Towards a Heuristic Model for Usable and Secure Online Banking

Mathias Mujinga
University of South Africa, mujinm@unisa.ac.za

Jan Kroeze
University of South Africa, jan.kroeze@gmail.com

Mariki Eloff
University of South Africa, eloffmm@unisa.ac.za

ACIS 2013
RMIT MELBOURNE

Information Systems: Transforming the Future

24th Australasian Conference on Information Systems, 4-6 December 2013, Melbourne

Proudly sponsored by

nab
ACIS 2013 Principal Sponsor

RMIT UNIVERSITY

CITRIX®

GS1® Australia

acs AUSTRALIAN COMPUTER SOCIETY

ACS Foundation
Advancing ICT through Education and Research

ACPHIS

AAIS
Australasian Association for Information Systems

Towards a Heuristic Model for Usable and Secure Online Banking

M Mujinga
School of Computing
University of South Africa, South Africa
Email: mujinm@unisa.ac.za

MM Eloff
Institute for Corporate Citizenship
University of South Africa, South Africa
Email: eloffmm@unisa.ac.za

JH Kroeze
School of Computing
University of South Africa, South Africa
Email: kroezjh@unisa.ac.za

Abstract

The main purpose of this paper is to propose a heuristic model for usable and secure online banking. The model is based on identified heuristics that contribute to the design of usable security in the context of online banking security. Little research has focused on the balance between usability and security in online banking authentication mechanisms when evaluating the effectiveness of security systems. Nielsen's ten usability principles are still important in designing usable secure systems, as indicated by the analysis of heuristics developed from recent studies. Online banking users are vulnerable to numerous old and new online security threats that target this group of users. An investigation into the usability of aspects of security design can benefit both online bankers and users in fostering a secure and usable banking environment. In this paper, we report on a work in progress that intends to develop a heuristic model for usable online banking security design. Going forward we intend to refine the model by collecting survey data from online banking users in South Africa and interviews with bank security personnel.

Keywords

Interpretivist, heuristic model, mixed methods, online banking, online banking security.

INTRODUCTION

Online security is a major concern for organizations and their clients who conduct business online. Banking institutions and e-commerce companies, such as Amazon and Yahoo, found that internet security is a major challenge for online business (Aladwani 2001; Luftman et al. 2005; Luftman and Ben-Zvi 2010; Bisong and Rahman 2011). Lack of trust and perceived (security) risk are major concerns for consumers adopting online purchasing and doing online banking (Sathye 1999; Aladwani 2001; Cheung et al. 2003; McCole et al. 2010; Nepomuceno et al. 2012).

Security design plays a major role, especially in applications where security is not the primary production task. Flechais et al. (2007) highlight the importance of usable security integration into the requirements and the design process. Design flaws in the usability of Microsoft Word security highlight this difficulty (Furnell 2005). MS Word lacks clear visibility for discovering its security tools, and it lacks explanation on how security tools are used to achieve specific security goals. In addition, previous studies highlighted the importance of education and training through information security awareness programs in shaping users' security behaviour (Thomson and von Solms 1998; Furnell et al. 2002; Leach 2003; Hentea 2005; Shaw et al. 2009; Puhakainen and Siponen 2010; Bulgurcu et al. 2010). In particular, ignoring human limitations in the design of security systems result in non-compliance to security requirements (Whitten and Tygar 1999; Perrig and Song 1999; Sasse et al. 2001). Emotions play a role in how users interact with information systems, and designers of information systems need to consider emotions (Peter and Beale 2008; Lim et al. 2008). Therefore it is recommended to take human limitations such as limited memory-load capability (Paas et al. 2003; Sasse et al. 2001) and human emotions into account in information system design, since the contents of people's knowledge, including their theories and beliefs, can be an important explanatory concept for understanding users' behavior in relation to systems (Payne 2009).

Achieving total security is impossible (Myles et al. 2003; ISO/IEC 2005; Dlamini et al. 2009). Human users have long been regarded as the weakest link in the security chain of information systems (Schneier 2000; Mitnick and Simon 2005; Huang et al. 2007). However, even with the best technical security mechanisms a system's weakest link tends to be the human user (Bishop 2012). The main challenge is obtaining the user buy-in to perform security tasks and embedding their behaviour into a secure culture and environment (Guo et al. 2011).

In this paper we agree with Whitten and Tygar (1999) who argued that general usability principles for interface design are not adequate to cater for the design of usable security. But general usability principles are the starting point for designing usable security. The nature of online banking makes it important to address its usability problems differently from other security systems since a breach in security may result in greater financial loss to organizations and individual users alike. We argue that the technical security aspects for protecting online banking systems can provide sufficient protection. The problem is the mismatch of expectations between the user and the system. There is a gap between system expectations of users and what users can actually do with regard to security – users do not have single model of security. We intend to find design principles that address these disparate online banking security system expectations together for a secure and usable system. The purpose of this paper is to propose a heuristics that can improve security of online banking. The model will provide design principles that assist in designing security systems (websites) that provide a secure and usable online banking environment, by addressing users' and developers' expectations.

This paper is organised as follows: First, the research problem is presented, followed by the research objectives and the research design to be used to address the research problem. The intended use of the mixed methods approach is then discussed, followed by an explanation and defence of the proposed heuristic model, and, finally, the conclusions of the paper.

ONLINE BANKING SECURITY

Online security is a subset of computer security. Internet computer security is important because technical reports compiled by security, risk and insurance organizations show that hackers and attackers target internet organizations, in particular small firms (Cashell et al. 2004; Panda Security 2010; Symantec 2013). Other popular targets are firms that store credit card numbers; today one can even buy a credit card number on the internet (Buck 2013; Cessna 2013). According to AON (2013) South African businesses are unprepared for the growing risk of cyber attacks. Online banking, also known as electronic banking (e-banking) or internet banking, is the functionality provided by banking institutions to enable bank clients to conduct banking transactions over the internet. Online banking can be conducted through a variety of devices and mediums. When a customer uses a cellphone or other mobile device, the terms are specifically mobile banking, m-banking, or cellphone banking. In this paper, the concern is mostly with online banking, which involves a customer visiting an online banking website to log in and conduct banking-related functions. The user can use any type of device, be it a mobile device or a personal computer.

Online banking users can conduct a variety of transactions, such as checking account balances, funds transfer between accounts, beneficiary payments, bill payments, prepaid services payments (electricity, airtime, etc.), traffic fines payments, and money-sending services. While appreciating the benefits that accompany online banking, users fail to realise that there are also responsibilities which are part and parcel of the service. There seems to be a lack of clarity on exactly what are the responsibilities of the user and banks in case of an online security breach. In the United States (US) banks are liable to breaches on personal accounts, while businesses carry higher liability on business accounts. Recent cases in the US provide conflicting outcomes on financial loss liability (Electronic Code of Federal Regulations-Part 205 2013). For instance, users carry a major part of the responsibility when it comes to security, and banks are not always liable for cyber attacks that steal a client's online login credentials, as shown by a recent legal judgement (Kitten 2011). Many such cases of online banking security breaches are now ending up in the courts of law to decide where the blame lies and precedents are being set (Beyli 2007; Kitten 2011; Vaas 2012; IOL 2013a, 2013b). In South Africa the lines of responsibility and accountability are not clear. In two recent cases (IOL 2013a; IOL 2013b) the bank refused to take full responsibility and only reimbursed half of the amount lost in one case, citing that the user has been negligent in being a victim of a phishing attack. In both cases the mobile service provider refused any liability after performing a Subscriber Identity Module (SIM) swap without proper identification of the customer (IOL 2013a; IOL 2013b).

Security of online banking has been a topic of discussion from the time the service was just a concept. Understandably, banks often are reluctant to disclose security and privacy breaches, but governments are now passing laws that oblige financial institutions to disclose such breaches (Romanosky et al. 2011). Over time, governments have enacted laws that mandate organizations, private and public alike, to disclose any breaches to their clients (Schwartz and Janger 2007), since most breaches affect the security and privacy of individuals negatively. Furthermore, there is a trade-off between security and usability, in which humans try to minimise mental effort, whilst maintaining an acceptable level of performance (Besnard and Arief, 2004).

Electronic commerce (e-commerce) relies heavily on the reliability and security of electronic payments systems of which online banking is at the core. Information systems are best protected by incorporating security from the early stages of design onwards (Sasse and Flechais 2005; Siponen et al. 2006; Flechais et al. 2007; Jones and Horowitz 2012; McKay et al. 2012; Mouratidis et al. 2012; Schneider et al. 2012). On the other hand, for systems to be used effectively, they need to be usable (Cranor and Garfinkel 2004). Often, usability and security are at odds and trade-offs need to be made (Schultz 2001; Cranor and Garfinkel 2004; Besnard and Arief 2004; Kainda et al. 2010). Common ground therefore needs to be found between security and usability, starting with security designers finding a balance between business enablement and protecting an organization's valuable assets. This can be achieved by mapping the risk to assets and the usability of the systems protecting the assets. At the core of this trade-off is the need to communicate risks to users and to understand the users' needs with regard to performing security tasks, so that security solutions are achieved in context. Therefore, security mechanisms need to be understood by users, to allow effective use and, by extension, protect business-critical assets. In the context of online banking, usable security systems can benefit both the banker and the user.

The internet brought about significant changes in business models for organizations through e-commerce and it has also provided banks' clients with alternatives ways of conducting banking transactions (Steinfield, 2002). Online banking has allowed banks to gain competitive benefits, reduce operational costs and enhance their performance (Hutchison and Warren 2003). Privacy and security of online banking transactions and confidentiality of personal information are among the biggest concerns for both the banking institutions and online banking users (Hutchison and Warren 2003).

USABLE SECURITY

Usability is "*the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component*" (IEEE Std. 610.12 1990). Usability design depends on the combination of the nature of the user, the task and the environment in which the task will be enacted (ISO/IEC 9126-1 (2001). In this section, the material that forms the basis of the proposed model is discussed. First contact with online banking is through the bank's login website. Therefore, usability of the website interface is important in creating a usable and secure system. Starting with general interface design principles, Shneiderman and Plaisant (2010) developed general principles for user interface design of human-computer interaction (HCI). Shneiderman and Plaisant (2010)'s 'eight golden rules' for interface design also guide the selection of the proposed heuristics in the model. The effects of emotions in HCI, specifically the designing for pleasure and enjoyment also help in improving the usability of an information system, since the increasing use of technology occurs in a multitude of places (Monk et al. 2002).

Online banking also needs to address these aspects of usability for users to find enjoyment and pleasure when using the system. The realisation that usability, on its own, does not guarantee effective use of a service or product gave birth to the term "user experience" (UX). ISO FDIS 9241-210 (2009) defines UX as "*perceptions and responses that result from the use or anticipated use of a product, system or service.*" UX is the momentary, primarily evaluative feeling one gets while interacting with a product or service, this feeling can either be good or bad (Hassenzahl 2008). UX is subjective and involves all aspects of the user before, during and after use (Hassenzahl et al. 2006). UX is influenced by three factors – system, user and usage context (ISO FDIS 9241-210 2009). Aspects of UX, including definition, measurement metrics and measurement methods have no agreed heuristics or best practices (Law et al. 2009). Generally, usability and UX need to be addressed since there is an overlap between the two HCI aspects (Hassenzahl et al. 2006). Therefore, there is need to address UX in the context of online banking.

Early usability studies focused on usability heuristics of general information systems, treating all information systems the same (Nielsen and Molich 1990; Molich and Nielsen 1990; Nielsen 1994a; Nielsen 1995a; Shneiderman and Plaisant 2010). As usability researchers and practitioners gained more insight into usability issues, specific systems contexts were deemed important. While some studies looked at principles and methods for the design of usable security (Sasse and Flechais 2005; Flechais et al. 2007), some looked at the successful design of secure information systems (Yee 2002; 2004; Johnston et al. 2003; Katsabas et al. 2005; Siponen et al. 2006), and others investigated secure design of specific information systems (Yeratziotis et al. 2012). A number of security design principles have been identified in literature for improving security systems design for specific systems (Sasse, Brostoff and Weirich 2001).

An online banking system for a specific bank is designed to cater for all clients of the bank, and the security settings do not provide for personalization and customization. Given the diversity in bank's clients in terms of language, culture and age, it is inevitable that there exists a variety of mental models that users create about the system. In South Africa, for instance, there are eleven official languages and even more cultures, but banks do not cater for all languages on online banking website. Three of the four major banks use only English for online banking, while the other major bank cater for both English and Afrikaans. However all banks provide telephonic assistance in all eleven official languages. Security is complex without including any dimensions such as language and their introduction is going to make it even more complex.

RESEARCH DESIGN

The security problem affects the researched banking organizations, the security personnel of banks, and the banks' clients. Online banking users come from varying backgrounds, such as different languages, culture, age, and sex. We posit that this diversity corresponds to a possible existence of multiple realities, which aligns with the qualitative research approach (Given 2008). Given points out that qualitative research is not designed to prove something, but to generate understanding – of which the researcher brings only one perspective of the phenomenon under study. Therefore, in this research work, the interpretivist approach has been chosen as an appropriate philosophical guide, as this allows for input from all participants to the phenomenon under study. Interpretive researchers assume that access to reality is through social constructions such as consciousness, language, shared meanings and instruments; therefore, the phenomenon under study is understood through meanings people assign to them (Myers 2009). These meanings can only be obtained by interacting with the participants while looking from the inside. Interpretive researchers also tend to focus on meaning in context, which is usually the socially constructed reality of the people under study (Myers 2009). Saunders et al. (2009) further state that interpretivism advocates that the researcher needs to understand the differences between humans as social actors – and that is the difference between conducting research on people, as opposed to other artificial objects. Locke (2001) describes interpretive (and related constructivist) paradigms as having an interest in understanding the world as viewed by those that who live in it; hence, the concern is with a subjective reality. The online banking security problem should be investigated by engaging those participating in the environment, namely, users and system developers.

There are mainly two research approaches – deductive and inductive. The deductive approach is an inquiry which assumes that a well-established theory or hypothesis is generated before the collection of research data (Saunders et al. 2009), such as a research inquiry to test a theory. In contrast, an inductive approach undertakes to generate a theory through the collection of research data (Saunders et al. 2009). The mixed methods design used in this study suggests that both approaches will be used, with more emphasis on the inductive approach. The deductive approach is used to refine themes for testing, using the inductive approach, achieved by using user questionnaire data as input for engaging with security system developers.

Mixed method research can be used for a variety of purposes in a research study. Venkatesh et al. (2013) suggest the following purposes for using mixed methods: complementarity, completeness, developmental, expansion, corroboration/confirmation and diversity. Completeness allows researchers to have a complete picture of the phenomenon under study, by looking at it from different lenses. A developmental approach, on the other hand, is predominant in sequential mixed methods, where questions for one strand emerge from the inferences of the other strand (Venkatesh et al. 2013). In this research study, mixed methods are used, for both completeness and developmental purposes. A complete picture of the phenomenon is obtained by investigating the online banking security problem from both perspectives of the users and system developers. The developmental nature of the design is achieved by using findings in the qualitative strand to enhance the qualitative strand. That is, principles for evaluation by the heuristic evaluation method are refined based on users' questionnaire analysis.

PROPOSED HEURISTIC MODEL

This section reviews previous studies in literature on usable security, and then proposes the heuristic model principles for online banking security. The Oxford Dictionary (2004) defines a heuristic as "*enabling a person to discover or learn something for themselves.*" Heuristics are usually used to represent features or aspects of the real world, for easier comprehension of the problem at hand.

Usability became an issue from the early 1990s onwards, and since then a number of usability-inspection methods have been identified, and numerous usability studies have been conducted. Among these methods, the main four identified back then were formal usability inspections, cognitive walkthrough, pluralistic usability walkthrough, and heuristic evaluation (Mack and Nielsen 1994), and they are still being used today. Nielsen and Molich (1990) defined heuristic evaluation method as follows: *"Heuristic evaluation is an informal method of usability analysis where a number of evaluators are presented with an interface design and asked to comment on it."*

Table 1: Online Banking Heuristics

No.	Principle	Online Banking Description	Nielsen (1995a)	Yee (2002; 2004)	Johnston et al. (2003)	Katsabas et al. (2005)	Shneiderman and Plaisant (2010)	Yeratziotis et al. (2012)
1	User control	Users should have the freedom to customise the interface, including security features, and provide a clearly marked reset to default settings button. This allows the user to be aware of the level of security, rather than security by obscurity.	✓	✓	✓	✓	✓	✓
2	Visibility	The interface should keep users informed about the system connection status and their level of security protection status.	✓	✓	✓	✓		✓
3	Errors	Provide users with detailed security error messages without codes, and then enable recovery through simple mechanisms.	✓		✓	✓	✓	✓
4	Help and documentation	Provide users with assistance on ways to use the service and security features.	✓			✓	✓	✓
5	User suitability	The system should provide enough information for novice users, while not providing too much information for experienced users.	✓			✓	✓	✓
6	Learnability	Ensure that security actions are easy to learn and remember. Therefore, it is important for the system to be as user-friendly and as easy-to-learn as possible.	✓		✓		✓	✓
7	Aesthetic and minimalist design	The interface and dialogue should contain only relevant system and security information. No inappropriate advertisements.	✓		✓			✓
8	User language	The system should speak the users' language, and avoid system-orientated terms following real-world conventions.	✓			✓		✓
9	Revocability	Allow the user to easily revoke previous security actions, whenever possible.		✓			✓	✓
10	Satisfaction	The system should ensure that users' experience with the service and security features is pleasant and satisfying; otherwise, they might be tempted to bypass security features altogether.			✓			✓
11	Clarity	Inform users about the consequences of any security-related actions before the action is taken. Especially irreversible actions must be clearly marked – e.g. paying into an incorrect beneficiary's account.		✓				✓
12	Path of least resistance	The system should require minimal effort in order to make use of security features.		✓		✓		
13	System protection	The interface must provide an unspoofable communication channel between the user and system entities, through core principles of information security confidentiality, integrity, availability, authenticity, non-repudiation and privacy.		✓				✓
14	Consistency	Do not make users wonder whether different situations, words, or actions mean the same thing. Follow standard conventions across platforms.	✓				✓	
15	Minimum authentication delay	By designing the application carefully, the system should provide minimum delay in authenticating users.				✓		
16	Security and privacy	The system should provide confidentiality, integrity availability and privacy.						✓

Usability testing can be a costly exercise; therefore, inspection methods that are more informal and less expensive tend to be more popular; heuristic evaluation falls into that category. The method involves developing usability principles (heuristics), also referred to as 'rules of thumb', that usability expert evaluators analyse for effectiveness in improving an application, or user interfaces' usability, and the severity of each usability problem is noted (Nielsen and Molich 1990; Mack and Nielsen 1993; Nielsen 1994b). Heuristic evaluation is regarded as a less expensive method, and it provides an effective way of identifying usability problems earlier in the development process of a user interface (Hollingsed and Novick 2007). Table 1 lists preliminary heuristics, their respective descriptions in the context of online banking, and sources previously highlighted the need to address the heuristic. The heuristics are listed in order of frequency appearance in literature and it combines usability and security heuristics. Nielsen's ground-breaking usability heuristics form the basis of most heuristics later developed in the areas of usability and usable security.

The heuristics in Table 1 will be evaluated in follow-up work, using checklist items based on a severity scale illustrated in Table 2. The model will be evaluated by the field experts, through a heuristic evaluation assessment tool with an extensive checklist for the evaluation of the heuristics, based on a checklist severity scale proposed by Nielsen (1994a) and shown in Table 2. Using a checklist for heuristic evaluation, similar to that developed by Pierotti (2007) for the ten usability heuristics of Nielsen (1995a), the heuristic model will be evaluated, using the severity scale:

Table 2: Usability Severity Rating Scale (Nielsen 1994a)

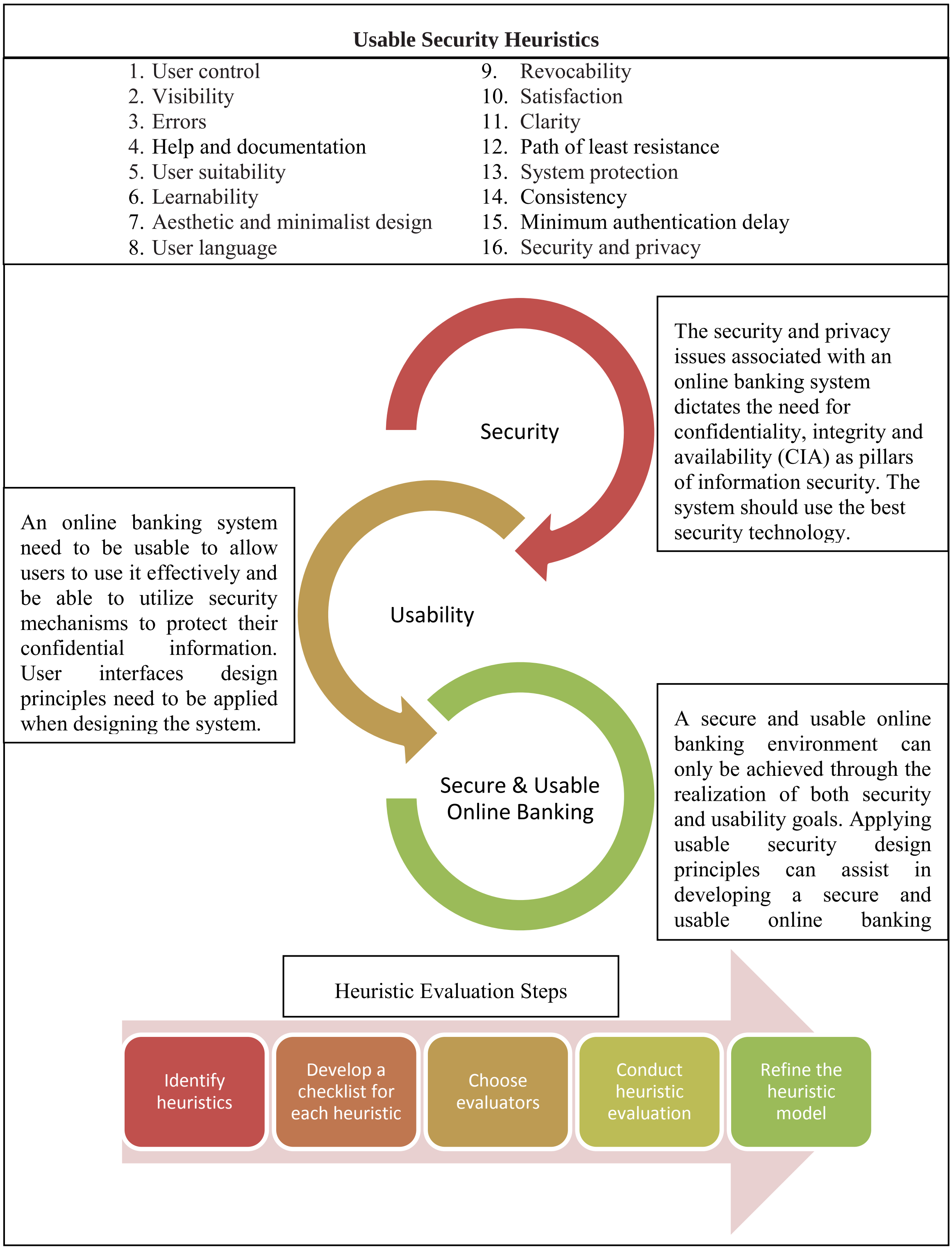
Rating	Description
0	Does not explain the problem at all.
1	May lightly address aspects of the problem.
2	Explains a small part of the problem, but there are major aspects still unexplained.
3	Explains a major part of the problem, but there are some aspects still unexplained.
4	Fairly complete explanation of why this is a usability problem, but there is still more to the problem.
5	Complete explanation of why this is a problem.

Figure 1 illustrates the heuristic model components: firstly it lists the preliminary heuristics (as explained in Table 1), followed by an illustration of how security and usability yield secure and usable online banking. Lastly, heuristic evaluation method steps to be followed are illustrated. It is important to note that security and usability as applied to an information system are inseparable. Hence all the heuristics are important in terms of both security and usability and they cannot be sub-divided to apply to only one aspect. Heuristic evaluation method involves a set of steps and the bottom part of Figure 1 illustrates the steps to be followed in this study as adopted from Nielsen (1995b). Firstly, the preliminary heuristics for usable and secure online banking are identified, and a checklist to be used for each heuristic is developed.

FUTURE WORK

The on-going investigation follows two strands: Firstly, it is concerned with understanding what standards or principles online security developers use in terms of making the security products usable, and why these are preferred over others; secondly, it sought to conduct a user evaluation of online security mechanisms, to open up existing security issues. The participants in the interviews will be information technology and communications (ICT) personnel, such as chief technology officers (CTO) and technicians working directly with security systems. Going forward our next step will be to collect data and evaluate the heuristics. Survey and grounded theory strategies will be used in this study. The survey uses a questionnaire instrument to collect deductive data for statistical analysis. The online banking users' data will be collected through a user evaluation questionnaire of the current online banking services offered by the major South African banks. The questionnaire probes questions that add value to the preliminary heuristics, and such responses will be cross-referenced with the data collected from interviews with security personnel in these banks.

The proposed model will be evaluated using a heuristic evaluation method. Using the chosen evaluators, usually between three and five as recommended by Nielsen (1995b), the online banking interface described through the heuristics will be evaluated. Based on the analysis, heuristics may be changed by adding some or removing those that are not applicable. The ratings in Table 2 help in identifying the severity of checklist items and whether a heuristic is applicable to the online banking system. The model is then refined, using the heuristic evaluation method by expert evaluators, using a comprehensive checklist for each identified heuristic. Finally by taking into consideration the results of the heuristic evaluation method a refined heuristic model will be presented.



Usable Security Heuristics

1. User control
2. Visibility
3. Errors
4. Help and documentation
5. User suitability
6. Learnability
7. Aesthetic and minimalist design
8. User language
9. Revocability
10. Satisfaction
11. Clarity
12. Path of least resistance
13. System protection
14. Consistency
15. Minimum authentication delay
16. Security and privacy

The security and privacy issues associated with an online banking system dictates the need for confidentiality, integrity and availability (CIA) as pillars of information security. The system should use the best security technology.

An online banking system need to be usable to allow users to use it effectively and be able to utilize security mechanisms to protect their confidential information. User interfaces design principles need to be applied when designing the system.

A secure and usable online banking environment can only be achieved through the realization of both security and usability goals. Applying usable security design principles can assist in developing a secure and usable online banking

Heuristic Evaluation Steps

Security
Usability
Secure & Usable Online Banking
Identify heuristics
Develop a checklist for each heuristic
Choose evaluators
Conduct heuristic evaluation
Refine the heuristic model

Figure 1: Heuristic Model for Usable Secure Online Banking

CONCLUSION

Understanding why users overlook security mechanisms will not only help in the formulation and enforcement of security policies, but also contribute to the design of such security technologies. A healthy security culture can be created by taking into consideration human aspects that make it difficult for users to comply with security requirements. The proposed heuristic model would facilitate the design and development of usable online banking security. As part of the ongoing research, the completed model would contribute to the ongoing efforts to design and develop usable and secure security systems in general. In the context of online banking, e-banking security has become a key competitive advantage, as breaches of the system can result in serious negative perceptions that might damage the image of the organization, in the long run. Finding ways to design online banking systems that are both secure and usable is an important step towards protecting this critical component of the global digital world. Trustworthy online banking has the capacity of contributing to the adoption of e-commerce. Furthermore, there is a need to study human behaviour when interacting with security, from development to usage of such mechanisms, with a special interest in usability of online banking security – in particular, whether the design process takes into account the users' capability to understand and use the system securely. The heuristic model has the potential of contributing by addressing the security problem from both the online user's side and the developer's side.

REFERENCES

Aladwani, A. M. 2001. "Online Banking: A Field Study of Drivers, Development Challenges, and Expectations," *International Journal of Information Management* (21:3), pp. 213-225.

AON 2013. "South African Businesses Unprepared for the Growing Risk of Cyber Attacks," Retrieved 11 October, 2013, from https://www.aon.co.za/index.php/en/news-articles/244-south-african-businesses-unprepared-for-the-growing-risk-of-cyber-attacks.

Besnard, D. and Arief, B. 2004. "Computer Security Impaired by Legitimate Users," *Computers & Security* (23), pp. 253-264.

Beyli, C. 2007. "Court Increases Liability for Breaches of Online Banking Security," Retrieved 11 October, 2013, from http://www.internationallawoffice.com/Newsletters/Detail.aspx?r=14246.

Bishop, M. (2012). Computer Security: Art and Science, (200), Addison-Wesley.

Bisong, A. and Rahman, M. 2011. "An Overview of the Security Concerns in Enterprise Cloud Computing," *International Journal of Network Security and Its Applications (IJNSA)* (3:1), pp. 30-45.

Buck, C. 2013. "Cyberattacks on the Rise as Credit, Debit Card Numbers Become Commodities," Retrieved 11 October, 2013, from http://phys.org/news/2013-06-cyberattacks-credit-debit-card-commodities.html.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Cashell, B., Jackson, W. D., Jickling, M., and Webel, B. April 2004. "The Economic Impact of Cyber-attacks," *Congressional Research Service*, Library of Congress.

Cessna, A. 2013. "Cyber-Attacks Targeting Card Numbers on the Rise," Retrieved 11 October, 2013, from http://www.creditcardprocessingspace.com/cyber-attacks-targeting-card-numbers-on-the-rise/

Cheung, C. M. K., Zhu, L., Kwong, T., Chan, G. W. W. and Limayem, M. 2003. "Online Consumer Behavior: A Review and Agenda for Future Research," *Proceedings of the 16th Bled eCommerce Conference*, June 2003, pp. 194.

Cranor, L. F. and Garfinkel, S. 2004. "Guest Editors' Introduction: Secure or Usable?" Security & Privacy, IEEE (2:5), pp. 16-18.

Dlamini, M., Eloff, J. H. P. and Eloff, M. M. 2009. "Information Security: The Moving Target," *Computers & Security* (28:3-4), May-June 2009, pp. 189-198.

Electronic Code of Federal Regulations, Part 205. 2013. Retrieved 11 October, 2013, from http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title12/12cfr205_main_02.tpl

Flechais, I., Mascolo, C. and Sasse, M. A. 2007. Integrating Security and Usability into the Requirements and Design Process, *International Journal of Electronic Security and Digital Forensics* (1:1), pp. 12-26.

Furnell, S. M., Gennatou, M., and Dowland, P. S. 2002. "A Prototype Tool for Information Security Awareness and Training," *Logistics Information Management* (15:5), pp. 352-357.

Furnell, S. 2005. "Why Users Cannot Use Security," *Computers & Security* (24:4), pp. 274-279.

Given, L. M. 2008. The SAGE Encyclopedia of Qualitative Research Methods, Sage Publications, Inc., London.

Guo, K. H., Yuan, Y., Archer, N. P. and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp. 203-236.

Hassenzahl, M., Law, E. L. C. and Hvannberg, E. T. 2006. “User Experience-Towards a Unified View,” *UX Workshop NordiCHI* (6), pp. 1-3.

Hassenzahl, M. 2008. “User Experience (UX): Towards an Experiential Perspective on Product Quality,” *Proceedings of the 20th International Conference of the Association Francophone d'Interaction Homme-Machine, ACM*, pp. 11-15.

Hentea, M. 2005. “A Perspective on Achieving Information Security Awareness,” *Informing Science: International Journal of an Emerging Transdiscipline* (2), pp. 169-178.

Hollingsed, T. and Novick, D.G. 2007. "Usability Inspection Methods after 15 years of Research and Practice," *Proceedings of the 25th Annual ACM International Conference on Design of Communication*, pp. 249.

Huang, D., Rau, P. P. and Salvendy, G. 2007. “A Survey of Factors Influencing People’s Perception of Information Security,” In: *Human-Computer Interaction, Part IV*, J. Jacko (Ed.). Heidelberg: Springer

Hutchinson, D., and Warren, M. 2003. "Security for Internet Banking: A Framework," *Logistics Information Management* (16:1), pp. 64-73.

IEEE Std 610.12. 1990. IEEE Standard Glossary of Software Engineering Terminology, *Institute of Electrical and Electronics Engineers*.

IOL 2013a. “How SIM Swap Led to Couple Losing R280 000,” Retrieved 11 October 2013, from http://www.iol.co.za/business/personal-finance/banking/how-sim-swap-led-to-couple-losing-r280-000-1.1507183#.UlQZghCF2UU.

IOL 2013b. “How Crooks Use SIM Swaps to Rob you,” Retrieved 11 October 2013, from http://www.iol.co.za/business/personal-finance/banking/how-crooks-use-sim-swaps-to-rob-you-1.1507185#.UlQc5BCF2UU

ISO/IEC 9126-1. 2001, Software Engineering - Product Quality - Part 1: Quality Model.

ISO/IEC 17799. 2005. IEC Code of Practice for Information Security Management.

ISO FDIS 9241-210. 2009. "Ergonomics of Human System Interaction - Part 210: Human-centered Design for Interactive Systems".

Johnston, J., Eloff, J. H. P. and Labuschagne, L. 2003. "Security and Human Computer Interfaces," *Computers & Security* (22:8), pp. 675-684.

Jones, R. A. and Horowitz, B. 2012. “A System-Aware Cyber Security Architecture,” *Systems Engineering*, (15:2), pp. 225-240.

Kainda, R., Flechais, I. and Roscoe, A. W. 2010. “Security and Usability: Analysis and Evaluation,” *International Conference on Availability, Reliability, and Security, IEEE*, pp. 275-282.

Katsabas, D., Furnell, S. and Dowland, P. 2005. "Using Human Computer Interaction Principles to Promote Usable Security," *Proceedings of the Fifth International Network Conference*, Samos, Greece, 5–7 July.

Kitten, T. 2011. “ACH Legal Ruling Favors Bank,” Retrieved 11 October, 2013, from http://www.bankinfosecurity.com/articles.php?art_id=3705&opg=1.

Law, E. L. C., Roto, V., Hassenzahl, M, Vermeeren, A. P. O. S. and Kort, J. 2009. "Understanding, Scoping and Defining User eXperience: A Survey Approach," P*roceedings of the 27th Annual CHI Conference on Human Factors in Computing Systems*, Boston, MA, USA, 4 - 9 April, pp. 719-728.

Leach, J. 2003. “Improving User Security Behaviour,” *Computers & Security* (22:8), pp. 685-692.

Lim, Y. K., Donaldson, J., Jung, H., Kunz, B., Royer, D., Ramalingam, S., Thirumaran, S. and Stolterman, E. 2008. Emotional Experience and Interaction Design,” *Affect and Emotion in Human-Computer Interaction*, Springer, Berlin, Heidelberg, pp. 116-129.

Locke, K. D. 2001. "Grounded Theory in Management Research," SAGE Publications, Inc., London.

Luftman, J., Kempaiah, R. and Nash, E. 2005. “Key Issues for IT Executives 2004,” *MIS Quarterly Executive* (4:2), pp. 269-285.

Luftman, J. and Ben-Zvi, T. 2010. “Key Issues for IT Executives 2010: Judicious IT Investments Continue Post-Recession,” *MIS Quarterly Executive* (9:4), pp. 263-273.

Mack, R. and Nielsen, J. 1993. "Usability Inspection Methods: Report on a Workshop held at CHI'92, Monterey, CA, May 3–4, 1992," *ACM SIGCHI Bulletin* (25:1), pp. 28-33.

Mack, R. and Nielsen, J. (Eds.) 1994. "Usability Inspection Methods," John Wiley and Sons, Inc., New York.

McCole, P., Ramsey, E. and Williams, J. 2010. “Trust Considerations on Attitudes Towards Online Purchasing: The Moderating Effect of Privacy and Security Concerns,” *Journal of Business Research* (63:9), pp. 1018-1024.

McKay, J., Marshall, P. and Hirschheim, R. 2012. “The Design Construct in Information Systems Design Science,” *Journal of Information Technology* (27:2), pp. 125-139.

Mitnick, K. D. and Simon, W. L. 2005. "The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders and Deceivers," Wiley.

Molich, R. and Nielsen, J. 1990. "Improving a Human-Computer Dialogue," *Communications of the ACM* (33:3), pp. 338-348.

Monk, A., Hassenzahl, M., Blythe, M. and Reed, D. 2002. "Funology: Designing Enjoyment," *CHI'02 Extended Abstracts on Human Factors in Computing Systems, ACM*, Minnesota, USA, 20-25 April, pp. 924.

Mouratidis, H., Kalloniatis, C., Islam, S., Huget, M. P. and Gritzalis, S. 2012. “Aligning Security and Privacy to Support the Development of Secure Information Systems,” *Journal of Universal Computer Science*, (18:12), pp. 1608-1627.

Myers, M. D. 2009. "Qualitative Research in Business and Management," Sage Publications, London.

Nepomuceno, M. V., Laroche, M., Richard, M. O. and Eggert, A. 2012. “Relationship between Intangibility and Perceived Risk: Moderating Effect of Privacy, System Security and General Security Concerns,” *Journal of Consumer Marketing* (29:3), pp. 176-189.

Nielsen, J. 1994a. "Enhancing the Explanatory Power of Usability Heuristics," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 1994)*, Boston, MA, USA, 24-28 April, pp. 152-158.

Nielsen, J. 1994b. "Usability Inspection Methods," *Conference Companion on Human Factors in Computing Systems, ACM*, pp. 413.

Nielsen, J. 1995a. "10 Usability Heuristics for User Interface Design." Retrieved 11 October, 2013, from http://www.nngroup.com/articles/ten-usability-heuristics/

Nielsen, J. 1995b. "How to Conduct a Heuristic Evaluation," Retrieved 11 October, 2013, from http://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/

Nielsen, J. and Molich, R. 1990. "Heuristic Evaluation of User Interfaces," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 1990), ACM*, Seattle, USA, 1-5 April, pp. 249.

Oxford Dictionary. 2004. "Oxford English Dictionary Online," Oxford University Press.

Paas, F., Renkl, A. and Sweller, J. 2003. “Cognitive Load Theory and Instructional Design: Recent Developments,” *Educational Psychologist,* (38:1), pp. 1-4.

Panda Security 2010. “Second International Barometer of Security in SMBs,” Retrieved 11 October, 2013, from http://press.pandasecurity.com/wp-content/uploads/2010/08/2nd-International-Security-Barometer.pdf.

Payne, S. J. (2009). “Mental Models in Human Computer Interaction,” *Human Computer Interaction: Fundamentals*, pp. 39-52.

Perrig, A., and Song, D. 1999. “Hash Visualization: A New Technique to Improve Real-World Security.” *International Workshop on Cryptographic Techniques and E-Commerce*, pp. 131-138.

Peter, C. and Beale, R. (Eds.). 2008. "Affect and Emotion in Human-Computer Interaction: From Theory to Applications," (4868), Springer.

Pierotti, D. 2007. "Heuristic Evaluation - A System Checklist." Retrieved 11 October, 2013, from http://www.anst.uu.se/larsoest/uploads/Main/HeuristicEvalChecklist.pdf.

Puhakainen, P. and Siponen, M. 2010. “Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study,” *MIS Quarterly* (34:4), pp. 757-778.

Romanosky, S., Telang, R. and Acquisti, A. 2011. “Do Data Breach Disclosure Laws Reduce Identity Theft?” *Journal of Policy Analysis and Management* (30:2), pp. 256-286.

Sasse, M. A., Brostoff, S. and Weirich, D. 2001. "Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security," *BT Technology Journal* (19:3), pp.122-131.

Sasse, M. A. and Flechais, I. 2005. "Usable Security," In Security and Usability: Designing Secure Systems That People Can Use," L.F. Cranor and S. Garfinkel (Eds.), O'Reilly Media Inc., USA, pp. 13 - 30.

Sathye, M. 1999. "Adoption of Internet banking by Australian Consumers: An Empirical Investigation," *International Journal of Bank Marketing* (17:7), pp. 324-334.

Saunders, M., Lewis, P. and Thornhill, A. 2009. Research Methods for Business Students, 5th Edition, Prentice Hall, England.

Schneider, K., Knauss, E., Houmb, S., Islam, S. and Jürjens, J. 2012. “Enhancing Security Requirements Engineering by Organizational Learning,” *Requirements Engineering* (17:1), pp. 35-56.

Schneier, B. 2000. “Secrets and Lies”, John Wiley and Sons.

Shaw, R. S., Chen, C. C., Harris, A. L. and Huang, H. J. 2009. “The Impact of Information Richness on Information Security Awareness Training Effectiveness,” *Computers & Education* (52:1), pp. 92-100.

Shneiderman, B. and Plaisant, C. 2010. "Designing the User Interface: Strategies for Effective Human-Computer Interaction," 5th Edition, Pearson Education, USA.

Schultz, E. E., Proctor, R. W., Lien, M. C. and Salvendy, G. 2001. “Usability and Security: An Appraisal of Usability Issues in Information Security Methods,” *Computers & Security* (20:7), pp. 620-634.

Schwartz, P. and Janger, E. 2007. "Notification of Data Security Breaches," *MLR* (105), pp. 913.

Siponen, M., Baskerville, R. and Heikka, J. 2006. “A Design Theory for Secure Information Systems Design Methods,” *Journal of the Association for Information Systems* (7:1), pp. 31.

Steinfield, C. 2002. "Understanding Click and Mortar E-commerce Approaches: A Conceptual Framework and Research Agenda,” *Journal of Interactive Advertising* (2:2), pp. 1-10.

Symantec 2013. “Internet Security Threat Report 2013: Volume 18,” Retrieved 11 October, 2013, from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_2129

1018.en-us.pdf.

Thomson, M. E., and von Solms, R. 1998. “Information Security Awareness: Educating Your Users Effectively,” *Information Management and Computer Security* (6:4), pp. 167-173.

Vaas, L. 2012. “Bank's shoddy security was to blame for $588,851 online robbery, US appeals court rules,” Retrieved 11 October, 2013, from http://nakedsecurity.sophos.com/2012/07/10/bank-online-security-breach/

Venkatesh, V., Brown, S. and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), March, pp. 21-54.

Whitten, A. and Tygar, J. D. 1999. "Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0," *Proceedings of the 8th USENIX Security Symposium, Citeseer*, pp. 169–184.

Yee, K. P. 2004. "Secure Interaction Design," *Financial Cryptography*, Springer, pp. 114.

Yee, K. P. 2002. "User Interaction Design for Secure Systems," *Information and Communications Security*, pp. 278-290.

Yeratziotis, A., Pottas, D. and Van Greunen, D. 2012. "A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm," *International Journal of Human-Computer Interaction* (28:10), pp. 678-694.

COPYRIGHT