Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2015 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2015

An Initial Study of Customer Internet Banking Security Awareness and Behaviour in China

Ruilin Zhu
University of Auckland, ruilin.zhu@auckland.ac.nz

AN INITIAL STUDY OF CUSTOMER INTERNET BANKING SECURITY AWARENESS AND BEHAVIOUR IN CHINA

Ruilin Zhu, Department of Information Systems and Operations Management, The University of Auckland Business School, Auckland, New Zealand, ruilin.zhu@auckland.ac.nz

Abstract

Internet banking is becoming increasingly popular throughout the world due to its convenience and low cost. The security issues surrounding internet banking are always the focus of both banks and customers. Although much emphasis has been laid on advanced security technology and the human factor in security, there is little research that aims to fully understand customer awareness and behaviour of internet banking security in China. This paper presents the findings from an initial study conducted to evaluate current levels of customer awareness of internet banking security and to map out the linkage between awareness and behaviour. Some of the findings raise implications which call for further investigation.

Keywords: internet banking, security awareness, behaviour, TPB

1 INTRODUCTION

Internet banking is now widespread around the world due to its convenience and low cost. As banks go all out to publicise internet banking, more and more customers are attracted to using this service. According to a survey of US customers by ABA (American Bankers' Association) in August 2014, internet banking remains America's most popular banking method, with 31% of respondents citing it as the banking method they use most often (ABA 2014). The same pattern has been seen in China; China Merchants Bank was the first bank in China to launch an internet payment system in 1997, and since then internet banking has spread widely and rapidly in China. Most commercial banks in China, including state-holding banks, joint-stock commercial banks, and local city commercial banks, provide the service as an important supplement to existing branch activities. By the end of July 2014, the number of internet banking customers in China had reached 271 million, up 8.7% since the previous year (CNNIC 2014).

In their desire to provide reliable and trustworthy service, the security issues surrounding internet banking have always been the priority on the banks' agenda. Many advanced and sophisticated technologies have been deployed, with digital certificates, USB-keys and OTP-tokens all being used to mitigate fraud. However, internet banking scams are still rampant and causing mounting losses, and internet banking security is still among customers' concerns (Ma 2012).

According to Financial Fraud Action UK (FFA), total losses associated with internet banking in the UK reached £40.9m in 2014 (FFA 2014). It is reported that between January 2012 and August 2013, China's public security bureaus cracked more than 110,000 cases relating to telecommunication fraud concerning 180,000 bank accounts. In the month of May 2012 alone, the Beijing Police Bureau cracked fraud totalling over 42 million Chinese Yuan, with 38% of the cases related to online trading (Li 2014).

Hal R. Varian observed that "modern cryptography is often hailed as the magic elixir that will make cyberspace safe for commerce; but it will only work if people use cryptographic security features effectively" (Varian 2000). Today's security problems are primarily due to the inadequate security awareness of users (Rowe et al. 2013; Waly et al. 2012) and their poor security behaviour (Shepherd et al. 2013).

Many studies have addressed this concern, however these are sporadic and patchy. Research into security awareness is almost always conducted from an employee's perspective in organisations; few studies have been initiated to analyse customer awareness. Moreover, awareness is an important factor that may enable exogenous influence over behaviour (Albrechtsen & Hovden 2010), but it remains unknown how awareness specifically may affect security behaviour in regard to internet banking, as the bank has no direct control over the customers' awareness and behaviour. In particular, as China is more severely plagued by online scams and frauds, internet banking is more likely to be attacked. Therefore it is high time to closely examine the current security situation in China.

Without possession of adequate information about the situation of customer awareness and behaviour regarding internet banking security, the first step is to conduct a survey and interview to investigate these issues. The research questions relate to (1) generally what the current customers' awareness and behaviour of internet banking security are; and (2) specifically how customers' awareness of internet banking security affects their security-related behaviour.

The outline for the paper is as follows: existing literature is examined in Section Two, where the theoretical framework will be introduced thereafter, the research method is presented in Section Three, and this is then followed by the Discussion and Conclusion sections.

2 LITERATURE REVIEW AND THEORETICAL FRAMEWORK

The concept of security awareness arises from the process of technological advances, which are featured with three stages of development (Thomson & von Solms 1998). With the introduction of the personal computer and the increasing complexity and reliability of information technology, information systems have become an indispensable part of daily operations with a diversified profile of end-users. In this regard, it is necessary to implement security awareness education for all users who are able to get access to this information. To be specific, security awareness is defined in the NIST (National Institute of Standards and Technology) Special Publication 800-16 as follows: "Awareness is not training. The purpose of an awareness presentation is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information" (NIST 1998).

This is echoed with a series of conceptual studies (Furnell et al. 2002; Hentea et al. 2006) that highlight the importance of information security awareness. Thereafter this topic has garnered increasing academic attention over the following periods. In particular, Puhakainen and Ahonen (2006) proposed a design theory for improving information security awareness campaigns, while D'Arcy et al. (2009) suggested that organisations can adopt user awareness of security policies as one of the three security countermeasures to reduce the misuse of information systems. To complement this, some scholars have explored the relationship between awareness and behaviour. Albrechtsen and Hovden (2010) specifically investigated the positive effect of awareness on behaviour. As a step further, Bulgurcu et al. (2010) conducted an empirical exploration that analysed the roles of information security awareness on an employee's compliance behaviour.

The researchers interested in this topic have mainly focused on the organisational level of information security awareness as most of the contexts were set in a company environment. Siponen (2001), therefore, introduced a five-dimension information security awareness framework, which expands to both organisational and societal levels, but the user dimension of the problem is nonetheless neglected (Furnell et al. 2006; Herath & Rao 2009). As a result, Tariq et al. (2014) call for studies that examine the issue from an individual's perspective.

In response, many studies have been advanced. However, almost all of these studies are discussed in the context of employee security awareness (Shaw et al. 2009; Valentine 2006), while little research (until quite recently) has been conducted to analyse the customer awareness for a certain device/service, for instance, smart phone (Mylonas et al. 2013) and internet banking (Daniel et al. 2014).

The most obvious difference lies in the role of end user. In organisations, the users are employees, who are "required" to enhance the level of security awareness, while in the case of internet banking, the users are customers, who are only "recommended" to do so. This major discrepancy indicates that most of the current understandings of awareness of security may not be directly used in the internet

banking setting. In addition, the extant research does not specify how awareness may affect customers' behaviour, as unlike the employees' in the organisations, the banks have little control over either customer awareness or behaviour. Consequently, even though the link has been theoretically established between them, the current research does not facilitate the practical implementation and utilisation of this relationship.

In order to address these concerns, I chose the Theory of Planned Behavior (TPB) (Ajzen 1991) as the theoretical framework, through which the research questions are examined and discussed. As an extension of the Theory of Reasoned Action (Ajzen & Fishbein 1980), TPB has been used in various studies in information systems research due to its parsimony and effectiveness. TPB examines and predicts an individual's intention to perform a certain behaviour by taking into account three determinants, viz., attitude (towards the behaviour), subject norm, and the perceived behavioural control.

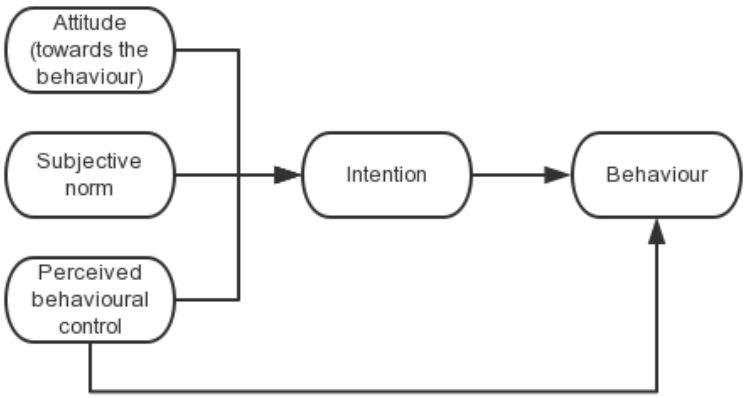

Figure 1 TPB, from Ajzen (1991)

Attitude refers to the overall evaluation of the behaviours, while subjective norm is the individual's belief of others' thought about whether he/she is able to perform the behaviour. Perceived behavioural control is related to the perception of the extent to which performance of the behaviour is easy or difficult (Ajzen 1991). It is worth mentioning that TPB also has a direct link between perceived behavioural control and the actual behaviour.

Conner and Armitage (1998) posit that as intention has determinants, the attitude, subjective norm, and perceived behavioural control may also be held to have determinants. To be specific, attitude is a function of a person's salient behavioural belief, which illustrates the perceived outcome of the behaviour. Perceived behaviour control includes both internal control factors, such as personal skills, abilities, and external control factors, such as dependence, and opportunities.

TPB is a well-researched research model that has been proved successful in explaining behaviours. While addressing simultaneously the construct of behaviour and some related factors that are examined in this research, it also leaves open the possibility for the researchers to specify the particular determinants that are associated with the three factors in an effort to tailor it for a certain research scenario. Given its usefulness and expandability, I utilise TPB in trying to work out the possible determinants that may affect the security-related behaviour with a focus on the security awareness.

3 METHODOLOGY

3.1 Method

The definition of security awareness (see above) mainly refers to the term in the context of individual, and it can be seen from these various descriptions that: (1) security awareness is not a process, but a state that results from a series of intended activities, and the knowledge that is used to protect recipients themselves and related benefiting parties from attacks; and (2) the level of security awareness can be gauged from the recipients' attitudes towards security issues. The nature of the definition, therefore, fits well with the qualitative research, which is designed to help researchers understand people and the social and cultural contexts within which they live (Myers & Avison 1997). As a result, I employed a qualitative method to investigate this issue. I triangulated the data by adopting both survey and interview. It is a way of assuring the validity of research through the use of a variety of methods to collect data on the same topic (Bryman 2004).

The survey took place from July to August 2014 in Chengdu, China. I conducted two-stage studies, which consisted of questionnaire and semi-structured interview. The survey questionnaire, which contained 29 questions, was mainly designed to estimate the level of awareness among customers regarding internet banking security. It also aimed to investigate customers' habits and experience of using internet banking.

This information will be useful in two ways: firstly, knowing more about the current state of customer security awareness and customer behaviour will help me assess the appropriateness of current internet banking security strategy, particularly in regard to human factors and potential frauds aimed at customers and their behaviour. Secondly, knowing more about customers' habits and experiences will help me determine how awareness, along with other factors, may affect behaviour.

In this regard, basic information concerning customers' general views of, and attitudes towards, internet banking security were gathered in Section 1 of the survey, while their knowledge about internet banking security was collected in Section 2. The main purpose of Section 3 was to investigate customers' habits and behaviour regarding internet banking.

After completing the survey, each subject was encouraged to share their ideas or opinions with the researcher in a semi-structured interview. The interviewees were allowed to express their views on aspects they considered to be of importance. These interviews helped me fully understand their real thoughts; as the intention was for customers to feel relaxed about communicating with me, no recording devices were used during the process (Silva & Backhouse 2003).

Semi-structured interviews were selected as the means of data collection due to two primary considerations. First, they are well-suited for the exploration of the perceptions and opinions of respondents regarding complex and sometimes sensitive issues and enable probing for more information and clarification of answers (Barriball & While 1994). Additionally, according to Bernard (1988), they are best used when the researcher will not get more than one chance to interview the subject and when the researcher will be sending several interviewers out into the field to collect data. The semi-structured interview guide provides a clear set of instructions for interviewers and can provide reliable, comparable qualitative data (Cohen & Crabtree 2006). The inclusion of open-ended questions provide the opportunity for identifying new ways of seeing and understanding the topic at

hand. Finally the varied professional, educational and personal histories of the sample group precluded the use of a standardised interview schedule.

After the interview, grounded theory was employed to analyse the data. Grounded theory is a qualitative research method that seeks to develop theory that is grounded in data systematically gathered and analysed. It has become increasing popular in information systems' domain (Bryant et al. 2004; Howcroft & Hughes 1999; Lings & Lundell 2005). According to Martin and Turner (1986), grounded theory is "an inductive, theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data". Grounded theory has proved to be extremely useful in developing context-based, process-oriented descriptions and explanations of information systems phenomena (Myers & Avison 1997), which fits well with the nature of this research.

3.2 Subject selection

Subjects were all the current internet banking users of one local bank in China, who were roughly categorised into three groups: IT background, financial background and other background. A total of 46 valid subjects (19 females and 27 males) participated in the survey, whose ages ranged from 17 to 54 (7 persons within the Group 17-24 age, 15 persons within Group 25-34 age, 16 persons within Group 35-45 age, and 8 persons within Group 45-54). What I wish to clarify here is that I intentionally chose the subjects with an IT background as in the real life, they are facing internet banking attack as well. In addition, a general sample makes the research more authentic and reliable.

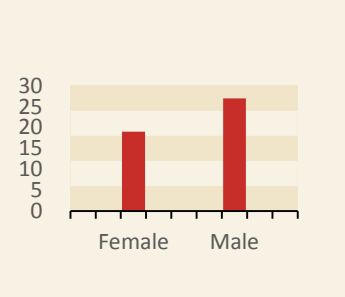

Figure 2 Gender of participants

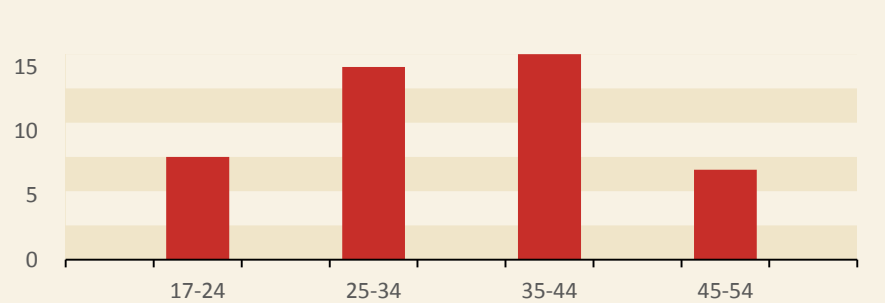

Figure 3 Age of participants

3.3 Procedural overview

With the permission of the banks concerned, the survey was conducted at one of its main branches located at Chengdu, China at noon for five consecutive weeks. This bank has the most extensive branch networks in the city and is the market leader. In China, people tend to have a rest at noon, giving the subjects enough time to participate without hurry. I identified the potential subjects after they finalised their own internet banking related transactions at the teller-counters, and then I invited them to participate in this activity by specifying the research target and nature. If they agreed to my request, I led them to a nearby VIP client room.

Standard tests were used in the survey; subjects were required to complete the whole test within 15 minutes and were not allowed to seek external help. Section 1, Section 2 and the first half of Section 3 were multiple-choice tests, while the second half of Section 3 was a ranking test; subjects were asked to rank the channels they most liked to use according to their own views and habits. After this, each subject had a five-minute break before I moved to the interview part, which typically lasted for another 30 minutes.

3.4 Data analysis

I split the sample into three groups (8 persons with IT background, 12 persons with financial background, and 26 persons with other backgrounds), according to the participants' responses, in order to examine any differences in their responses. I hence employed the grounded theory to analyse the data, as the purpose of this research is to explore the situation regarding customer awareness of security. Moreover, the exploratory nature of the research question and the objective of gaining an understanding of the situation required an in-depth qualitative data analysis method to generate results.

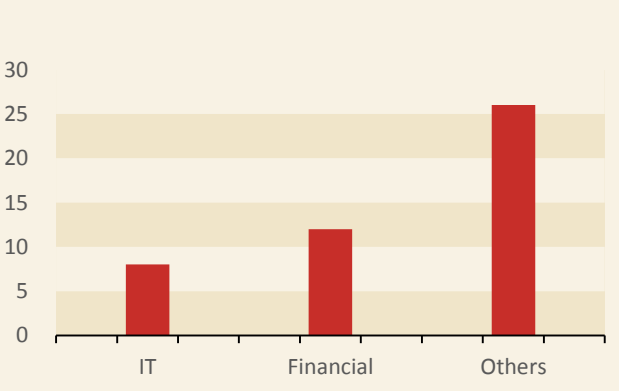

Figure 4 Background of participants

As grounded theory lends itself to the exploration of under-theorized areas (Burck 2005), it is able to aid a researcher to generate theory and in-depth understanding about the processes and to develop conceptual analyses of the social world. Given the understudied nature of internet banking security awareness in China, it is appropriate for me to adopt this method. Moreover, in order to conduct the grounded theory research, scholars should not start with any pre-conceived concepts, which must emerge from the data (Matavire & Brown 2008). As I do not possess any further understanding regarding this topic, this rule was therefore satisfied.

I started the analysis as soon as the data was being collected. Following the principle of constant comparison (Glaser et al. 1968), I systematically compared each new data to former ones, the main purpose of which was to generate theory-based understanding. In this process, data is compared for similarities and differences to form categories until each category identified in the theory is saturated (Glaser 1992).

4 FINDINGS

The survey and interview have revealed some illuminating findings, and will help me better understand the issues surrounding customer security awareness and behaviour.

- Finding 1: Customers are concerned about internet banking security

About 64% of subjects said they were really worried about the security of internet banking, but had nevertheless become users of the service. In later interviews it was found that none of these customers had actually been attacked by scammers, but they still felt uncertain about their fund safety and privacy, and were suspicious of internet banking technologies. One subject said he had reduced the frequency with which he used internet banking, and that he only kept a small amount in his internet banking account. This suggests that the safety of internet banking is the key to building customers' trust in this service. No internet banking service will succeed without this trust. Delivering useful security information to customers and making them more aware of internet banking security is one of the ways to gain their trust and dispel doubts, thereby encouraging them to use internet banking reasonably.

- Finding 2: Not every customer actively cares about internet banking security

More than 50% of subjects indicated that they never ask for information about internet banking security; in other words, a large proportion of customers never visit the website, read brochures or contact the call centre. This indicates that customers are more likely to be the passive recipients of security information in awareness activities, which appears to contradict the belief that if the individual is concerned about security, he/she may be actively seeking relevant information.

- Finding 3: Customers are affected by others' opinions

I notice that from the subjects' perspective, security is more like an intangible confidence rather than a tangible object. Most of them mentioned if some of their friends become sceptical of the security of internet banking, they may gradually reduce the usage frequency. Moreover if they found their friends seldom use the security-enhancing features, they are very likely to stop using them.

- Finding 4: Customers are not really familiar with internet banking security

Although 66.7% of subjects claimed "they know more or less" about internet banking security, it was discovered that nearly half of the subjects did not know what dynamic passwords or digital certificates are or what phishing means. This suggests that customers tend to presume they are more familiar with this information than they really are, which can lead them to relax their vigilance and expose themselves to potential risk. I further notice that those who do not familiarise themselves with security tend to use internet banking in a comparatively dangerous way. For instance, if encountering a possible phishing attack, instead of stopping using or reporting to the bank immediately, some of them may still stay on the webpage for a while.

- Finding 5: Customers are not acquainted with basic technologies and the main threats of internet banking

None of the subjects in the survey knew enough to answer all the basic questions regarding internet banking security in Section 2; about 20% of subjects did not know the website address of their internet bank and nearly 45% did not know the number of the bank's call centre. Subjects with an IT background were familiar with the basic technologies employed for internet banking and the main threats, but even they were unsure about the procedures they should follow when encountering urgent problems. Nearly half of the subjects from financial or other backgrounds did not know the technologies, the main threats, or the procedures. This suggests that customers are not fully informed about internet banking security.

- Finding 6: Each channel has its own advantages for customers

According to the survey, 40.5% of subjects prefer to go to a website to find out about the security of internet banking before setting up an account, while 24.3% would choose to visit a branch of the bank. If they come across problems when using internet banking, 40.5% of subjects would ring the call centre for help while 27% would choose the website. 67.6% of subjects would call the call centre for urgent problems, and 59.5% would use the same channel to offer feedback. Some of the subjects also indicated that they do not stay on any channel for long, suggesting they have only limited time to learn about security-related information.

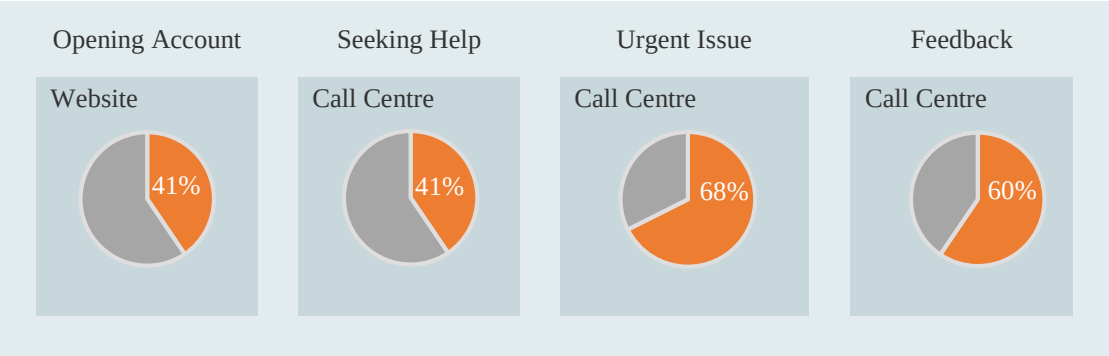

Figure 5 Channels

- Finding 7: The utilisation of complicated settings may backfire

The most frequently faced problems for those subjects who used digital certificates were difficulties with the installation of certificate drivers and the download of digital certificates. Subjects said they felt frustrated when they still failed after several attempts; some said that for fear of the inconvenience a USB-key may cause, they had chosen either an OTP-token or mobile-phone password, neither of which are considered as safe as a digital certificate. For some subjects, as they said, in order to minimise the inconvenience from inputting several different passwords when logging-in or conducting online transactions, they enable the password-remember functions on the browser, which however is obviously not recommended by the banks,

In general, subjects are concerned about internet banking security, but they lack the necessary knowledge to effectively address this concern. Moreover, they are generally dissatisfied with the awareness activities currently being offered by their bank.

5 DISCUSSION

Based on the findings, I further categorise them according to a few specific factors that are related to the three determinants of the intention and security-related behaviour, thereby expanding the TPB to the following one.

Finding 1 and finding 2 are grouped as anecdotes of their attitudes towards the security behaviour. Finding 3 is viewed as the normative structure to subjective norm. Finding 4 is about the customers' general familiarity of internet banking security, while finding 5 is concerned with their knowledge. These two are taken as the internal control factors that are attached to perceived behavioural control. In contrast, finding 6 and finding 7 refer to the availability of the channel and the technology, which are related to the external control factors.

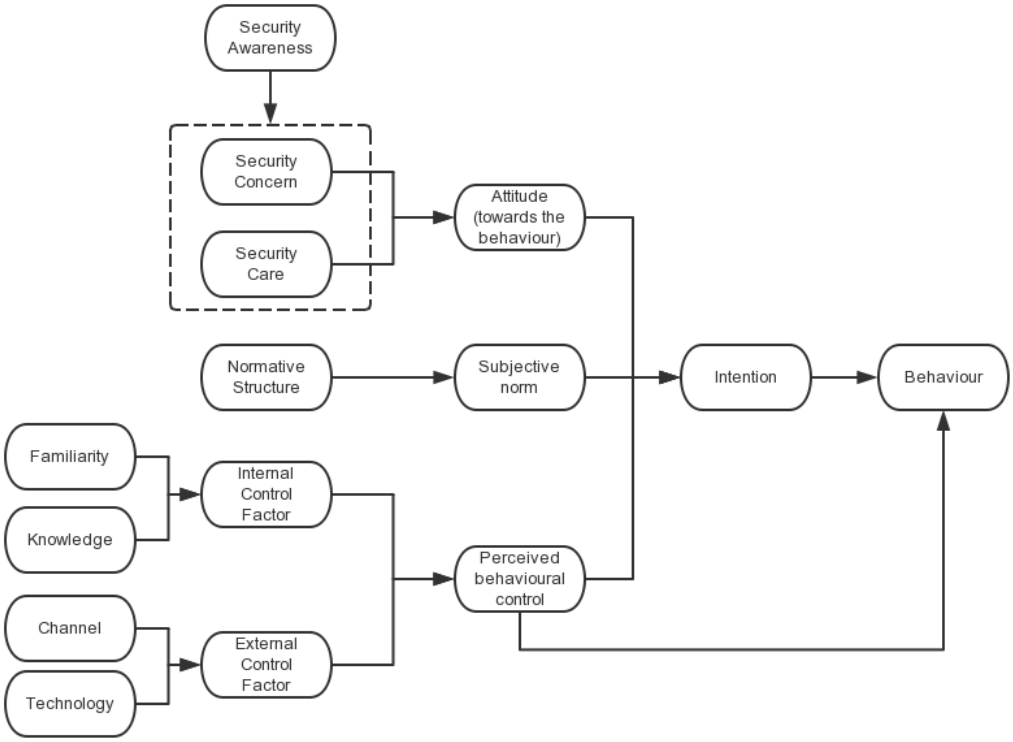

Figure 6 Expanded model

There are several important suggestions stemming from the expanded model that may add to the current understanding of customer awareness and behaviour of internet banking security in China.

- Mixed security awareness

According to the research, I have found the subjects have mixed security awareness of internet banking security: while being concerned about the security of internet banking, they do not actually actively care about it. Similarly, there is a sharp contrast between customers' keen concern on the one hand and their lack of basic knowledge on the other.

One possible explanation is that subjectively customers are indeed very worried about the internet banking security, but objectively they do not possess enough understandable and useful information regarding the issue, which results in their incapability of being security sensitive.

- Attitude is not positively related to behaviour

The model highlighted the once established link between attitude and behaviour. However, unlike previous research that found the link to be positive, I have found that this link can be negative. Even the attitudes of customers towards internet banking security are obvious from the survey; whilst almost everyone claims he/she values and advocates security and security-related behaviour, their actual behaviours that are obtained from the survey and interview are not consistent with this.

There are a few possible reasons. (1) Their attitudes are indeed positive but not adequately positive to enable them to strictly perform secure behaviours. That is to say, before I could determine their positive relationship, I must firstly find out the threshold value of the attitude that may lead to a positive link. (2) Even though their attitudes are positive enough, they have not obtained necessary knowledge or skill to transfer this attitude into action. (3) The subjects' roles in internet banking are different – they are customers, who tend to enjoy a user-friendly, convenient, and one-click service from the banks – unlike the supervised employees.

- Importance of normative structure

It can be seen from the model that normative structure has a clear influential effect on behaviour. To be specific, the subjects are susceptible to others' views and decisions, and they tend to follow these. It suggests that if other people around an individual have a certain level of awareness, it is very possible that he/she may possess a similar one and then act accordingly. This factor is currently overlooked in the internet banking security awareness and behaviour research.

- Importance of control factors

I specify four control factors from this survey and interview, which are further grouped into internal control factor and external control factor. Altogether, they have a clear impact on behaviour. Moreover, some of them may have indirect effects on security awareness and attitudes as aforementioned.

6 CONCLUSION & FUTURE WORK

6.1 Conclusion

Increasing numbers of customers have begun to use internet banking services because of their great convenience and swiftness. However, these big advantages have not gone unnoticed by those wishing to scam. The same benefits that customers enjoy can also be shared with those wanting to compromise security. Ensuring the safety of internet banking is one of the most important duties and commitments for banks.

Apart from technology, the human factor is another essential element in the prevention of fraud. Customer awareness of internet banking security is one effective method that should be taken into full consideration. However, the research indicates that, despite widespread fraud, the general level of customer awareness in regard to internet banking security remains low. There is an urgent need for

improvement here. In addition, even a high awareness alone does not necessarily ensure a high possibility of secure behaviour, as the latter may not be directly positively affected by the former.

The implications of this research are twofold. Academically, not only did I take the lead in understanding the current situation of security awareness and behaviour in China, but I have also initially examined another possible linkage between this awareness and behaviour, and empirically highlighted a possibility of the negative relation. This serves to complement the current research endeavours. Practically, my research sheds light on the internet banking strategy that the banks may adopt to enhance their customers' awareness and encourage reasonable behaviour. The banks may not simply persuade the customer to use their internet banking service in a safe manner, but instead according to the findings, they should provide them with adequate and necessary knowledge and skills.

The research does have some limitations. Firstly, the number of subjects is not large enough, which may affect the generalisation of the findings. I therefore plan to conduct a survey with Amazon Mechanical Turk, which should provide a larger sample covering a range of demographic characteristics (Paolacci et al. 2010). Secondly, this survey does not take into consideration the different types of bank. The scale and governance system of a bank may have an influence on its customers' level of awareness and behaviour regarding internet banking security. This also calls for deeper exploration. Finally, the survey was conducted in a city in western China, and its findings may not apply to other cities in different regions, where the economy and IT penetration vary.

6.2 Future work

The survey yielded preliminary results regarding customer awareness of and behaviour regarding internet banking security; some of these findings will be addressed in future phases of the research in order to extend the understanding of this issue.

As for the inadequacy of customer awareness of internet banking security, it is necessary to find and quantify the factors that may affect the level of customer awareness of internet banking security in order to generalise the findings. As for the need to improve customer security awareness and behaviour, workable solutions that take account of all factors should be designed and put forward. A set of criteria to evaluate the effect of these solutions on customer awareness and behaviour is also needed. As for the expanded model of customer awareness and behaviour of internet banking security, a thorough investigation is needed to quantitatively examine the role of each factor, and verify the relationships among all the factors.

REFERENCES

ABA. (2014). ABA Survey: More Consumers Embracing Mobile Banking. Retrieved from http://www.aba.com/Press/Pages/082014ConsumerSurveyMobileBanking.aspx

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432-445.

Barriball, K. L., & While, A. (1994). Collecting Data using a semi-structured interview: a discussion paper. Journal of advanced nursing, 19(2), 328-335.

Bernard, H. R. (1988). Research methods in cultural anthropology: Sage Newbury Park, CA.

Bryant, T., Hughes, J., Myers, M. D., Trauth, E., & Urquhart, C. (2004). Twenty Years of Applying Grounded Theory in Information Systems: A Coding Method, Useful Theory Generation Method, or an Orthodox Positivist Method of Data Analysis? Information Systems Research (pp. 649-650): Springer.

Bryman, A. (2004). Triangulation and measurement. Loughborough University, Department of Social Sciences, United Kingdom.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Burck, C. (2005). Comparing qualitative research methodologies for systemic research: The use of grounded theory, discourse analysis and narrative analysis. Journal of Family Therapy, 27(3), 237-262.

CNNIC. (2014). Statistical Report on Internet Development in China. Retrieved from http://www1.cnnic.cn/IDR/ReportDownloads/201411/P020141102574314897888.pdf

Cohen, D., & Crabtree, B. (2006). Qualitative research guidelines project. Retrieved from http://www.qualres.org/

Conner, M., & Armitage, C. J. (1998). Extending the theory of planned behavior: A review and avenues for further research. Journal of applied social psychology, 28(15), 1429-1464.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, 20(1), 79-98.

Daniel, W., William, K., Ling, M., Lai, S., & Tevanotai, A. (2014). Awareness in e-Banking Security and usage. Paper presented at the Information Science, Electronics and Electrical Engineering (ISEEE), 2014 International Conference on.

FFA. (2014). Fraud the Facts 2014. Retrieved from http://www.financialfraudaction.org.uk/download.asp?file=2796

Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. Logistics Information Management, 15(5/6), 352-357.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. Computers & Security, 25(1), 27-35.

Glaser, B. G. (1992). Emergence vs forcing: Basics of grounded theory analysis: Sociology Press.

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The discovery of grounded theory; strategies for qualitative research. Nursing Research, 17(4), 364.

Hentea, M., Dhillon, H., & Dhillon, M. (2006). Towards changes in information security education. Journal of Information Technology Education: Research, 5(1), 221-233.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

Howcroft, D., & Hughes, J. (1999). Grounded Theory: I mentioned it once but I think I got away with it. Paper presented at the Information Systems–The Next Generation. Proceedings of the 4 th UKAIS Conference. York UK. pp129-141.

Li, A. (2014). Real Life Examples of Online Scams and Fraud in China. Retrieved from https://www.chinacheckup.com/kb/explanations/examples-online-scams-fraud-china

Lings, B., & Lundell, B. (2005). On the adaptation of Grounded Theory procedures: insights from the evolution of the 2G method. Information Technology & People, 18(3), 196-211.

Ma, Z. (2012). Assessing serviceability and reliability to affect customer satisfaction of internet banking. Journal of Software, 7(7), 1601-1608.

Martin, P. Y., & Turner, B. A. (1986). Grounded theory and organizational research. The Journal of Applied Behavioral Science, 22(2), 141-157.

Matavire, R., & Brown, I. (2008). Investigating the use of grounded theory in information systems research. Paper presented at the Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology.

Myers, M. D., & Avison, D. (1997). Qualitative research in information systems. Management Information Systems Quarterly, 21, 241-242.

Mylonas, A., Gritzalis, D., Tsoumas, B., & Apostolopoulos, T. (2013). A qualitative metrics vector for the awareness of smartphone security users Trust, Privacy, and Security in Digital Business (pp. 173-184): Springer.

NIST, S. (1998). 800-16 (1998). National Institute of Standards and Technology (NIST) information technology training requirements: A role-and performance-based model (NIST Special Publication 800-16). Washington, DC: US Department of Commerce.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on amazon mechanical turk. Judgment and Decision making, 5(5), 411-419.

Puhakainen, P., & Ahonen, R. (2006). Design theory for information security awareness. working paper, Faculty of Science, University of Oulu, Finland.

Rowe, B. R., Pokryshevskiy, I. D., Link, A. N., & Reeves, D. S. (2013). Economic Analysis of an Inadequate Cyber Security Technical Infrastructure. National Institute of Standards and Technology Planning Report, 13-11.

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.

Shepherd, L. A., Archibald, J., & Ferguson, R. (2013). Perception of risky security behaviour by users: Survey of current approaches Human Aspects of Information Security, Privacy, and Trust (pp. 176-185): Springer.

Silva, L., & Backhouse, J. (2003). The circuits-of-power framework for studying power in institutionalization of information systems. Journal of the Association for Information Systems, 4(1), 14.

Siponen, M. (2001). Five dimensions of information security awareness. Computers and Society, 31(2), 24-29.

Tariq, M. A., Brynielsson, J., & Artman, H. (2014). The security awareness paradox: A case study. Paper presented at the Advances in Social Networks Analysis and Mining (ASONAM), 2014 IEEE/ACM International Conference on.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. Information management & computer security, 6(4), 167-173.

Valentine, J. A. (2006). Enhancing the employee security awareness model. Computer Fraud & Security, 2006(6), 17-19.

Varian, H. R. (2000). Managing Online Security Risks. Economic Science Column, The New York Times.

Waly, N., Tassabehji, R., & Kamala, M. (2012). Improving organisational information security management: The impact of training and awareness. Paper presented at the High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS).