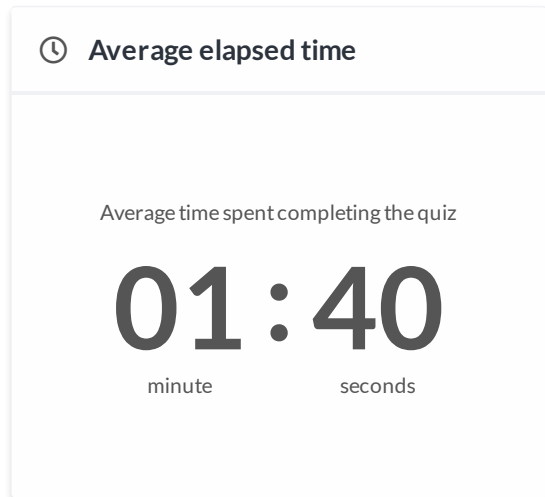
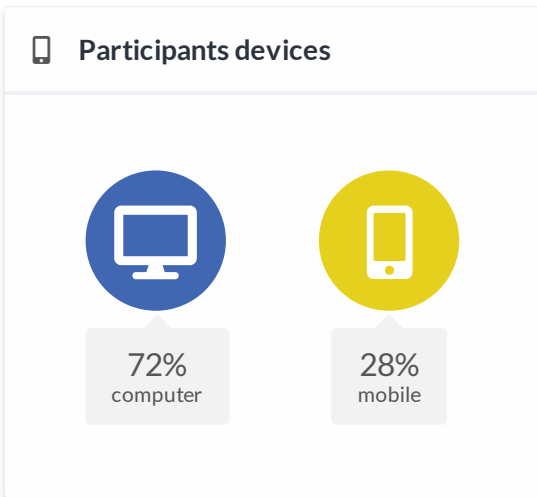
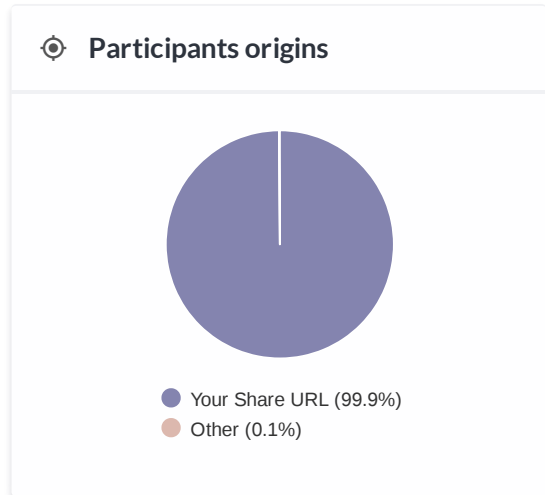
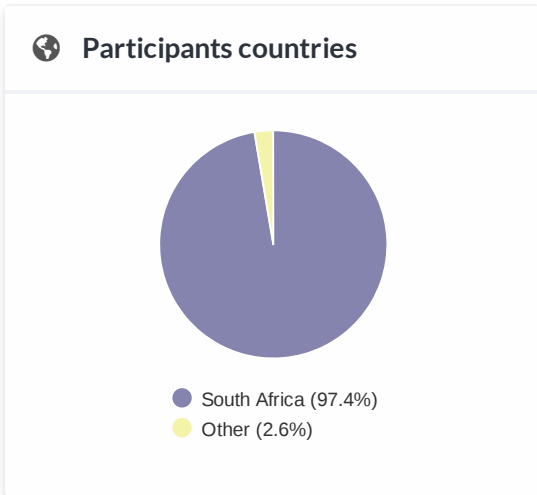
Sabric Survey Malware Protection (Lifetime)	
Title	Analytic
Watch Time	38,613 (minutes)
Average View Duration	0:56
Views	40,731
Impressions	104,038
Average % Viewed	92%
Highest watch time by device	Computer - 66%
Male	58%
Female	42%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

C.5 Computer Hygiene Cyber Security Quiz Results and Video Statistics

Computer Hygiene

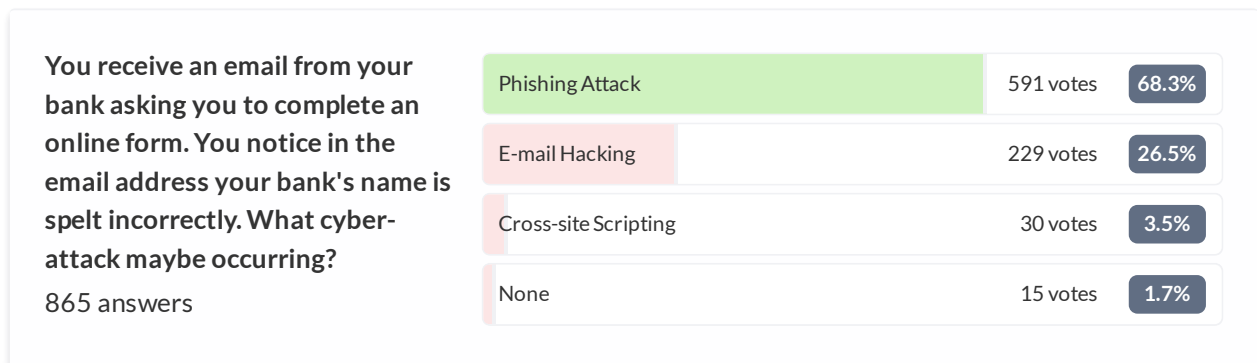
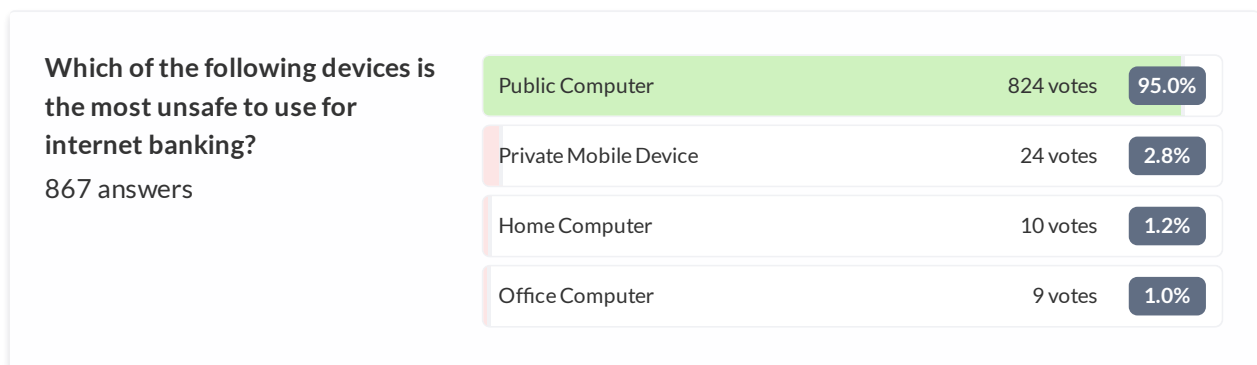
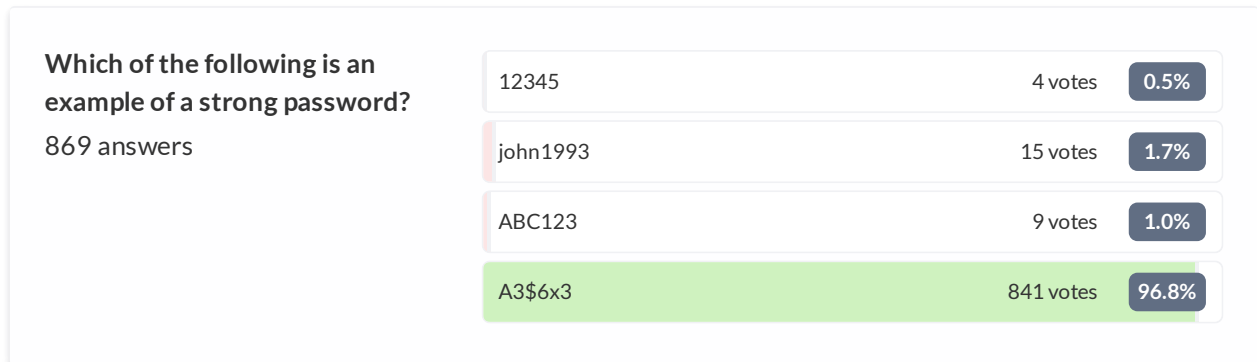
Created on February 21, 2018 by Rahul Maharaj

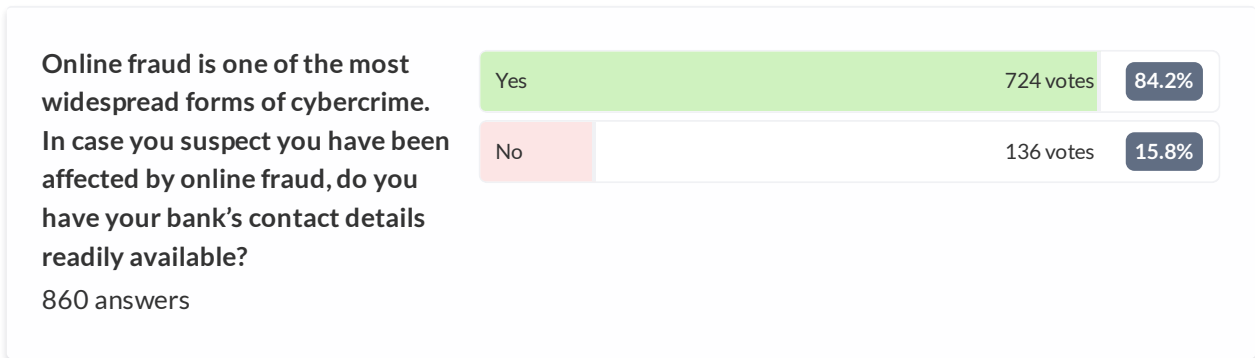
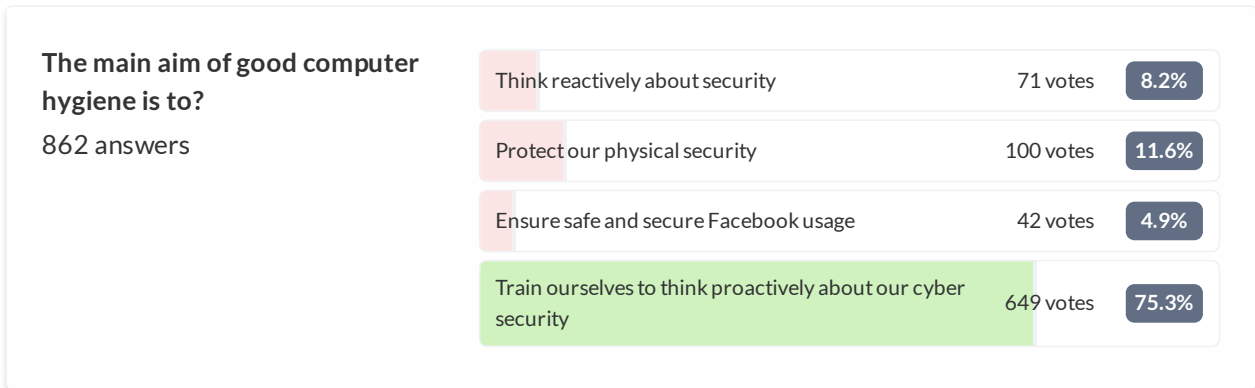
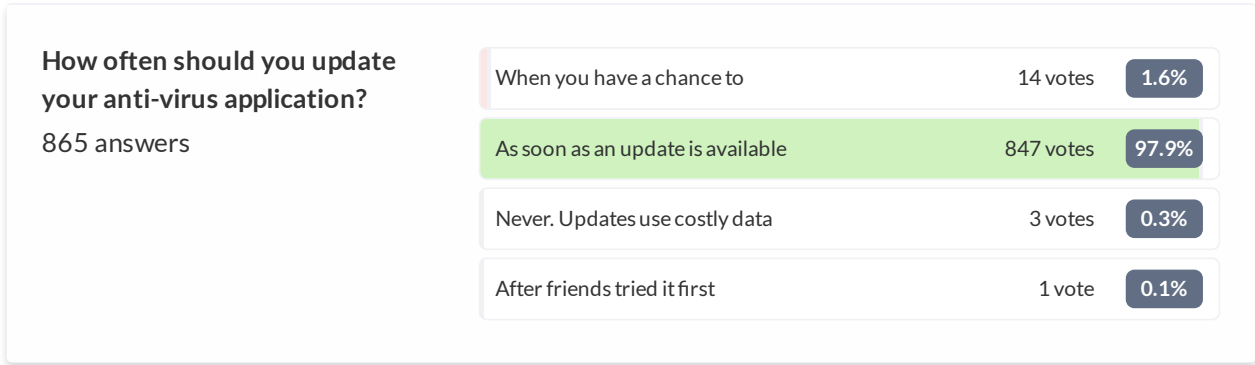




Computer Hygiene

Created on February 21, 2018 by Rahul Maharaj







Sabric Survey Computer Hygiene (Lifetime)	
Title	Analytic
Watch Time	20,615 (minutes)
Average View Duration	1:00
Views	20,258
Impressions	50,393
Average % Viewed	91%
Highest watch time by device	Computer - 60%
Male	65%
Female	35%
AVE	Digital platforms provide very accurate analytics so an AVE is not typically measured on YouTube.

Appendix D

Academic Publications

Appendix D includes the academic papers that were written throughout the duration of the study:

1. International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018)

D.1 HAISA 2018 Publication

The paper titled 'Social Networking: A Tool for Effective Cyber-security Education in Cyber-Driven Financial Transactions', was published in the proceedings of the 2018 HAISA international conference that took place in Dundee, Scotland

Social Networking: A Tool for Effective Cybersecurity Education in Cyber-Driven Financial Transactions

Rahul Maharaj and Rossouw von Solms

Nelson Mandela University, Port Elizabeth, South Africa
s212254189@mandela.ac.za, rossouw.vonsolms@mandela.ac.za

Abstract. Cyberspace technology and cyber-driven services are core in today's modern world. This means that cyber services can be found in many facets of societies and many of the world's industries. This is also true for banking and users of cyber-driven financial transactions. Cybersecurity education is becoming imperative for users to be able to protect themselves better against a wide variety of threats. This is especially true for banking users, who due to the financial nature, are affected by a growing number of cyber-related threats. This paper presents an educational approach using social networking to assist in educating modern users of cyber-driven financial transactions.

Keywords: E-banking, Education, Cybersecurity Education, Social Networking, Cyber-driven financial transactions.

1 Introduction

In modern times, the rise of information technology (IT) can be seen in many facets of industry. IT innovations and developments shape the way end-users interact with traditional industries. These information technologies and their "partner" cyberspace have become intertwined in end-users' lives. Cyberspace and IT can both be seen as critical aspects of end-users' day to day lives. Although cyberspace has brought about numerous benefits, it has also introduced aspects of danger and risks in end-users' modern way of living. As end-users become more and more reliant on cyberspace, the chances of them becoming potential victims of cybercrime increases unless they are made aware and vigilant of the dangers surrounding their cyber activities. Examples of these possible dangers include e-mail hacking, phishing attacks and social engineering attacks. It is essential that end-users are made aware of these potential dangers and how to protect themselves more effectively. This is particularly important for end-users involved in cyber-driven financial transactions. Due to the financial nature of these cyber-driven financial transactions, users of these cyber services are often faced with more threats. According to the Financial Fraud Action UK (Five et al., 2017), financial fraud losses across payment cards, remote banking and cheques totalled £366.4 million between January and June 2017. During that period compromised personal and financial data was seen as a key driver of the financial losses (Five et al., 2017). Criminals utilized attacks similar to the above mentioned. Thus, it is critically important that end-users, specifically when conducting cyber-driven financial transactions, are made aware of the dangers and risks associated with negligent behaviour when doing so.

2

This paper attempts to address the lack of education surrounding end-user cyber-driven financial transactions by introducing an alternative education approach utilizing two prominent social networking platforms, Facebook and YouTube. This paper will focus on the introduction of this educational approach as part of a joint research project undertaken with the South African Banking Risk Information Centre (SABRIC).

2 Background

The aim of this section is to provide a sound base and motivation for cybersecurity education, awareness and training to individuals exposed to sensitive personal and organizational cyber, especially users of cyber-driven financial transaction.

2.1 Cybersecurity Education, Awareness and Training

Cybersecurity is comprised of various elements, varying from technical to operational and behavioural security. There is no single solution to address it and therefore a multifaceted approach needs to be taken. Cybersecurity education, awareness and training provide end-users with the ability to recognize related threats where acceptable and act on them appropriately. Traditionally cybersecurity education, awareness and training programs have been targeted at organizations. However, in modern times cyberspace is at a simple “click” or “tap” away for everyone and thus cybersecurity education should be part and parcel of the lives of all end-users. This includes banking users involved in cyber-driven financial transactions, where end-users are particularly vulnerable.

2.2 Banking and Cyberspace – The shift in responsibility

Banking is one of the oldest industries in the world. As with many long-standing industries, banking has evolved over time, embracing new technologies and markets. This is also true for cyberspace, as many financial institutions and the way they transact are heavily dependent on cyberspace and IT (Horn, 2010). As financial institutions introduced more cyber-related services, it allowed users to take a more active role in their personal financial management. As seen with the introduction of the ATM and in more recent times mobile and internet banking. This shift, puts more responsibility in the hands of users, as they now become a potential point of weakness in the banking process. This statement is echoed in research where end-users are often considered weak links in the information security process (Al Awawdeh & Tubaishat, 2014; Aloul, 2012; Frauenstein & Von Solms, 2014). Thus, as mentioned in the previous section, modern banking users involved in cyber-driven financial transactions are very dependent and will benefit from appropriate education, awareness and training. As this will enable them to conduct personal banking in a more secure and safe manner, giving users peace of mind.

2.3 Cyber-Driven Financial Transaction Education

Cyber-driven financial transactions can be regarded as any transaction that occurs involving cyberspace. Examples of cyber-driven financial transactions include ATM usage, online purchases and credit card usage. As such, it can be seen that the majority of transactions that occur in modern banking can be regarded as cyber-driven financial transactions. As stated in the Ombudsman's Annual Report for Banking Services South Africa (2016), a large number of users are negatively affected by cyber-crime. Human error or, as mentioned previously, negligence is a large contributor, in financial loss experienced by users during cyber-driven financial transactions. Human error can be as a result of inexperience, improper training, the making of incorrect assumptions and other circumstances (Whittman & Mattord, 2013). Therefore, it can be argued that there is a need for proper education, awareness and training among users of cyber-driven financial transactions. Education and training are literally 'placed' between users and the cyberspace or systems utilized (Whitman & Mattord, 2012). It is through proper education, awareness and training that it is possible to foster a cyber-culture of secure cyber usage towards conducting safe cyber-driven financial transactions. It is thus clear that users may be self-responsible for malicious cyber-driven financial incidents due to their lack of related education, awareness and training or ignorance on the subject matter. Further, that education plays an important role in cyber-driven financial transactions to ensure that users are knowledgeable about utilizing cyber services in a secure manner. Through proper education, that increases their awareness, it reduces their inherent negligence and ignorance and therefore assists in mitigating the related risks associated with cyber-driven financial transactions.

Financial institutions, offering these cyber-driven financial services, do offer some educational material and services to educate their clients and therefore helping to mitigate the associated risks. Even though the educational content is correct, the content may be challenging to locate and also, the material is not necessarily presented in a manner that appeals to the average user. The following section will discuss an alternative educational approach that aims to educate users of cyber-driven financial transactions allowing them to conduct these cyber services safely and securely.

3 Instrument Implementation

It is clear from the foregoing sections that users of cyber-driven financial transactions are extremely vulnerable. This is due to the increased threats they face and the lack of appealing education surrounding the subject matter. This section will provide insight into how an alternative educational approach was created in partnership with the South African Banking Risk Information Center (SABRIC).

3.1 Research Approach

This research resides in the problem-solving domain and follows a mixed methods approach. The research approach followed is that of an experiment, utilizing an instrument within the social media domain to gather data. The instrument in this context is the

4

cybersecurity education tool utilizing a social media quiz and video combination created in order to raise awareness and educate users of cyber-driven financial transactions.

The structure of the following sections and subsections will firstly provide the context and environment in which the instrument will be implemented; secondly to describe the instrument and its content, thirdly to describe the research agent and finally to describe the instrument's implementation.

3.2 Context of Implementation

Cyber usage and cybersecurity is a topic often addressed in the South African banking industry. The majority of security-related efforts resides in the technical space. However, technical security safeguards are only as secure as the users involved in the process at hand. As stated in literature, hardware and software security mechanisms are widely used to strengthen information systems (IS) against attacks, however, these systems are still vulnerable because of user's undesirable behaviour (Öğütçü, Testik, & Chouseinoglou, 2016). As cyber services and technology has integrated into the daily lives of many people, including those involved in cyber-driven financial transactions, it has become critical to ensure that users are educated about threats and dangers related to their cyber services. The context in which this study occurs is at a national level, using social networking platforms as an educational tool. A fun social networking quiz (to raise awareness) and a related informative video (to educate) therefore had to be created. This two-fold approach and the use of social networking form the basis of the instrument. The design of the instrument was carefully considered and is discussed in the next subsection.

3.3 The Instrument (Social Networking Game Quiz and Video)

The instrument is targeted at the majority of South African banking clients - the majority of which make use of cyber-driven financial services. Therefore, considerations in the design of the instrument include; audience-appropriate content, delivery mechanism, ease of use and understanding. Existing educational instruments used by South African banks were considered as a basis for the instrument. However, the current state of awareness and education is lacking and unappealing. During an initial discussion with the South African Banking Risk Information Center (SABRIC), a two-fold approach, a combination game-type quiz and an accompanying video, was decided upon. This approach served as the basis for the instrument for two major reasons. Firstly, social networking, particularly Facebook and YouTube are growing rapidly in South Africa and allow for a far wider audience to be reached. Secondly, a social networking game and video approach lower the audience preconceived notions about typical education, which can be seen as dull and unappealing. This makes the instrument more mass marketable. The design and content will be discussed in the following subsections.

3.3.1 Design

This subsection will address the reasons why a social networking game quiz and video combination was chosen as the most suitable instrument to raise awareness and educate users of cyber-driven financial services. The focus of this section will, therefore, be the design of the instrument.

Firstly, the instrument's approach must cater to a wide audience. Due to SABRIC's involvement, the instrument had to be designed to reach a national audience. This was achieved by making use of social networking (Facebook and YouTube) as the platform for which the instrument would be hosted. Facebook, as of the fourth quarter of 2017, has 2.2 billion active users, with a significant amount being South African (Statista, 2017). This allowed the instrument to be reached by many users of cyber-driven financial transactions, accomplishing the goal of being able to reach a wide audience. Secondly, the design of the instrument had to be "fun" and interactive. This allowed, as previously mentioned to lower the preconceived notions of traditional learning. This was achieved by using a high score type quiz format. The quiz served as an awareness-raising tool. Using a quiz format allowed for the instrument to be interactive and have that "fun" factor. This interactive approach appeals to many social networking users as quizzes are typically popular with some quizzes seeing an average of 60 000 user engagements (Boland, 2017). Thirdly, the instrument had to allow for users to be educated in an alternative manner. This was done by a short, suitable video. Once the user completed the quiz (raising awareness) they were then prompted with a video on the subject matter. Video was used due to its ease of use and lack of effort required by the user to educate themselves. Videos produced were short as this enables a user to keep focus throughout the duration of the video, enabling them to better concentrate.

An element of educational reinforcement is also incorporated in the instrument. This is done by introducing a message after a user selects an answer. The message relates to the question, after a participant, answers the quiz questions the message is displayed. This enables the user to learn (reinforcing), alongside the "fun" quiz.

In order for the user to benefit, the content of the quiz and video is very important to ensure focused and relevant learning takes place. The content found in both the video and quiz are obviously of particular importance.

3.3.2 Content

Five quizzes with five related videos were created. Topics were chosen following close liaison with SABRIC regarding what affects the typical cyber-driven financial transaction user most. Examples of topics include online shopping, malware, card fraud, cyber hygiene and mobile banking. Online shopping will be used as an example in this paper.

The questions asked in the quizzes were topic related and pertaining to safe and secure online shopping. Table 1 represents the online shopping quiz questions and answers.

Table 1. Online Shopping Sample Question

Question: Which of the following contribute to unsafe online shopping?	
Answer A:	Saving of payment information in web browsers
Answer B:	Using a well-known online merchant
Answer C:	Making use of 3-D secure payment
Answer D:	Looking for the closed padlock symbol
Correct Answer Text: Right answer! Never save payment information in your web browser as it may be used if someone gets a hold of your device.	Incorrect Answer Text: Wrong answer! Some sites (as well as all browsers) offer to “remember” your payment information (e.g. password) for your convenience upon subsequent purchases. Never accept to have your "financial information" stored on any website/web browser.

As in the above table, quiz questions were structured as multiple-choice questions with four possible answers. The video that relates to the quiz is roughly 1 minute and 30 seconds long. As mentioned previously, the videos were kept short in order to hold the user’s attention. The online shopping video comprises of the following five pointers for safe and secure online shopping. These five pointers are;

1. Look out for the padlock followed by HTTPS next to the URL when transacting online – the ‘S’ indicates that you are connected to a secure and encrypted website.
2. When registering on a secure site, choose a strong password and do not save your login details on any computer or mobile device. Never re-use the same password on multiple domains.
3. Avoid sharing your personal information, online merchants don’t need your ID number or date of birth to process your order, but cybercriminals can use this to steal your identity.
4. Check your bank balance after making any online shopping payments. Report any fraudulent transactions to your bank as soon as possible.
5. For added online shopping verification, register your bank card with 3D Secure.

The message behind this video is to educate the users to perform online shopping in a safer and more secure manner. The video itself is an animated production, with a ‘look and feel’ that should appeal to users.

As discussed, this study focuses on five topics, namely; online shopping, malware, card fraud, cyber hygiene and mobile banking. However, the topic of online shopping will be discussed as an example in this paper. The instrument was designed to meet the following goals. Firstly, the instrument had to reach a wide audience. Secondly, it had to be “fun” and interactive. This was done through the creation of a social media game quiz and related video. All quizzes comprise of five, close-ended questions and are linked to the video. After a user selects an answer, regardless if it is a correct or incorrect answer, an educational message is displayed. This, as previously mentioned, adds an element of educational reinforcement.

The effectiveness of this instrument as a cybersecurity educational tool will be determined by the research agent, to be discussed in the next section.

3.4 Research Agent

The research agent consists of two parts. The initial part of the research agent constitutes the quiz. The quiz, alongside raising user awareness, has been used to capture statistical data about the level of awareness and knowledge that users of cyber-driven financial transactions possess. The quiz questions are close-ended, multiple-choice questions which relate to the most prominent threat situations users face concerning cyber-driven financial transactions. This allows for some approximation of users’ awareness levels and knowledge to be rated per quiz. The primary data gathered from the quiz includes; correct and incorrect answers, while additional data captured and calculated includes; average score, number of participants, participant country, participant device, gender and average elapsed time. The ratio of correct and incorrect answers gives some indication of the users’ level of awareness and knowledge on the specific topic. Incorrect answers indicate that users might lack awareness and knowledge to conduct these cyber services in a safe and secure manner.

The second part of the research agent consists of a single question asked at the end of each video. The question asked, attempts to determine if the user feels more positive and assured of the level of knowledge on the subject matter acquired. Users are only asked this question, once they complete both the quiz and the video.

Both parts of the research agent, therefore, form part of the instrument and is applied in the context of this study. The combination of both parts of research agent, indicates the level of awareness and education before and after the instrument has been used. All five quizzes and related videos follow the research agent outlined in this section. The instrument’s implementation will be presented in the following section.

3.5 Implementation (Experiment)

The research agent was distributed through social media channels in the form of the final instrument. The distribution took place primarily through a Facebook campaign which took place in partnership with SABRIC. This allowed for a wider audience to be reached, as SABRIC is an authority in the local banking environment. The initial campaign began on the 27th of March 2018. SABRIC released a media statement alongside

8

a sponsored Facebook campaign. The sponsorship consisted of promoting the associated videos themselves through paid adverts on YouTube and promoting the quizzes via sponsored adverts on Facebook directly. This sponsorship allowed for a greater target audience to be reached. While the campaign was being run, the quizzes were also shared from other sources. These sources included, the researcher's own Facebook and any participants that opted to share the quizzes themselves. At present the social media campaign is still ongoing, as such participants are still taking part in quizzes and viewing the educational videos.

The following section will discuss the results of the research agent with the focus being on the topic: online shopping.

4 Analysis and Results

As mentioned previously, there are five quizzes with five related videos. Quizzes are based on topics most prevalent to users of cyber-driven financial transactions, according to SABRIC. This section will discuss the results of a single quiz, namely; online shopping, as the social media campaign is still ongoing and part of a larger research project.

At present, the online shopping quiz has 420 participants of which 86% fully completed the quiz. This results in a total of about 389 participants. 57% of participants were female and 43% were male. A small number of participants accessed the quiz via a mobile device (37%) while the majority of participants accessed it via their desktop machine (63%). Due to social media being accessed worldwide, participants were not only from South Africa. At present 92.2% of participants are South African, while 1.8% are United States citizens, 2.4% are United Kingdom citizens, 3% are Icelandic citizens and 0.6% are from other countries.

Within the quiz, six questions relating to online shopping were asked. These questions were asked before mention was made to the associated educational video. Only once a participant has completed the initial quiz, they can view the associated video. Once the video was watched, a follow-up question was asked, in order to assess if the participant felt he/she learned something from the quiz and related video. The overall results show that participants, regardless of their score, felt as though they had learned something and that they could conduct their cyber-driven financial transactions in a more safe and secure manner. The table below shows the results for the online shopping quiz.

Question Number	Correctly Answered (%)	Incorrectly Answered (%)
1	89.0	11.0
2	51.4	48.6
3	94.4	5.6
4	79.6	20.4
5	61.9	38.1
6	75.4	24.6

Table 2. Online Shopping Participant scores

As seen in the above table, participants scored well in the quiz.

Due to the videos being promoted separately from the Facebook quizzes, the online shopping video was viewed at present 38 141 times. One hundred percent of the users that answered the poll, responded positively to the question whether the video was indeed useful and added value. It can be seen from the number of views recorded that users preferred to go directly to the video rather than following the quiz-video route. This might be interpreted that a large number of users are already aware they lack proper knowledge to deal with the cyber threats they face. Irrespective of the standalone YouTube video views, results show that a combination of both the quiz and video can be a successful educational combination. In general, this study confirms that participants gained relevant knowledge and confidence on how to conduct online shopping safely and securely in cyberspace, through a social networking educational approach.

5 Conclusion

Cyber-based services are found in many businesses and industries today. This is particularly true in the banking sector, where users make use of ATMs, internet and mobile banking. These users of cyber-driven financial transactions pose a great risk to themselves, through negligent or ignorant behaviour. Therefore, relevant cybersecurity education and awareness is a must for these users. Social media and social networking can indeed be used as an educational tool towards effective cybersecurity education, under the following conditions: firstly, the material can be accessed with ease, secondly, the material is appealing to users and thirdly, that the material is not too data and time-consuming.

This study has shown that if implemented correctly and made appealing, users can be made more aware and educated through the means of social media. Allowing them to conduct their cyber-driven financial transactions in a more safe and secure manner. It is therefore concluded that, social networking and social media in general and specifically in the format used in this study, can be a possible option for the education of users of cyber-driven financial transactions. However, further research should be done to improve the process.

10

6 Future Work

The results shown in this paper is part of a larger ongoing study. The next stage will be to complete the social media campaign and verify all quiz results to show statistical significance. This will allow for the educational approach of utilizing social networking for cybersecurity education to be verified.

Acknowledgements. The South African Banking Risk Information Center (SABRIC) is acknowledged for their contribution towards this research project.

References

- Al Awawdeh, S., & Tubaishat, A. (2014). An information security awareness program to address common security concerns in IT unit. *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations*, 273–278. <https://doi.org/10.1109/ITNG.2014.67>
- Aloul, F. a. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, 3(3), 176–183. <https://doi.org/10.4304/jait.3.3.176-183>
- Boland, G. (2017). What to know about quizzes on social in 2017 - NewsWhip. Retrieved March 2, 2018, from <http://www.newswhip.com/2017/04/know-quiz-content-2017/>
- Five, T., Campaign, S. F., Office, H., Taskforce, J. F., Fraud, F., Uk, A., & Five, T. (2017). 2017 half year fraud update : Fraud : January to June 2017, (September).
- Frauenstein, E. D., & Von Solms, R. (2014). Combatting phishing: A holistic human approach. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. <https://doi.org/10.1109/ISSA.2014.6950508>
- Horn, S. (2010). *Cyberville: Clicks, Culture, and the Creation of an Online Town*. Grand Central Publishing. Retrieved from <https://books.google.co.za/books?id=7VGZCwAAQBAJ>
- Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83–93. <https://doi.org/10.1016/j.cose.2015.10.002>
- Ombudsman Annual Report for Banking Services. (2016). Ombudsman Annual Report 2016 for Banking Services.
- Statista. (2017). Worldwide 2017 | Statista. Retrieved March 2, 2018, from <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>
- Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security. Course Technology*. <https://doi.org/10.1016/B978-0-12-381972-7.00002-6>
- Whittman, M. E., & Mattord, H. J. (2013). Management of Information Security Fourth Edition, 545. <https://doi.org/2013945552>

The true warrior understands and seizes
the moment by giving an effort so intense
and so intuitive that it could only be
called one from the heart.

Pat Riley