Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach

J. Jansen[1,2]

[1]Faculty of Humanities and Law, Open University of the Netherlands
[2]Cybersafety Research Group, NHL University of Applied Sciences
e-mail: j.jansen@nhl.nl

Abstract

In this paper, a conceptual research model is proposed to study safe online banking behaviour. The Protection Motivation Theory functions as the core of the model. The model is extended with additional variables, making it suitable for the online banking context. The coping perspective, which is central to the Protection Motivation Theory, seems to be valuable to study behaviour in information systems. By taking a cognitive behavioural perspective, it can be examined how individuals cope with threats, which may contribute to the development of effective intervention programs aimed at safe online banking.

Keywords

Protection Motivation Theory, Online Banking, Customer Behaviour, Risk, Coping

1. Introduction

This study concentrates on online banking, a means by which customers can access different kinds of banking services via the internet. By 2014, more than eighty percent of Dutch citizens aged sixteen and over had adopted this service (Eurostat, 2014). Online banking is not without risk, it also attracts criminals. The rise of online banking has changed the nature of attacks on the flow of payments. Attacks are now more targeted at customers instead of banks (NVB, 2011).

The Dutch Banking Association (NVB) annually reports figures concerning online banking fraud. The financial damage in 2013 caused by fraudulent transfers was estimated to be 9.6 million euros. Online banking fraud is mainly caused by phishing and malware attacks. The financial damages in 2011 and 2012 were respectively 35.0 and 34.8 million euros (NVB, 2013). Although the numbers tend to decline, it is still a considerable problem that banks and users of online banking need to deal with.

A trend regarding online banking is that customers are attributed with more responsibility (Anderson, 2007; Davinson and Sillence, 2014). This is not surprising because the safety and security of online banking cannot be addressed by one party; it is a joint responsibility of multiple parties. Thus, customers also have certain responsibilities considering the safety and security of online banking. Consequently, customers should be able to cope with threats aimed at online banking.

The definition of coping used in this study is that customers are aware of the threats of online banking, (try to) prevent them, recognize them and act accordingly. First, someone must be aware of a specific threat, such as fraud. If the threat, despite all actions, could not be avoided, it is important to recognize or detect it as soon as possible. If a threat is quickly noticed, its impact might be reduced or possibly mitigated entirely. In other words, coping is not only about eliminating threats, but also about managing them. This study focuses on two specific parts of coping, namely the identification and prevention of threats. The coping approach is supported by various scientific disciplines, such as health and consumer psychology, but is relatively new in the field of information systems (Lai *et al.* 2012).

As of January 1st 2014, Dutch private customers who use online banking need to adhere to the so-called unified safety rules for online banking, which are defined in the General Terms & Conditions of all banks in the Netherlands. This effort is made under the supervision of the Dutch Banking Association and the Dutch Consumer Association, to create more uniformity in the policies of banks. The safety rules are: keep your security codes secret, make sure that your debit card is not used by other persons, secure the devices you use for online banking properly, check your bank account regularly, and report incidents directly to your bank.

The purpose of this study is to gain insight into the factors that affect customers to take protective measures against online banking fraud, i.e. to comply with the unified safety rules. The main research question is: What factors affect customers to take safety measures to protect themselves against online banking fraud? The outcome of this study is a conceptual research model to study safe online banking behaviour. The Protection Motivation Theory is used as a theoretical lens to study this problem.

This study is part of a PhD research program on the safety and security of online banking. This program is funded by the Dutch banking sector (represented by the Dutch Banking Association), the Police Academy, and the Dutch National Police.

2. Conceptual Research Model for Safe Online Banking

In this section, a brief overview is given of the Protection Motivation Theory (PMT), its constructs and the reasons why this specific theory is chosen. The constructs are divided in four levels: threat appraisal, coping appraisal, protection motivation, and control variables. Additional constructs which seem valuable for the online banking context are presented within these categories. These are: trust in online banking, locus of control, injunctive norms, descriptive norms and attitude. Conclusively, the conceptual research model is presented and explained.

2.1. Selecting the Protection Motivation Theory

There are several theories that try to explain and predict behaviour (Floyd *et al.* 2000). For example, in information systems research already much is known about the adoption of technology. Technologies that have been studied are often *beneficial technologies* (Chenoweth *et al.* 2009), of which online banking is an example.

Regarding the use of *protective technologies*, which are focused on preventing negative outcomes, less is known (Chenoweth *et al.* 2009). Few studies have been conducted on security behaviour of end users and on how such behaviour can be changed (Ng *et al.* 2009). Research has shown that there are significant differences between the use of beneficial and protective technologies (Dinev and Hu, 2005). Therefore, other theories than adoption theories may be more appropriate.

After evaluating several psychological theories, the PMT (Rogers, 1975) is chosen as the basis for this study, a social cognitive theory that predicts behaviour (Milne *et al.* 2000). The main reasons for this choice are as follows. The PMT has been successfully applied to understand and predict the use of various protective measures (Milne *et al.* 2000) and is considered one of the most powerful explanatory theories for safe behaviour (Floyd *et al.* 2000). The theory is applied, sometimes in an adjusted form, to the field of information systems and has been found useful in predicting individual computer security behaviour in both home (Anderson and Agarwal, 2010; Chenoweth *et al.* 2009; Crossler, 2010; Johnston and Warkentin, 2010; Lai *et al.* 2012; Liang and Xue, 2010) and working situations (Herath and Rao, 2009; Ifinedo, 2012; Lee, 2011; Lee and Larsen, 2009; Pahnila *et al.* 2007; Vance *et al.* 2012; Workman *et al.* 2008; Workman *et al.* 2009), making it a useful theory for studying safe online banking behaviour. Strength of the PMT is that it includes the concept of risk, which is neglected in adoption theories (Johnston and Warkentin, 2010). Furthermore, attention is not only paid to the predicting variables, but also to how these variables are related. Finally, the theory is useful for the development of interventions (Floyd *et al.* 2000).

2.2. The Protection Motivation Theory and its constructs

Central to the PMT are two cognitive processes, namely threat appraisal and coping appraisal. In the threat appraisal process, individuals evaluate the likelihood and impact of a threat. This is followed by the coping appraisal process in which individuals evaluate possible coping strategies against the threat. This process is driven by the effectiveness of a strategy or measure, the degree to which the individual is able to perform the required action and the costs involved. The cognitive processes are initiated by receiving information, which is called sources of information, and includes environmental and interpersonal sources. Both processes in their turn affect the protection motivation, i.e. the intention to perform certain behaviour. For more information about the PMT, see Milne *et al.* (2000) and Norman *et al.* (2005).

2.2.1. Threat appraisal

In the threat appraisal process, an estimate is made of the threat. This is performed initially, because a threat must be observed first before one can assess coping strategies (Floyd *et al.* 2000; Liang and Xue, 2009). Crossler (2010 p.2) defines this process as “an individual’s assessment about the level of danger posed by a security event”. Threat appraisal consists of the constructs *perceived vulnerability* and *perceived severity*, which both make up *perceived risk*. The *rewards* construct is also part of the threat appraisal process. However, rewards are barely operationalized in PMT studies (Milne *et al.* 2000). This is mainly because the conceptual difference between the value of a reward for risky behaviour and the response costs for a security measure (see coping appraisal) is not always clear (Abraham *et al.* 1994). Therefore, this construct is dropped. For threat appraisal one additional construct is added, namely *trust in online banking*.

In the context of online banking, perceived risk is defined as "the potential of loss in the pursuit of a desired outcome from using electronic banking services" (Yousafzai *et al.* 2003 p.851). When a risk is perceived, individuals will change their behaviour based on how much risk they are willing to accept for the particular threat (Workman *et al.* 2008). Based on this notion, it is expected that the higher the perceived risk, the more likely a customer will be inclined to take protective measures.

Perceived vulnerability is "an individual's assessment of the probability of a threatening security event occurring" (Crossler, 2010 p.2). This involves an individual's believe on how likely it is to be victimized by online banking fraud. It is expected that perceived vulnerability has a positive influence on perceived risk. The perceived impact of a threat is "an individual's assessment of the severity of the consequences resulting from a threatening security event" (Crossler, 2010 p.2). This involves how serious the consequences of online banking fraud are perceived. It is expected that perceived severity of a threat has a positive influence on perceived risk. Liang and Xue (2010) argue that perceived vulnerability and perceived severity have an interaction effect on the formation of perceived risk. They state that perceived risk is a calculation of probability times impact and that when one of the two is zero, the perceived risk disappears. This effect will be included in the model.

Literature on online banking adoption has repeatedly shown that a high level of trust reduces the perception of risk (e.g. Yousafzai *et al.* 2009). This study adopts the definition of Yousafzai *et al.* (2003 p.849) who define trust in online banking as "a psychological state which leads to the willingness of customer to perform banking transactions on the Internet, expecting that the bank will fulfil its obligations, irrespective of customer's ability to monitor or control bank's actions". Trust is not often integrated in PMT studies. However, it is an important construct in risk literature. Therefore, a logical place for trust in the conceptual model is within the treat appraisal process. It is hypothesised that trust in online banking has a negative influence on risk perception.

2.2.2. Coping appraisal

Assessing threats is not enough. When individuals feel vulnerable and think that the potential severity of a threat is high, that does not change their behaviour immediately. There are additional barriers that must be overcome (Furnell *et al.* 2006). The coping appraisal process includes an evaluation of the estimated coping strategies to avoid or minimize the threat. Crossler (2010 p.2) defines this process as "an individual's assessment of his ability to perform a given behaviour and his confidence that a given behaviour will be successful in mitigating or averting the potential loss or damage resulting from a threatening security event, at a perceived cost that is not too high". Threat appraisal consists of the constructs *response efficacy*, *self-efficacy* and *response costs*. Four additional constructs are added, namely *locus of control*, *injunctive norms, descriptive norms* and *attitude*.

Response efficacy "concerns beliefs about whether the recommended coping response will be effective in reducing threat to the individual" (Milne *et al.* 2000 p.109). If the individual is sufficiently satisfied that the protective measure will actually work, then that is an incentive to apply it. Liang and Xue (2010) argue that it is possible that response efficacy, what they call safeguard effectiveness, interacts with perceived risk. This interaction effect is included in the model.

Self-efficacy "concerns an individual's beliefs about whether he or she is able to perform the recommended coping response" (Milne *et al.* 2000 p.109). Rhee *et al.* (2009) studied self-efficacy and its impact on safe behaviour by end users. In their article, it is explained that it is important to assign a domain-specific framework to self-efficacy, which increases its predictive value. Rhee *et al.* (2009 p.818) speak of self-efficacy in information security, which they define as "a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability". The assumption is that the higher the self-efficacy in terms of taking safety measures, the more an individual will be inclined to take such measures.

Response costs "concern beliefs about how costly performing the recommended response will be to the individual" (Milne *et al.* 2000 p.109). This involves both tangible and intangible costs. When the costs of applying safety measures exceed the costs of a potential threat, then the response costs have a negative influence on protection motivation.

In line with the work of Workman *et al.* (2008), locus of control is considered to be part of the coping appraisal process. This concept is concerned with the conviction of individuals whether they have the outcome of a given situation under control (internal locus of control), or that it is controlled by others (external locus of control). In the case of online banking, it is possible that customers push off responsibility for its safety to the supplier, i.e. the bank. In addition, customers might feel that they have no control over the safety and security of online banking. Consequently, locus of control has impact on the behaviour of individuals. It determines whether the behaviour is proactive (taking responsibility) or reactive (leaving it to others) (Workman *et al.* 2008). The assumption is that when a customer feels in control of the situation, he or she will be motivated to take action.

According to Anderson and Agarwal (2010 p.616) there is lack of attention for social variables in information systems research "even though the information systems adoption literature and the underlying theories they draw upon suggests […] that norms can be influential in the formation of behavior". Therefore, the constructs injunctive and descriptive norms are added to the model. Ifinedo (2012) placed norms within the coping appraisal process, which is also done in this study.

"Injunctive norms refer to perceptions concerning what should or ought to be done with respect to performing a given behaviour, whereas descriptive norms refer to perceptions that others are or are not performing the behavior in question" (Fishbein and Ajzen, 2010 p.131). Both injunctive and descriptive norms have a positive influence on protection motivation.

Finally, attitude is added to the model, which is defined as "an individual's positive or negative feelings (evaluative effect) about performing the target behavior" (Fishbein and Ajzen, 1975 p.216). The relation between attitude and intentional behaviour is extensively tested in information systems research (Venkatesh *et al.* 2003). It is assumed that a positive attitude towards protective measures will have a positive influence on taking such measures.

2.2.3. Protection motivation

The protection motivation is the decision or intention to proceed to, continuation of, or the avoidance of the studied behaviour (Floyd *et al.* 2000). "Protection motivation is an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity" (Rogers, 1975 p.98). The protection motivation can manifest itself in an adaptive or maladaptive coping response. An adaptive response implies that customers protect themselves. A maladaptive response is the opposite, namely that customers do not protect themselves. This response suggests that an individual is at risk.

In this study, the PMT is applied to explain why online banking customers adopt the desired behaviour, i.e. an adaptive coping response. The desired behaviour is compliance with the unified rules for safe online banking, the outcome variable of the conceptual model. Thus, the independent variable consists of multiple actions. This is, however, not an issue considering that securing online banking, as is the case with securing a computer, "is about performing a number of different practices, not one in particular" (Crossler and Bélanger, 2014 p.54). These authors furthermore state that a more holistic view on safe behaviour is acquired when measuring multiple behaviours instead of one.

In information systems research, it is preferred to measure actual behaviour instead of intentional behaviour (Anderson and Agarwal, 2010; Workman *et al.* 2009). However, this will be difficult to achieve. Therefore, it is chosen to measure intentional behaviour. Anderson and Agarwal (2010 p.614) who also studied intentional behaviour instead of actual behaviour justified their choice by findings from earlier studies which indicated that the relationship between intentional and actual behaviour is strong, consistent and theoretically grounded.

2.2.4. Control variables

For this study, four control variables are included. These are *internet experience*, *habit*, *victimization of online banking fraud* and *demographic variables*. The first three are considered prior experience, an aspect of the PMT which is often neglected

(Vance *et al.* 2012), but is deemed a strong predictor of future behaviour (Norman *et al.* 2005). In order to keep the model as parsimonious as possible, personality variables like risk propensity and trust propensity are omitted.

While online banking is not a new phenomenon, it is a relatively new online service. According to Mannan and Van Oorschot (2008) people who adopt online banking at later times are less technical savvy. Prior experience with a website or other internet activities can have an impact on current behaviour of customers in terms of security choices (Chen and Bansal, 2010). In this study, it is assumed that more experienced internet users better understand security issues regarding online banking and therefore are more inclined to protect themselves against the possible threats.

A study that included prior experiences, in the form of habit, is that of Vance *et al.* (2012). Habit theory assumes that many actions are taken without thinking about it deeply, and that actions are performed because individuals are accustomed to them (Vance *et al.* 2012). Habits are thus acts performed unconsciously or automatically. Consequently, it is proposed that habits related to information security have a positive impact on complying with the safety rules for online banking.

Prior experience as an online banking fraud victim can also influence the protection motivation. People who once were victimized might easily regard themselves as victims again (Workman *et al.* 2008). In this study, it is expected that earlier victimization motivates a customer to take measures to prevent fraud in the future.

Finally, demographic variables are included in the model. The demographic variables that will be included are gender, age, educational level and work situation. It is not only important to determine which variables matter in terms of taking measures to keep online banking as safe as possible. It is also important to identify whether there are differences between specific groups of customers. By including such variables, it will be possible to make targeted recommendations for intervention strategies.

2.3. The model

The protection motivation, in this case compliance with the rules for safe online banking, results from the threat and coping appraisal processes (Figure 1). The arrows in this model indicate which variables have an impact on what other variables. A minus-sign means that a negative relationship is expected. In other cases, the expected relationship is positive. The circles represent interaction effects.

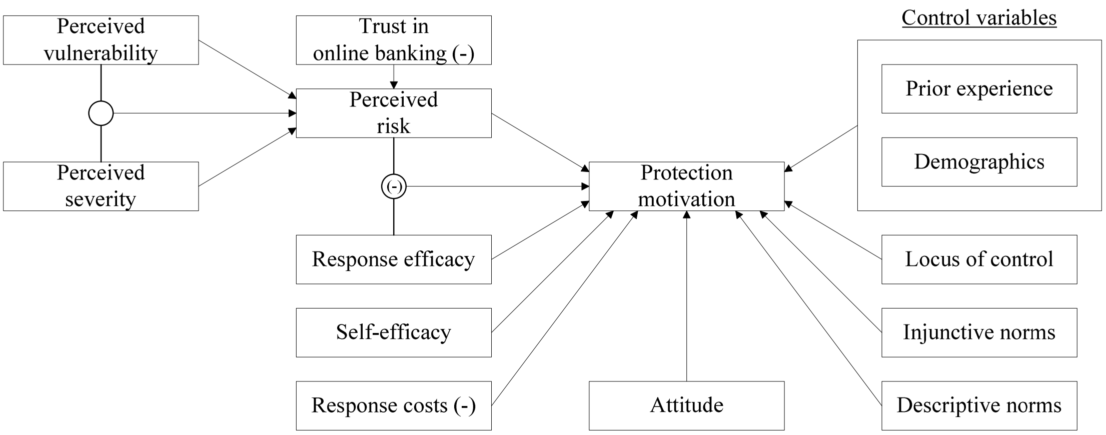

Figure 1: Conceptual research model

The protection motivation is a positive function of risk perception, response efficacy, self-efficacy, locus of control, injunctive norms, descriptive norms and attitude, and a negative function of response costs. In the model, protection motivation is controlled for by prior experience and demographic variables. Risk perception in its turn is positively influenced by perceived vulnerability and perceived severity, and negatively by trust in online banking.

3. Conclusions and future research

Research shows that technical security cannot guarantee the safety of online banking; the behaviour of end users is also vital (Davinson and Sillence, 2014; Furnell *et al.* 2006; Liang and Xue, 2010; Ng *et al.* 2009; Rhee *et al.* 2009). It is recognized that research is scarce in the domain of individual security related behaviour (Liang and Xue, 2010). Anderson and Agarwal (2010 p.613) state for example: “there is limited understanding of what drives home computer users to behave in a secure manner online, and even less insight into how to influence their behaviour”.

Based on the above, it is concluded that the PMT is a suitable theory to take as a starting point for further study. In literature, no studies were found that applied the PMT to online banking. By applying the PMT to a new territory, it can be assessed whether the PMT, extended with additional variables, maintains its value. The proposed model will be evaluated in a later study on a representative sample of Dutch online banking customers. In addition, the PMT approach seems applicable to more fields other than online banking.

4. References

Abraham, C.S., Sheeran, P., Abrams, D. and Spears, R. (1994), "Exploring teenagers’ adaptive and maladaptive thinking in relation to the threat of HIV infection", *Psychology & Health,* Vol. 9, No. 4, pp253–272.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34, No. 3, pp613–643.

Anderson, R. (2007), "Closing the phishing hole: Fraud, risk and nonbanks", *Proceedings of the Payments System Research Conferences*, pp1–16.

Chen, L.-C. and Bansal, G. (2010), "An integrated model of individual web security behavior", *Proceedings of the 16th Americas Conference on Information Systems*, pp485–492.

Chenoweth, T., Minch, R. and Gattiker, T. (2009), "Application of protection motivation theory to adoption of protective technologies", *Proceedings of the 42nd Hawaii International Conference on System Sciences*, pp1–10.

Crossler, R. and Bélanger, F. (2014), "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument", *ACM SIGMIS Database*, Vol. 45, No. 4, pp51–71.

Crossler, R.E. (2010), "Protection motivation theory: Understanding determinants to backing up personal data", *Proceedings of the 43rd Hawaii International Conference on System Sciences*, pp1–10.

Davinson, N. and Sillence, E. (2014), "Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions", *International Journal of Human-Computer Studies,* Vol. 72, No. 2, pp154–168.

Dinev, T. and Hu, Q. (2005), "The centrality of awareness in the formation of user behavioral intention toward preventive technologies in the context of voluntary use", *Proceedings of the International Conference of Information Systems,* pp1–5.

Eurostat (2014), "Individuals using the internet for internet banking", http://ec.europa.eu/eurostat/tgm/refreshTableAction.do;?pcode=tin00099&language=en, (Accessed 2 March 2015).

Fishbein, M. and Ajzen, I. (1975), *Belief, attitude, intention and behavior: An introduction to theory and research*, Addison-Wesley, MA, ISBN: 978-0-2010-2089-2.

Fishbein, M. and Ajzen, I. (2010), *Predicting and changing behavior: The reasoned action approach*, Taylor & Francis, New York, ISBN: 978-0-8058-5924-9.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W. (2000), "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 2, pp407–429.

Furnell, S.M., Jusoh, A. and Katsabas, D. (2006), "The challenges of understanding and using security: A survey of end-users" *Computers & Security*, Vol. 25, No.1, pp27–35.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: A framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18, No. 2, pp106–125.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31, No. 1, pp83–95.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: An empirical study", *MIS Quarterly*, Vol. 34, No. 3, pp549–566.

Lai, F., Li, D. and Hsieh, C.-T. (2012), "Fighting identity theft: The coping perspective", *Decision Support Systems*, Vol. 52, No. 2, pp353–363.

Lee, Y. (2011), "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective", *Decision Support Systems*, Vol. 50, No. 2, pp361–369.

Lee, Y. and Larsen, K.R. (2009), "Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems*, Vol. 18, No. 2, pp177–187.

Liang, H. and Xue, Y. (2009), "Avoidance of information technology threats: A theoretical perspective", *MIS Quarterly*, Vol. 33, No. 1, pp71–90.

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: A threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11, No. 7, pp394–413.

Mannan, M. and Van Oorschot, P.C. (2008), "Security and usability: The gap in real-world online banking", Proceedings of the 2007 Workshop on New Security Paradigms, pp1–14.

Milne, S., Sheeran, P. and Orbell, S. (2000), "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory", Journal of Applied Social Psychology, Vol. 30, No. 1, pp106–143.

Ng, B.-Y., Kankanhalli, A. and Xu, Y.C. (2009), "Studying users' computer security behavior: A health belief perspective", *Decision Support Systems*, Vol. 46, No. 4, pp815–825.

Norman, P., Boer, H. and Seydel, E.R. (2005), *Protection motivation theory*, In: Predicting health behaviour: Research and practice with social cognition models, Open University Press, Maidenhead, pp81–126.

NVB (2011), *"Annual report 2011",* Dutch Banking Association, Amsterdam, pp.1–52.

NVB (2013), *"Position paper online payments: May 30th 2013"*, Dutch Banking Association, Amsterdam, pp1–5.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*. pp156–165.

Rhee, H.-S., Kim, C. and Ryu, Y.U. (2009), "Self-efficacy in information security: Its influence on end users' information security practice behavior", *Computers & Security*, Vol. 28, No. 8, pp816–826.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol. 91, No. 1, pp93–114.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating IS security compliance: Insights from habit and protection motivation theory", *Information & Management*, 49, pp190–198.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, Vol. 27, No. 3, pp425–478.

Workman, M., Bommer, W.H. and Straub, D. (2008), "Security lapses and the omission of information security measures: A threat control model and empirical test", *Computers in Human Behavior*, Vol. 24, No. 6, pp2799–2816.

Workman, M., Bommer, W.H. and Straub, D. (2009), "The amplification effects of procedural justice on a threat control model of information systems security behaviours", *Behaviour & Information Technology*, Vol. 28, No. 6, pp563–575.

Yousafzai, S., Pallister, J. and Foxall, G. (2009), "Multi-dimensional role of trust in Internet banking adoption", *The Service Industries Journal*, Vol. 29, No. 5, pp591–605.

Yousafzai, S.Y., Pallister, J.G. and Foxall, G.R. (2003), "A proposed model of e-trust for electronic banking", *Technovation*, Vol. 23, No. 11, pp847–860.