Association for Information Systems
AIS Electronic Library (AISeL)

WHICEB 2015 Proceedings | Wuhan International Conference on e-Business

Summer 6-19-2015

Customer Awarenessof Internet Banking Security in China

Ruilin Zhu

Information Systems & Operations Management Department, The University of Auckland Business School, Auckland, New Zealand 1010, ruilin.zhu@auckland.ac.nz

*Customer Awarenessof Internet Banking Security in China

Ruilin Zhu[1]

[1]*Information Systems & Operations Management Department, The University of Auckland Business School, Auckland, New Zealand 1010*

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 of internet banking security in China. This paper presents the findings of a research conducted to evaluate current levels of customer awareness of internet banking security. Some of the findings raise implications which call for further investigation.

Keywords: customer awareness, internet banking, security, survey

1. INTRODUCTION

Internet banking is now widespread around the world due to its convenience and low cost. As banks go all out to publicize internet banking, more and more customers are attracted to use this service. According to an August 2014 survey of US customers by ABA (American Bankers' Association), internet banking remains America's most popular banking method with 31% preference (ABA, 2014). The same pattern has been seen in China, where by the end of June 2013, the number of internet banking customers in China had reached 240 million, up 9% since last year (CNNIC, 2013).

In their desire to provide reliable and trustworthy service, the security issues surrounding Internet banking have always been the first 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.

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 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 such fraud totaling over RMB 42 million, 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 (Chen, Shaw, & Yang, 2006). Improving the awareness of security is consequently viewed as equally if not more important than technological solutions (S. Timms, 2004).

Many studies have addressed this concern. However, almost all of these researches discuss employee security awareness in organizations; few have been conducted toanalyse customer awareness of internet banking security. In particular, as China is more severely plagued by the online scams and frauds, the internet banking is more likely to be attacked. Therefore it is high time that we should closely examine the current security situation in China.

* Corresponding author.Email: ruilin.zhu@auckland.ac.nz

Since few researches have so far focused on security awareness in internet banking, we do not possess adequate information about current levels of customer awareness of Internet banking security. Accordingly, it was decided to take a first step to investigate the issue by conducting a survey to look into customer security awareness.

The remainder of the paper is organized as follows. Section Two starts with the literature review and specifies the research questions, and the research method is presented thereafter in Section Three. We summarizes our findings and discussions in the following sections, which are followed by a conclusion.

2. LITERATURE REVIEW

The concept of security awareness arises from the process of technological advances, which are featured with three-stage of development(Thomson & von Solms, 1998). With the introduction of the personal computer and the increasing complexity and reliability of information technology, the information systems have become the indispensable part of daily operations with the profile of the end-users diversifying. In this regard, it is necessary to implement security awareness education for all users who are able to get access to the information. This is echoed with a series of conceptual studies (S. Furnell, Gennatou, & Dowland, 2002; Hentea, Dhillon, & Dhillon, 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, Hovav, and Galletta (2009) suggested that organizations can adopt user awareness of security policies as one of the three security countermeasures to reduce the information systems misuse. As a complement, Bulgurcu, Cavusoglu, and Benbasat (2010) conducted an empirical exploration that analyzed the roles of information security awareness on an employee's compliance behaviour.

The researchers interested in this topic have mainly focused on the organizational 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 organizational and societal levels, but the user dimension of the problem is nonetheless neglected (S. M. Furnell, Jusoh, & Katsabas, 2006; Herath & Rao, 2009). As a result, Tariq, Brynielsson, and Artman (2014) call for the studies that examine the issue from an individual perspective.

In order to address this concern, many researches have been advanced. However, almost all of these researches are discussed in the context of employee security awareness(Shaw, Chen, Harris, & Huang, 2009; Valentine, 2006), while few researches (until quite recently) have been conducted to analyze the customer awareness for a certain device/service, for instance, smart phone(Mylonas, Gritzalis, Tsoumas, & Apostolopoulos, 2013) and internet banking(Daniel, William, Ling, Lai, & Tevanotai, 2014).

The most obvious difference for them lie in the role of end user. In organizations, the users are employees, who are "required" to enhance the level of security awareness, while as for the case of internet banking, the users are customer, 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 for internet banking setting. In addition, the extant researches are inconsistent rather than systematic, and their findings are sporadic and patchy. They merely listed their results instead of analyzing them. Moreover before delineating the security awareness in full details and understanding them in depth, they made a series of concrete recommendations, which hence are very limited in their effectiveness.

In general, as not possessing adequate information about the situation of customer awareness of internet banking security, we decide to take a first step to investigate the issue by conducting a survey to look into customer security awareness. The question generally relates to what is the current situation of customer

awareness of internet banking security – what and to what extent they have known about relevant information, and how they obtained it.

3. METHODOLOGY

3.1 Method

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 awareness presentation is simply to focus attention on security. Awareness presentations are intended to allow individual to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information” (NIST, 1998).

The definition 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’ knowledge of security and their attitudes towards security issues.The nature of the definition, therefore, fits well with the qualitative research, which aredesigned to help researchers understand people and the social and cultural contextswithin which they live(Myers & Avison, 1997). As a result, we 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. We conducted a 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 will help us assess the appropriateness of current internet banking security strategy, particularly in regard to human factors and potential frauds aimed at customers. Secondly, knowing more about customers’ habits and experiences will help us determine why current strategy is successful or unsuccessful.

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 experience of internet banking.

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

Semi-structured interviews were selected as the means ofdata collection due to two primary considerations. First, they are well suited for the exploration of theperceptions and opinions of respondents regarding complexand sometimes sensitive issues and enable probingfor more information and clarification of answers(Louise Barriball & While, 1994).Then according toBernard (1988), it is best used when the researcher will not getmore than one chance to interview the subject and when the researcher will be sending severalinterviewers out into the field to collect data.The semi-structured interview guide provides a clear set of instructions for interviewers andcan provide reliable, comparable qualitative data(Cohen D, 2006).The inclusion of open-ended questions provide the opportunity foridentifying new ways of seeing and understanding the topic

at hand. Finally the varied professional, educational and personal historiesof the sample group precluded the use of a standardizedinterview schedule.

3.2 Subject selection

Subjects were all the current internet banking users of one local bank in China, who were roughly categorized 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 we want to clarify here is that we intentionally chose the subjects with IT background as in the real life, they are facing internet banking attack as well. In addition, a general sample make our research more authenticate and reliable.

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. We identified the potential subjects after they finalized their own internet banking related transactions at the teller-counters, and then we invited them to participate into this activity by specifying the research target and nature. If they agreed to our request, we led them to a near-by 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. Section1, 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 we moved to the interview part, which typically lasted for another 30 minutes.

3.4 Data analysis

We 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 Q2, in order to examine any differences in their responses.The purpose of this research is to explore the situation of customer awareness of security. The exploratory nature of the research question and the understanding-of-a-situation objective required an in-depth qualitative data analysis method to generate results. We hence employed the grounded theory to analyze the data.

Grounded theory is a qualitative research method that seeks to develop theory that isgrounded in data systematically gathered and analyzed. It has become increasing popular in information systems domain(Bryant, Hughes, Myers, Trauth, & Urquhart, 2004; Howcroft & Hughes, 1999; Lings & Lundell, 2005). According toMartin and Turner (1986), grounded theory is 'an inductive, theory discovery methodology that allows theresearcher to develop a theoretical account of the general features of a topic while simultaneouslygrounding the account in empirical observations or data'. Grounded theory has proved to be extremely useful in developingcontext-based, process-oriented descriptions and explanations of information systems phenomena(Myers & Avison, 1997).

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 the internet banking security awareness in China, it is of appropriateness for us to adopt this method. Moreover, in order to conduct the grounded theory research, scholars should not start with some pre-conceived concepts, which must emerge from the data (Matavire & Brown, 2008). As we do not possess any further understanding towards this topic, this rule is therefore satisfied.

I started the analysis as soon as the data was being collected. Following the principle of constant

comparison (Glaser, Strauss, & Strutzel, 1968), I systematically compared each new data to former ones, where the main purpose is 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 us better understand the issues surrounding customer security awareness.

(1) 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.

(2) 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 these 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.

(3) 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.

(4) 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 may 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.

(5) The current security information is not very useful

Among those subjects who said they would actively seek security information, only 32.6% thought this information is usually “quite useful” compared with 50% who said it is “somewhat useful” and 17.4% who found it “rarely useful”. Some subjects complained in the interviews that they never get any information about internet banking security from the bank – just literature promoting the bank’s products.

(6) Each channel has its own advantages for customers

According to the survey (See Figure 1), 40.5% of subjects prefer to go to a website to find out about the security of online banking before setting up an internet banking 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.

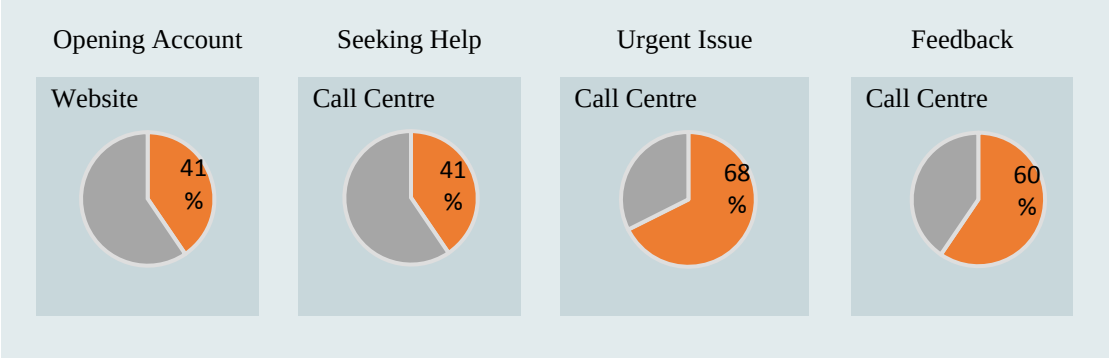

Figure 1 Channels

(7) The utilization of advanced devices 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 supposed to be as safe as a digital certificate.

(8) Brief summary

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

5. DISCUSSION

There are several important implications stemming from the survey that may add to our understanding of customer awareness of internet banking security in China.

(1) Inadequacy of customer security awareness

According to the survey, current customer awareness of internet banking security is inadequate. There is a sharp contrast between customers' keen concern about the security of internet banking on the one hand and their lack of basic knowledge on the other – they do not know enough about internet banking security to protect themselves from attacks, nor do they know how to get the relevant information from their bank.This inadequacy may well lead to the erosion of trust in internet banking security, and make internet banking fraud more likely.

(2) Inadequacy of bank activity

The survey highlighted two obvious ways in which the banks' response is inadequate. The current information being offered about internet banking security does not satisfy customers. Secondly, the banks are not conducting a systematic or organized programme of activities to raise the security awareness of their customers. This is the direct cause of poor security awareness among customers. Banks should take a more active role in optimizing their delivery of customer security awareness.

(3) Inadequacy of internet banking security strategy

For banks, the chief change in the transfer from traditional banking to internet banking lies in the shift from "product-oriented" to "customer-oriented" service (Sciglimpaglia & Ely, 2002). This is underlined in the fact that, in terms of security management, human factors have become more important than the technology (Desman, 2003). However, the fact that a large proportion of existing internet banking customers lack basic

knowledge about security suggests that the customers' importance in security has been valued. Furthermore, banks expect to achieve security simply by utilizing advanced devices, regardless of whether these are convenient for customers to use. This is another fundamental reason for the inadequacy of customer security awareness.

(4) Importance of customer awareness for internet banking security

Communication between banks and customers now relies on a range of channels: not just bricks and mortar branches but also official websites, call centres and other portal terminals. This means many of the traditional methods of enhancing customer awareness, such as a discussion forums, risk awareness events, newsletters and articles, management centres etc., are no longer suitable. Furthermore, customers may only be willing or able to invest limited time and effort in gathering security related information from these channels. Each channel has its advantages. The current low level of security awareness is probably due to the disproportionate utilization of these communication channels.

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 willing to scam. The same benefits that customers enjoy can also be shared with those wanting to compromise. 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 full consideration.However, the survey 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, banks are failing to deliver effective programs to raise customer awareness of internet banking security. This also needs to be addressed, and banks' strategy adjusted accordingly.

The survey identifies several key issues in terms of customer awareness of internet banking security. These concern the role of customers, the range of communication channels, and the time customers are willing to devote to security issues through these channels. These factors affect the appropriateness and effectiveness of the banks' customer security awareness measures, and should be thoroughly investigated.

The research does have some limitations. Firstly, the number of subjects is not large enough, which may affect the generalization of the findings. We therefore plan to conduct a survey with Amazon Mechanical Turk, which should provide a larger sample covering a range of demographic characteristics (Paolacci, Chandler, & Ipeirotis, 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 of internet banking security. This also calls for deeper exploration. Finally, the survey was conducted in a western city in 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 internet banking security; some of these findings will be addressed in future phases of the research in order to extend our 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 generalize the findings. As for the need to improve customer security awareness, 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 is also needed.

ACKNOWLEDGMENTS

The author thanks Mr. Ho Wai Chong for his great support with the survey and helpful advice on this paper. I would also like to thank all the participants of the survey for their invaluable feedback.

REFERENCES

ABA. (2014). Internet remains top banking method, but branches gain popularity.

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.

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.

Chen, C. C., Shaw, R., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: a case study of an information security awareness system. *Information Technology Learning and Performance Journal, 24*(1), 1.

CNNIC. (2013). Statistical Report on Internet Development in China.

Cohen D, C. B. (2006). Qualitative Research Guidelines Project.

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.

Desman, M. B. (2003). The ten commandments of information security awareness training. *Information Systems Security, 11*(6), 39-44.

FFA. (2014). Fraud the Facts 2014.

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.

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.

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

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.

S. Timms, C. P., and A. Beard. (2004). Information security breaches survey 2004.

Sciglimpaglia, D., & Ely, D. (2002). *Internet banking: A customer-centric perspective.* Paper presented at the System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on.

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.

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*.