Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

"Security begins at home": Determinants of home computer and mobile device security behavior

Nik Thompson [a,*], Tanya Jane McGill [b], Xuequn Wang [b]

[a] School of Information Systems, Curtin University, Kent Street, Bentley, Western Australia, 6102, Australia
[b] School of Engineering and Information Technology, Murdoch University, South Street, Murdoch, Western Australia, 6150, Australia

ARTICLE INFO

Article history:
Received 16 March 2017
Received in revised form 30 May 2017
Accepted 4 July 2017
Available online 12 July 2017

Keywords:
Behavioral IS security
Information security
Mobile device security
Home computer security
Protection motivation theory

ABSTRACT

Personal computing users are vulnerable to information security threats, as they must independently make decisions about how to protect themselves, often with little understanding of technology or its implications. However, personal computing users are under-represented in security research studies, especially for mobile device use. The study described in this paper addresses this research gap by evaluating data from 629 home computer and mobile device users to improve understanding of security behavior in both contexts. The research model extends protection motivation theory by including the roles of social influences and psychological ownership, and by including actual behavior. The model was separately tested with home computer users and mobile device users and data reveals that some of the determinants of security behavior differ between home computer and mobile device use. The results show that perceived vulnerability, self-efficacy, response cost, descriptive norm and psychological ownership all influenced personal computing security intentions and behavior for both home computer users and mobile device users. However, perceived severity was only found to play a role in mobile device security behavior and neither response efficacy nor subjective norm influenced security intentions for either type of user. These findings are discussed in terms of their practical and research implications as well as generating new research opportunities into personal computing security.

1. Introduction

The pervasiveness and accessibility of the Internet have provided immense social benefit by linking communities and dissolving geographic boundaries. However, while communities have been brought together by developments in technology, this free, borderless communication has opened up new avenues for crime and fraud, exposing millions of home computer users to cyber criminals across the globe. To compound this issue further, attackers increasingly pick the soft targets in order to minimize their effort. Attacks such as the record 1.2 Tbps Denial of Service attacks reported in late 2016 (Symantec Security Response, 2016) demonstrate that malicious actors have their sights set on the home computer sector, not just as the eventual targets, but even as instruments in larger attacks.

Kaspersky's Threat Evolution report provides some insights into the extent of the issues faced in the mobile arena. In Q1 2016 over 2 million malicious installation packages were detected by their mobile telemetry. This was an increase of 11 percent over the previous quarter, and 23 percent over Q3 2015

[*] Corresponding author.
E-mail address: nik.thompson@curtin.edu.au (N. Thompson).

http://dx.doi.org/10.1016/j.cose.2017.07.003
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

(Kaspersky Labs, 2016). The trend is continuing, with no signs of slowing. The same report highlights the growth in attacks on mobile banking apps. For example, a single strain of the *Marcher* Trojan was attacking nearly 40 mobile banking apps in Europe. This suggests that home users are increasingly at risk when they transact on the Internet.

Studies of user security behavior with an organizational focus have been more prevalent than those relating to home user behavior, often aiming to reveal the factors that may influence an employee's intention to comply with information security policies (e.g. Ifinedo, 2012; Siponen et al., 2014). However, this over-representation of organization-focused research is giving way to more recent studies of home computer users (Anderson and Agarwal, 2010; Liang and Xue, 2010; Mwagwabi et al., 2014; Woon et al., 2005; Zhang and McDowell, 2009) in recognition of the vulnerability of home users and the potential flow on effects from home user breaches to organizational breaches (Jenkins et al., 2014; Winkler, 2009). While there may be similarities in "security behavior" that span both the organizational and home environments, Li and Siponen (2011) identified nine contextual factors that differentiate the home setting from organizational use, including the role of technical support, training, sanctions and organizational policies among others, calling for focused research with home users. It is, therefore, necessary to directly study the home user environment to better understand and ultimately safeguard this large segment.

Protection Motivation Theory (PMT) (Rogers, 1975, 1983) has been widely used to try to explain user security behavior with some success (e.g., Crossler et al., 2014; Herath and Rao, 2009; Ifinedo, 2012; Vance et al., 2012); however, the majority of this research has taken place in an organizational context and research using it to understand personal computing security behavior has shown more mixed results, particularly with respect to the role of perceived vulnerability to threats (Liang and Xue, 2010; Mwagwabi et al., 2014; Zhang and McDowell, 2009). The study described in this paper addresses the need to improve understanding of home computer and mobile device computing security behavior by testing a model of personal computing security behavior that is based on PMT, but is extended to incorporate findings from the personal computing domain on the roles of psychological ownership and social influence (Anderson and Agarwal, 2010; Tu et al., 2015).

Johnston et al. (2015) argue that future studies should investigate the applicability of PMT in different security domains. There has been a rapid expansion of personal computing from being primarily computer based to encompassing a variety of mobile devices, and this has implications not only for the individuals affected but for organizations that allow employees to access personal online accounts from organizational computers or support Bring Your Own Device (BYOD). In this paper, the proposed model is tested for both home computer use, and for mobile device use, in order to better understand the factors that are most likely to influence user behavior on a given platform. To the best of our knowledge, this is the first study to do this, and the results show that there are differences in the determinants of security behavior between device types.

The study also looks beyond security intentions to actual security behavior. Much of the previous behavioral information security research employs intention based models that use behavioral intention as a surrogate for actual behavior, yet individuals do not always act in accordance with their behavioral intention (Ajzen et al., 2004). Thus further understanding of the relationship between intentions and actual behavior in the personal computing security domain is required. The proposed model provides a framework to do so, and this study examines the relationship between security intentions and actual security behavior for both home computer use and mobile device use, and possible reasons for the difference that is found are explored.

2. Related work

2.1. *PMT as a framework to study home computer security*

PMT (Rogers, 1975, 1983) was developed to explain how to influence risky behavior and to understand how the components of a persuasive message are critical. Grounded in the theory of fear appeals, it suggests that the behavior of individuals when faced by a risk is dictated by their threat appraisal (how severe they perceive the impact of this threat to be and how likely they believe it is to occur) and their coping appraisal (how effective and costly they perceive threat avoidance behavior to be and their appraisal of their ability to perform the protective behavior). Although originally developed in the health domain to consider risks of smoking or transmittable diseases, PMT has been found useful in research of other kinds of risks, notably those in the computer security arena.

Rogers' original PMT (Rogers, 1975) considers the components of fear appeals and how these components influence the process of coping or taking a protective behavioral response. PMT was later revised to pay greater attention to the sources of information contributing to the process and to cognitive mediating processes (Maddux and Rogers, 1983; Rogers, 1983). The addition of self-efficacy, costs associated with protective behavior and perceived rewards for not performing behavior provided a more comprehensive model.

Threat appraisal includes perceived vulnerability and perceived severity of risks, as well as any perceived rewards associated with the risky behavior. Elements of high vulnerability, high severity and low reward would predispose individuals to a higher protection motivation and thus behavior. Coping appraisal is made up of the perceptions of response efficacy and self-efficacy as well as any perceptions of costs associated with the protective response behavior. Self-efficacy is the belief that individuals hold about their own abilities to perform a protective behavior. Response efficacy is the belief regarding the effectiveness of the protective behavior, if taken. Response cost relates to any costs associated with taking the protective behavior. In a computer security context, this cost is not always reflected in monetary terms. It may be also perceived in terms of convenience or time taken to perform a task. If an individual believes that the recommended protective behavior is effective, that the response cost is acceptable, and that they have the ability to take the necessary action, then they are more likely to undertake the protective behavior.

2.2. *Extending the PMT for the personal computing security arena*

Many information security research models are directly derived from PMT, whereas others (e.g., Bulgurcu et al., 2010) draw from the more general Theory of Planned Behavior (TPB) (Ajzen and Fishbein, 1980) that offers a view of how behavioral and control beliefs direct the intentions of the individual. Security studies that include a comprehensive set of the original PMT constructs are generally able to explain 0.34–0.50 of the variance in a studied population. While this is greater than studies using TPB have been able to achieve (Sommestad and Hallberg, 2013), there is still scope to extend PMT to increase its explanatory capability in the home computer security domain.

Previous research that has adapted and extended PMT to reflect the personal computing security domain includes studies by Johnston and Warkentin (2010) and Anderson and Agarwal (2010). Johnston and Warkentin (2010) explored the role of social influence and found that it had a stronger relationship with intentions to perform security behaviors than either response efficacy or self-efficacy. Anderson and Agarwal (2010) explored the roles of both social influences and psychological ownership and found that broadening the consideration of influences on security intentions beyond the PMT constructs was of value in helping to improve personal computing security behavior.

3. Model and hypotheses

This research aims to improve understanding of personal computing security behavior by proposing and testing a research model, illustrated in Fig. 1, which is applicable to both home computer user and mobile device user behavior. In the proposed model, we extend the core PMT model in a several ways. First, people's opinions and behavior are likely to be influenced by others. Social and peer influences were included in the TPB as subjective norm (Ajzen and Fishbein, 1980). The TPB was later extended by Sheeran and Orbell (1999) to include descriptive norm. Our model incorporates both subjective and descriptive norm: where subjective norm is defined as to a user's beliefs as to whether others want them to perform security behaviors and descriptive norm refers to what a user believes most other people do in terms of protecting their devices. These external influences have been included in the model to better represent drivers of security related behavior.

Psychological ownership refers to the relationship between a person and an object, in which the person perceives a connection with the object (Pierce et al., 2003). Psychological ownership was included as an additional determinant of security related intentions to account for feelings of psychological ownership potentially being associated with sense of responsibility (Beaglehole, 1932), in this case for the device and the software and information it contains, and thus associated with differing levels of security related behaviors (Anderson and Agarwal, 2010; Van Dyne and Pierce, 2004).

The potential role of prior experience with information security breaches is also included as it may influence future threat appraisal (Maddux and Rogers, 1983). Finally our research model includes security behavior, which is a valuable addition as it addresses the call for more use of measures of actual behavior (Crossler et al., 2013).

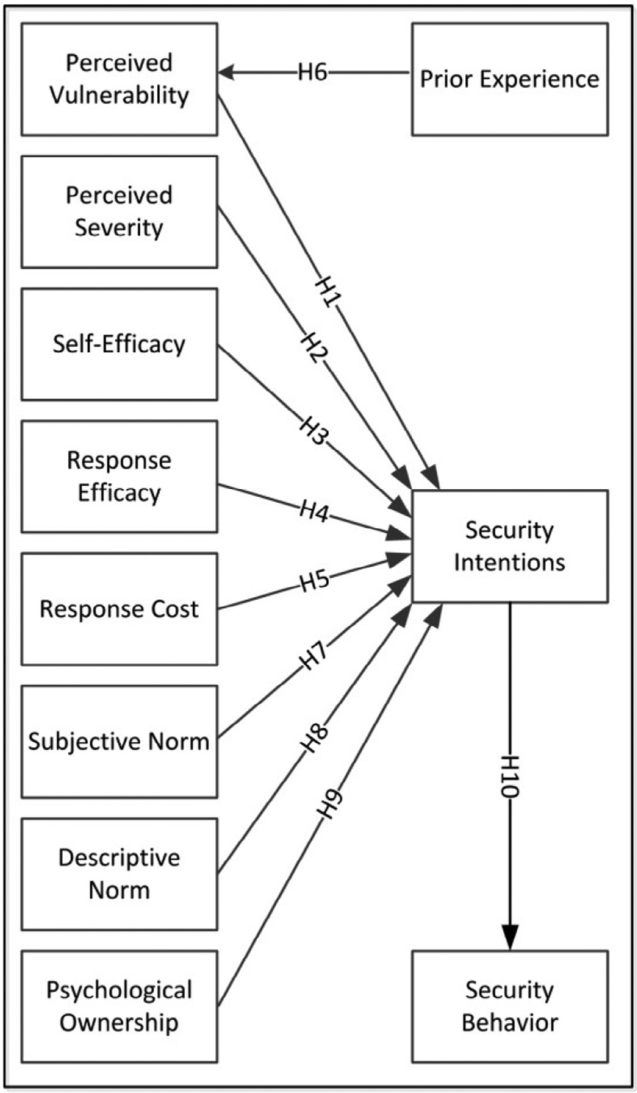


Fig. 1 – Research Model.

The model has been designed to provide a more complete understanding of user security behavior in the personal computing domain than the models used in previous studies such those of Anderson and Agarwal (2010) and Tu et al. (2015). While recognizing the potential value of also considering social norms and psychological ownership, it includes a more extensive set of the PMT (Rogers, 1975, 1983) constructs and extends beyond security intentions to model actual behavior.

3.1. *PMT-related hypotheses*

Although Rogers (1983) added perceived rewards associated with not performing the recommended behavior, relatively few studies have explored its role in determining protection motivation. Abraham et al. (1994) have suggested that rewards and response cost can be operationalized as a single construct by rewording. Based on this, we did not consider the role of rewards in this study.

Threat appraisals have been found to predict security intentions in some studies, although there have been mixed findings. Perceived vulnerability to threat refers to users' subjectively estimated probability that a security threat will occur and in this study perceived vulnerability is defined as the extent to which a user believes they are likely to experience security threats to their personal computing device. Perceived vulnerability to threats has generally been found to influence security behavior in the organizational domain (Ifinedo, 2012; Ng et al., 2009; Siponen et al., 2014; Workman et al., 2008), but there have been less consistent findings about its impact on personal information security behavior. For example, although Liang and Xue (2010), Chenoweth et al. (2009) and Claar and Johnson (2012) found the anticipated positive influence, Crossler's (2010) study found that perceived vulnerability unexpectedly had a negative influence on security behavior. Also, neither Woon et al. (2005), Zhang and McDowell (2009) nor Tsai et al. (2016) observed any effect. Despite the mixed previous findings in the personal computing domain, consistent with the relationship proposed by PMT (Rogers, 1983), we hypothesize that:

H1. *Perceived vulnerability will positively influence personal computing security intentions*

In this study, we define perceived severity as the extent to which users believe that the consequences of threats to their personal computing device would be detrimental. In the organizational domain, perceived severity has generally been found to influence security intentions (e.g., Posey et al., 2015; Siponen et al., 2014; Vance et al., 2012). However, some authors believe that there are differences in threat appraisal influences in the personal computing domain and that they are associated with more emotional responses to threats (Liang and Xue, 2010; Mwagwabi et al., 2014; Zhang and McDowell, 2009). Consistent with this, findings on the role of perceived severity have been somewhat mixed in the personal computing domain. Woon et al. (2005) found that personal computing users are more likely to enable wireless security measures if they believe a breach on their home wireless network would be detrimental. In a study of BYOD policy compliance, Crossler and Bélanger (2014) found that perceived severity was positively related to security behaviors. However, Zhang and McDowell (2009) found that it did not significantly predict password security behavior and Tsai et al. (2016) unexpectedly found that perceived severity had a negative influence on the security intentions of personal computing users.

Despite the lack of clarity around this relationship, we propose that consistent with PMT (Rogers, 1983), users will be more likely to intend to take protective measures with their personal computing device if they believe that the consequences of threats would be severe, and hypothesize that:

H2. *Perceived severity will positively influence personal computing security intentions*

Coping appraisal generally plays a much clearer role in positively influencing security intentions. In an organizational context, intention to comply with policies has been shown to be influenced by self-efficacy as well as response efficacy (e.g. Herath and Rao, 2009; Ifinedo, 2012). Studies of employees' security behavior when dealing with email messages or attachments have shown the importance of both self-efficacy (Ng et al., 2009) and response efficacy (Herath et al., 2014).

In the non-work context, LaRose et al. (2008) found that of the factors they studied, self-efficacy and response efficacy were the most important to promote secure behavior online. Tu et al. (2015) found that both self-efficacy and response efficacy positively influenced intention to protect mobile devices. Both self-efficacy and response efficacy have also been shown to influence intention to use anti-spyware software (Liang and Xue, 2010), intention to comply with password guidelines (Mwagwabi et al., 2014), enabling of firewalls (Woon et al., 2005) and frequent backing up (Crossler, 2010). One of the few exceptions to this pattern is Tsai et al. (2016). They found that while response efficacy was the second strongest predictor of security intentions in their model, the relationship between self-efficacy and general security intentions was not significant, suggesting that there is a still a need for further study to fully understand this relationship. Consistent with the majority of previous research we hypothesize that both self-efficacy and response efficacy will have positive influences on the security intentions of personal computing users:

H3. *Self-efficacy will positively influence personal computing security intentions*

H4. *Response efficacy will positively influence personal computing security intentions*

Response cost refers to not only financial cost, but also to any time, effort or inconvenience that the user may associate with the protective behavior. These costs often reduce behavioral motivation as the individual may perform some kind of cost-benefit analysis before proceeding with an action. Response cost has been shown to play an important role in the personal computing domain, such that increases in perceived response cost negatively influence intentions to perform security behaviors (Liang and Xue, 2010; Mwagwabi et al., 2014; Woon et al., 2005). Thus, we hypothesize that:

H5. *Response cost will negatively influence personal computing security intentions*

3.2. Prior experience with a security incident

Prior security threat experience is often left out of PMT based security research in spite of the fact that this factor was presented as a relevant source of information shaping threat appraisal in the revised PMT model (Rogers, 1983).

Personal experience with exposure to threats is considered to be another form of acquired knowledge that could affect perceived vulnerability (Weinstein et al., 2000) and through it, behavior. Consistent with this, in the organizational information security domain, Boss (2007) found that both personal experience and knowledge about others' exposure to information security threats influenced perceived vulnerability. The role of previous experience with security threats may be all the more crucial in a home user environment, as personal computing users may have had little or no security awareness training (Furnell et al., 2007), and hence may depend more on personal experience when shaping their own behaviors and responses.

Some prior research has explored the role of previous security threat experience in the context of personal computing. Tsai et al. (2016) found that prior experience directly predicted general behavioral security intentions. Lee et al. (2008) found that prior experience influenced intention to adopt virus protection. In the context of password security, Mwagwabi et al. (2014) found that prior exposure to hacking influenced perceived vulnerability to password related threats. We define prior experience as prior exposure to an information security breach, experienced by a user, and propose that if a user has experienced a breach such as having an online account hacked the experience should elevate their perceived vulnerability. Therefore, it is hypothesized that:

H6. *Prior experience of a security breach will positively influence perceived vulnerability*

3.3. *Social and peer influences*

Subjective norm refers to an individual's perceptions as to whether significant others/peers desire them to perform a behavior. It has been found to be a significant determinant of behavioral intention (Ajzen, 1991; Taylor and Todd, 1995). Descriptive norm refers to perceptions regarding what an individual believes most other people do. It has been found to be an additional determinant of behavioral intention beyond the TPB constructs (Rivis and Sheeran, 2003).

There has been little research on the role of subjective norm or descriptive norm in personal information security behavior but it is likely that they are pertinent, because the formal approaches to improving security behavior that organizational users are exposed to are not found in the personal use sphere (Anderson and Agarwal, 2010; Tu et al., 2015). Devices and software are supplied with little or no documentation, and users are expected to independently seek any further information from online resources. Usability developers strive for products that a new user is able to simply pick up and immediately start operating. This initial ease of use, however, comes at a cost as the users may have gaps in their security knowledge. These gaps can then be filled by discussing products with friends and relatives, thus heightening the potential role of subjective norm and descriptive norm.

Anderson and Agarwal (2010) considered both and found that subjective norm influenced intention to perform security related behaviors on home computers, but not those associated with protecting the Internet. Conversely, descriptive norm was a significant determinant of intention to perform security behaviors to protect the Internet, but not to protect one's own home computer. More recently, Tu et al. (2015) also explored the role of social influences on protection against personal device theft and found that they played an important role in determining users' knowledge of responses to threat, perceptions of the degree of threat and intentions to take protective action. Similarly, Tsai et al. (2016) showed that subjective norm had a strong effect on security intentions, and called for future work to explore the role of descriptive norm. From this we hypothesize that:

H7. *Subjective norm will positively influence personal computing security intentions*

H8. *Descriptive norm will positively influence personal computing security intentions*

3.4. *Psychological ownership*

Prior research has considered the role of feelings of psychological ownership in shaping an individual's behaviors and attitudes. This for instance has been studied in the context of employee's behaviors in a work role (Van Dyne and Pierce, 2004). Psychological ownership is the phenomenon experienced when an individual develops possessive feelings toward a particular target, whether that be a tangible or an intangible object (Beaglehole, 1932). In this study, psychological ownership refers to the extent to which a user feels ownership of a computing device and the software and information it contains, such that it becomes an "extension of the self" (McCracken, 1986). Beaglehole (1932) also suggests that these feelings of ownership trigger a sense of responsibility for the target. This sense of responsibility may be manifested in differing levels of security related behaviors.

In an organizational context, Van Dyne and Pierce (2004) proposed that psychological ownership would be related to extra, volitional behaviors. These discretionary actions such as volunteering to help others are intended to benefit the organization: the target of the feelings of ownership. At home, security behaviors are neither mandated nor checked, and may be analogous to this situation as discretionary activities intended to preserve the security of the device and information. Consistent with this, Anderson and Agarwal (2010) proposed that psychological ownership of both one's own computer and the Internet are positively associated with behavioral intentions to protect them. They found that home users had high levels of psychological ownership for their computers and that this weakly influenced their intentions to protect their computer. Their participants had lower levels of psychological ownership of the Internet, but a relationship was also found with intentions to protect the Internet. Thus we hypothesize that:

H9. *Psychological ownership will positively influence personal computing security intentions*

3.5. *Measures of actual behavior*

Problems with the security behavior of home computer users have been reported widely (Howe et al., 2012). Although less is known about the security behavior of mobile users (Mylonas et al., 2013), it is an emerging issue (Androulidakis, 2016). Much of the prior work on behavioral information security employs intention based models that use behavioral intention as a surrogate for actual behavior; these are largely based on models such as TPB (Ajzen and Fishbein, 1980) and PMT (Rogers, 1983), which assume that behavior is predicted by behavioral intentions. This assumption continues to inform model development in information security, in spite of reports that it is not uncommon to observe that individuals often fail to act in accordance with their behavioral intention (Ajzen et al., 2004). Thus further understanding of the relationship between intentions and actual behavior in the home computer security domain is required.

Our proposed research model includes a relationship between security intentions and actual security behavior to reflect the extent to which intentions translate into actual behavior. Several previous information security studies provide evidence to support this extension of the model. In the organizational security domain, Siponen et al. (2014) found that intention to comply with security policies had a strong influence on actual compliance. In the personal computing domain studies by Liang and Xue (2010) and Shropshire et al. (2015) have confirmed the relationship, therefore, we hypothesize that:

H10. *Security intentions will positively influence information security behavior*

3.6. Different personal computing environments: home computer versus mobile device

Personal computing was previously largely restricted to desktop and laptop computers. However, the use of smartphones and tablets to access and store personal data, and for tasks such as shopping and banking is growing rapidly (Dulaney et al., 2014). Although in the past users have been reluctant to undertake financial transactions on their smartphones (Chin et al., 2012), banks and businesses are investing significantly in the creation of user friendly applications to encourage customers to access their services using smartphones and tablets. Gartner Inc. predict that “by 2018, more than 50% of users will go to a tablet or smartphone first for all online activities” (Dulaney et al., 2014, p. 2).

In a mobile device environment, many functions are operationalized differently. This is due to a combination of the different operating environment (i.e. on the move), different constraints (e.g. battery life, network speed) and different interfaces (e.g. touch screen instead of keys). The predominantly touch screen interface may also have implications for individual security behavior. Limited screen-space and on screen keyboard render it difficult to utilize special characters or even capital letters and thus make complying with recommendations for password strength more difficult. Users on smartphone platforms are taught that there are different rules for smartphones, for example, by companies who forgo the password complexity rules when logging in from a mobile device (Facebook, 2016). At the operating system level, mobile platforms contain very advanced and highly granular access control models (e.g. Google Inc, 2016). This results in a large number of prompts which may not be intuitive to the user, potentially habituating them to simply click through (Anderson et al., 2017).

With the shift to increased use of mobile devices for personal computing comes the need for more understanding of how the information security behavior for different device types is influenced. This is particularly important as there have been many reports that users display less safe behavior with mobile devices than with their home computers (Kelley et al., 2012; Mylonas et al., 2013; Wood et al., 2015). For example, Mylonas et al. (2013) reported that the security awareness of mobile device users is limited and Kelley et al. (2012) found that they ignore security messages. A Symantec report (Wood et al., 2015) noted that many users only consider security threats with respect to their home computers.

In order to better understand the potential role of device type in personal computing security behavior, the research model was evaluated in the context of both home computer use and mobile device use, to investigate whether the context or environment may influence the perceptions and ultimately security behaviors of users. Thus, we propose the following research question:

RQ1: Do the determinants of personal computing security behavior differ between home computer and mobile device use?

4. Method

In this study, home computers are considered to include both desktop and laptop machines. Whilst laptops provide greater flexibility in terms of the locations they can be used, they offer essentially the same functionality and operating environments as desktops, therefore the desired security behavior is largely the same. Smartphones and tablets differ from home computers in that they utilize apps from an app-store rather than regular “boxed” software and provide a touch screen interface; in this study these are categorized as mobile devices. Although there are also devices that overlap these two categories (e.g. Microsoft Surface Pro), these are not included in the study.

The target population for the study was personal computing users, and data to test the proposed research model was collected from two groups of users: home computer (desktop/laptop) users and mobile device (smartphone/tablet) users via an anonymous online questionnaire.

4.1. Sample and data collection procedure

A third party recruiting company was used to recruit participants from a wide spectrum of backgrounds including age, gender, level of education, computer skills and computer security knowledge. The recruiting company used census balanced random sampling to identify potential participants from their panel members, and they were then contacted via email and invited to complete the questionnaire, which was hosted on SurveyMonkey. All participants were located in the United States, aged 18 or over and had both a home computer and a mobile device. Respondents first answered several background questions about themselves and provided basic usage information for both types of devices. They were then randomly allocated to one of two groups to answer more detailed security perceptions and usage questions relating to either home computer, or mobile device security.

4.2. Measures

The constructs measured were: prior experience, perceived vulnerability, perceived severity, self-efficacy, response efficacy, response cost, subjective norm, descriptive norm, psychological ownership, security intentions and security behavior. To ensure validity and reliability of the items used to measure the model constructs, we selected items that had been validated in relevant behavioral security research studies wherever possible. These items were slightly reworded for the personal computing domain as necessary. Appendix A provides a list of all of the items and their sources, and as can be seen only the items used to measure psychological ownership had to be newly created. The two sets of items (for home computers and mobile devices) were kept consistent and varied only in the device that was referred to: either "smartphone / tablet" or "home computer / laptop". Given the broad range of threats to which personal computing users may be subject, the introductory material and the questionnaire items referred to security breaches in general, but gave examples of possible threats and their impacts. (Table A1)

The items to measure each of the constructs of interest, apart from prior experience and security behavior, were measured on 7 point Likert scales from 1 "Strongly Disagree" to 7 "Strongly Agree". The item used to measure prior experience was measured on a scale of 0 if the participant answered "No" to having experienced a security breach or 1 (low impact) to 5 (high impact) depending on the extent of the impact of the breach. Security behavior was measured using five items each of which asked whether the participant about whether or not they performed a specific common security behavior. These items were chosen as representative of recommended personal computing security behaviors and each was answered as 1 for "Yes" or 0 for "No" or "Unsure". A composite variable was calculated as the sum of the responses to the five items.

The initial items were pilot tested with several members of the target population and in response to their feedback minor changes were made to the wording of several items and to the survey interface to improve understandability.

4.3. *Data screening*

Data screening was undertaken to identify participants who had not fully engaged with the questionnaire and thus impacted data quality. This screening involved removal of responses with zero variance, and responses where questionnaire completion took either below half of the minimum estimated completion time or twice the maximum estimated completion time (Huang et al., 2012).

5. Results

A total of 629 valid responses (62.5% female and 37.5% male) were used in the analysis: 322 from home computer respondents and 307 from mobile device respondents. Table 1 provides background information about them. The age distribution of the participants differed from that of the US population at the time the data was collected in that there was a greater representation of users in the 55–64 age group, and a lower representation of those under 34 (Kaiser Family Foundation, 2014). There were no significant differences between the home computer respondents and mobile device respondents in terms of gender (χ^2 [1, N = 624] = 1.643; p = 0.200) or age (χ^2 [6, N = 623] = 2.011; p = 0.919).

The majority of participants rated their skill with computers as good or excellent (64.7%), however, only 18.9% had previously received any information security training. There were no significant differences between home computer respondents and mobile device respondents in either self-rated skill with computers (χ^2 [4, N = 629] = 1.417; p = 0.841) or whether they had received information security training (χ^2 [1, N = 629] = 0.691; p = 0.406).

Table 1 – Background information about participants.

	Home computer respondents	Mobile device respondents
Gender		
Male	39.9%	35.0%
Female	60.1%	65.0%
Age		
18–24	2.5%	2.9%
25–34	8.2%	7.9%
35–44	12.3%	15.4%
45–54	19.8%	19.7%
55–64	33.0%	33.1%
65 or older	24.2%	21.0%
Self-rated skill with computers		
Poor	0.6%	0.7%
Below average	3.1%	2.9%
Average	29.5%	33.9%
Good	46.6%	44.0%
Excellent	20.2%	18.5%
Previous information security training		
Yes	20.2%	17.6%
No	79.8%	82.4%

The model was tested using Partial Least Squares (PLS), a structural equation modeling method for complex predictive models and theory building (Barclay et al., 1995; Chin, 1998). SmartPLS 2.0 (Ringle et al., 2005) was used to estimate the model and the bootstrap re-sampling method (using 1000 samples) was used to determine the significance of the paths in the structural model. PLS was the preferred analytical technique of this study as Shapiro–Wilk tests were significant, showing that the measurements were not normally distributed. According to Hair et al. (2014), PLS is more appropriate with non-normally distributed data.

Before evaluating the models, we conducted two common method variance (CMV) tests to examine whether common method bias was a concern (Podsakoff et al., 2003). First, an explanatory factor analysis of all items extracted nine factors explaining 77.61% of the variance, with no single factor accounting for significant loading (at the $p < 0.05$ level) for all items. Further, an unmeasured latent method factor was added and all items were loaded on both their theoretical constructs and the method factor (Bagozzi, 2011). This model fit well: χ2 [951] = 2855.81, p < .00, RMSEA = .056, SRMR = .033, and CFI = .99. All item loadings on the common method factor were much lower than the loadings on their respective constructs, and most loadings on the common method factor were not significant. Therefore, CMV is probably not a concern in this data set.

First construct validity of the proposed measurement model were determined, and once a satisfactory measurement model was obtained, the structural model was estimated for both home computers and mobile device use. The measures of reflective constructs from the home computer dataset demonstrate good psychometric properties. Convergent validity was confirmed by meeting the following criteria (Gefen and Straub, 2005; Hulland, 1999): the loadings of each item were all significant and above the cut-off value of 0.60 (see Appendix B Table B1); the composite reliabilities (CR) and Cronbach's Alphas (CA) of all constructs were above 0.70 (Table 2); the average variance extracted (AVE) of all constructs was above the threshold value of 0.50 (Table 2). Discriminant validity was established by ensuring that the square root of AVE for each construct exceeded the correlations between that construct and any other construct (see Appendix B Table B2). Following the same process, we also examined the data from the mobile device users, and the results show that reflective measures have similarly good psychometric properties (see Table 2 and Appendix B Table B1 and Table B3).

Next, the structural model was examined. The results for home computer and mobile device users are shown side by side in Fig. 2. The majority of the hypotheses were supported for each group, and for all but one hypothesis the outcomes were the same for each group. The model explained a substantial amount of the variability in security intentions (60% for home computer users and 62% for mobile device users), but only 11% of the variability in security behavior was explained for home computer users and 22% for mobile device users.

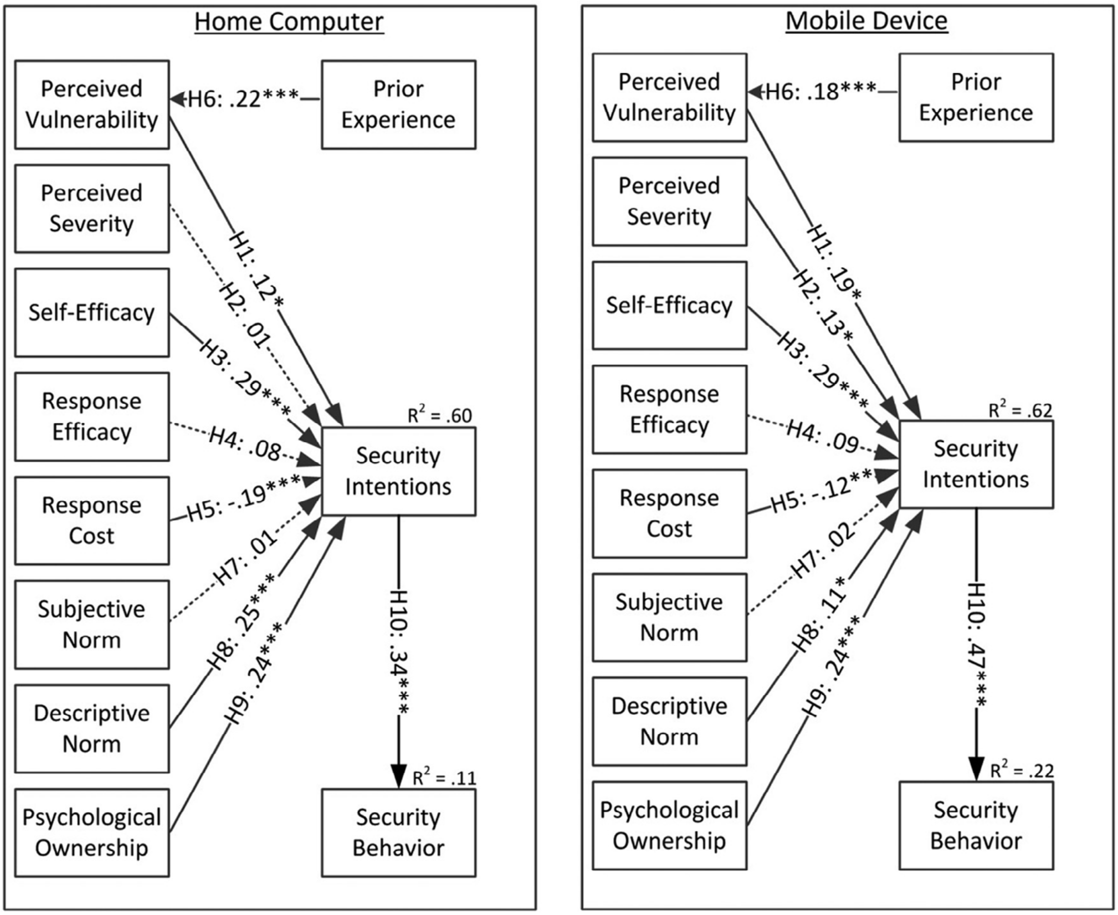
As hypothesized, perceived vulnerability positively influenced security intentions for both the home computer users and the mobile device users, thus H1 was supported. A mixed result was however obtained for H2; while perceived severity did not significantly influence home computer user intentions to undertake security behaviors, it did for mobile device users; therefore H2 was only partially supported.

Table 2 – Construct validity and reliability.

Constructs	Home computer model			Mobile device model		
	CA	CR	AVE	CA	CR	AVE
Perceived vulnerability	.92	.94	.72	.93	.95	.75
Perceived severity	.94	.95	.78	.94	.96	.76
Self-efficacy	.90	.92	.67	.92	.94	.71
Response efficacy	.94	.95	.84	.95	.97	.87
Response cost	.95	.96	.76	.95	.96	.76
Prior experience*	-	-	-	-	-	-
Subjective norm	.94	.96	.88	.96	.97	.92
Descriptive norm	.94	.95	.84	.94	.96	.84
Psychological ownership	.91	.93	.65	.92	.94	.68
Security intentions	.96	.97	.89	.96	.97	.90
Security behavior	-	-	-	-	-	-

*As a single item was used to measure prior experience and a composite score was used to measure security behavior, CA, CR and AVE were not computed.

With respect to coping appraisals, both self-efficacy and response cost significantly influenced security intentions



*Note: *p < .05, **p < .01, ***p < .001.*

Fig. 2 – Structural model results.

Table 3 – Predictive relevance (Q^2).

	Home Computer Model Q^2	Mobile Device Model Q^2
Perceived vulnerability	.72	.75
Perceived severity	.78	.79
Self-efficacy	.67	.71
Response efficacy	.84	.87
Response cost	.76	.76
Subjective norm	.88	.92
Descriptive norm	.84	.84
Psychological ownership	.65	.68
Security intentions	.89	.90

as proposed, but response efficacy did not have a significant effect. Thus H3 and H5 were supported but H4 was rejected.

Previous experience with information security incidents was included in the research model, and proposed to have an impact on threat appraisal by influencing perceived vulnerability (Maddux and Rogers, 1983). As hypothesized, prior experience had a positive influence on perceived vulnerability for both home computer and mobile device use, and H6 was, therefore, supported.

Mixed results were obtained with respect to the role of social influences. Subjective norm did not influence security intentions for either type of user, but descriptive norm had a significant influence on security intentions for both home computer security and mobile device security. Therefore, H7 was rejected but H8 was supported.

As hypothesized, psychological ownership had a significant positive influence on security intentions for both the home computer use and the mobile device user, so H9 was supported. H10 was also supported for both types of device use as security intentions significantly influenced security behavior.

The Stone–Geisser (Q2) test was also conducted to assess the predictive quality of our model (Geisser, 1975; Stone, 1974). As shown in Table 3, all values of Q^2 are above 0. Therefore, our model has good predictive relevance.

To further explore whether the determinants of personal computing security behavior differ between home computer and mobile device use, cross-group comparisons were conducted. Specifically, the formula of Keil et al. (2000) was used to assess the statistical differences of the path coefficients between home computer and mobile device. These findings are summarized in Table 4 and show that there were significant differences in path coefficients between home computer users and mobile device users for all proposed relationships that were supported except for the relationships between self-efficacy and security intentions, and psychological ownership and security intentions, which were of equal strength.

6. Discussion

As proposed in the PMT (Rogers, 1975, 1983), perceived vulnerability, self-efficacy and response cost were all important in determining personal computing security intentions. However, perceived severity was only found to play a role in mobile device security behavior and response efficacy did not influence security intentions in either group.

Although perceived vulnerability to threats has generally been found to influence security behavior in organizational settings (Ifinedo, 2012; Ng et al., 2009; Siponen et al., 2014; Workman et al., 2008), there have been mixed findings about its impact on personal computing behavior. The current findings are consistent with those of Liang and Xue (2010), Chenoweth et al. (2009) and Claar and Johnson (2012). One possible explanation for the mixed findings is that vulnerability may mean different things to users depending on their environment (Dang-Pham and Pittayachawan, 2015).

The previous mixed findings about the role of perceived severity in personal computing were echoed in the results of this study, with it only being a determinant of security intentions for mobile device protection, but not for home computer protection. One explanation for why only perceived severity only influenced security intentions for the mobile device users lies in the concept of connectedness. Connectedness is a positive emotional appraisal which is characterized by a feeling of staying in touch within ongoing social relationships (Rettie, 2003). When home computers are used for communication this is typically asynchronous in nature, such as social media or email. Mobile

Table 4 – Path coefficient comparison between home computer users and mobile device users.

Path	Home Computer Users (N = 322)		Mobile Device Users (N = 307)		P value	Sig?
	Standardized path coefficient	S.E.	Standardized path coefficient	S.E.		
PV → SI	.12	.05	.19	.08	$p < .001$	Yes
PS → SI	.01	.04	.13	.06	$p < .001$	Yes
SE → SI	.29	.07	.29	.05	$p > .05$	No
RE → SI	.08	.07	.09	.06	$p < .05$	Yes
RC → SI	−.19	.04	−.12	.04	$p < .001$	Yes
PE → PV	.22	.06	.18	.05	$p < .001$	Yes
SN → SI	.01	.05	.02	.06	$p < .05$	Yes
DN → SI	.25	.06	.11	.05	$p < .001$	Yes
PO → SI	.24	.07	.24	.06	$p > .05$	No
SI → SB	.34	.06	.47	.05	$p < .001$	Yes

Note: PE = prior experience, PV = perceived vulnerability, PS = perceived severity, RC = response cost, RE = response efficacy, SE = self-efficacy, DN = descriptive norm, SN = subjective norm, PO = psychological ownership, SI = security intentions, SB = security behavior.
Note: In both models, the path RE - > SI and SN - > SI are not significant. Therefore, the significant result of comparison test may not be meaningful.

devices on the other hand are used for real-time communication, which enhances a feeling of connectedness which may in turn trigger intentions to take protective actions if any threat to this feeling is perceived as severe. Thus, the relationship between perceived severity and security intentions may be moderated by need for connectedness.

The positive effect of self-efficacy and negative effect of response efficacy on security intentions for both home computer users and mobile device users is consistent with previous research in the personal computing domain (Liang and Xue, 2010; Mwagwabi et al., 2014; Woon et al., 2005). The lack of impact of response efficacy on security intentions for either device type was surprising, as the relationship has been consistently observed in both organizational and personal computing settings. In their meta-analysis of PMT security studies, Sommestad et al. (2015) found that relationship strength was lower when the behaviors being investigated were more general, compared to studies that looked at a specific behavior such as enabling a firewall. In the current study participants were asked about a range of common security behaviors, so this may have contributed to the results, but this seems unlikely to be the only reason.

The role of prior experience with security incidents in influencing perceived vulnerability was also explored in this study. We found that when a personal computing user has previously experienced a security breach they are more likely to feel vulnerable to threats. It appears that this experience provides acquired information that changes how people assess their vulnerability, countering a tendency to underestimate it (West, 2008).

In addition to examining relationships associated with PMT (Rogers, 1975, 1983), this study extended the core PMT model, and the inclusion of the additional constructs provided useful insight into personal security behavior. Although both subjective norm and descriptive norm were expected to influence intentions to practice security behavior, the results indicate that in both contexts, descriptive norm is a significant predictor of security intentions, yet subjective norm is not. The lack of influence of subjective norm suggests that in the personal computing domain, whilst users are influenced by what they see others do, they are not currently as aware of any expectations about security behavior that may exist, and even if they are aware of them, are not motivated by them. This possible explanation is consistent with the relatively low average levels of subjective norm in this study (home computers 3.97 and mobile devices 3.77 out of 7) and the weak relationships found by Anderson and Agarwal (2010). The findings of this study differ from those in the organizational domain where expectations may be very explicit, and where the "significant others" include authority figures as opposed to just friends and family. Godlove (2012) noted that direct supervisors were more important determinants of the effect of subjective norm on security intentions than peers, and in the personal computing domain there are no formal supervisors.

Descriptive norm, however, is simply a perception of what others do. Thus, it can be formed independently and need not depend on social interaction or conversations. In both home computer and mobile contexts, levels of descriptive norm were higher than those of subjective norm (5.29 and 4.43 out of 7) and found to be significant predictors of security intentions. Furthermore, the strength of this relationship is much stronger in the home computer context, which is consistent with the greater representation of home computers in security information/media coverage. It is possible that this leads to more complete normative beliefs around home computers, which influenced the results.

The results of this study confirmed the importance of psychological ownership in influencing security behavioral intentions in the personal computing domain, such that the higher the level of psychological ownership felt, the more likely users were to intend to protect their home computers and mobile devices. The relationship strengths are higher than those reported in Anderson and Agarwal (2010) and relatively consistent with those in a recent study that looked at how psychological ownership influences disclosure of personal data (Cichy et al., 2014).

The model explained a greater proportion of the variability in home computer security intentions than that explained in the study by Anderson and Agarwal (2010) (60% versus 43%), and also explained slightly more of the variability in mobile device security intentions than was explained in the study by Tu et al. (2015) (62% versus 58.6%). This suggests that using PMT (Rogers, 1975, 1983) as a base for this kind of research, but extending it to obtain greater explanatory ability is a valuable approach to gaining greater understanding of personal computing security behavior.

As predicted, intentions to perform security behaviors were shown to significantly influence actual security behavior for both home computer users and mobile device users. There was, however, a significant difference in the strength of the relationship between the two types of device, with the relationship being stronger for mobile devices, and hence with a greater proportion of the variance in behavior explained. The relatively low levels of ability to explain security behavior are consistent with other personal information security research. For example in previous studies, intentions to adopt new security software explained 24.8% of adoption behavior (Shropshire et al., 2015), and 21% of spyware software adoption behavior (Liang and Xue, 2010). In studies where intentions prove to have a stronger relationship with actual behavior there has generally been training and/or fear appeals used (e.g., Boss et al., 2015). Sheeran (2002) notes that one factor that determines how well intentions predict behavior is whether the behavior being predicted is a single action or an outcome that can only be achieved by performing a variety of single actions. Intentions are likely to be superior predictors of single actions. Securing a personal device generally requires multiple actions, and it is perhaps not surprising that the ability to explain a lot of the variance in security behavior been limited.

The differences between the two domains are, however, of interest. A factor that may moderate the relationship between intention and behavior is habit (Dupuis et al., 2016), as research has shown that the relationship is weaker for behaviors that are more routine and stable (Wood et al., 2002). Home computer security behaviors appear to be more stable and entrenched than mobile device security behaviors (Imgraben et al., 2014; Mylonas et al., 2013; Tu et al., 2015) explaining the weaker relationship.

6.1. *Limitations and future research*

The mixed findings around some relationships are of particular interest as these generate new research questions and highlight areas for refinement of the research model. In particular, the role of perceived severity and its link to security intentions is of note, as this relationship was only significant for mobile device users. More research is required around this domain to understand how factors such as device usage pattern and feelings of "connectedness" may influence intentions and the enactment these protective behaviors. Given the findings on the roles of subjective norm and descriptive norm it would also be useful for future work to investigate how personal computing users obtain knowledge about security, and how this links with their mental models and normative beliefs.

While the proposed model explained variability in intention to perform security behaviors relatively well for both types of device, it was much less successful in explaining the security behavior of home computer users. Future research should investigate factors that influence security behavior directly in order to obtain a more complete picture of what determines information security behavior. These factors may include habit (Dupuis et al., 2016), need for connectedness (Rettie, 2003) and personality (Shropshire et al., 2015).

Whilst the current study goes beyond intentions to actual behavior it is limited by its reliance on self-report measures of security behavior with data collection at only a single point of time. Consistent with the call by Crossler et al. (2013) for more focus on actual behavior as opposed to security intentions, the measurement of security intentions and behavior also require further attention. The availability of validated measures of intention such as the Security Behavior Intentions Scale (SeBIS) (Egelman and Peer, 2015), will facilitate cross study comparisons; however, to improve understanding of information security behavior more availability of standard validated measurement instruments and methods of direct measurement are needed. Direct observation of user behavior is an under-explored research approach, which has potential to provide a greater insight into ongoing behavior than self-report scales.

A further limitation of the study is that fear (an emotional feeling toward threat) was not included in the proposed model. Fear was included in the revised PMT (Rogers, 1983) and several recent studies have explored its potential mediating role (e.g., Boss et al., 2015; Posey et al., 2015). Differences in how security threat appraisals affect fear in different contexts may impact on security behavior.

6.2. *Implications for practice*

This research has considered significant factors leading to security intentions and behaviors and provided a much needed perspective on the under-researched home computer and mobile device segments. The findings when considered together shed light on the research question, revealing that there are possible differences in the determinants of personal computing security behavior between home computer and mobile device use. This suggests that knowledge and experience of security tasks may be tied to the operating context and users may not always generalize security knowledge across all computing devices. It is possible that this may lead to greater risks in the mobile environment if traditionally desktop applications are ported to a mobile environment without adequate real world security evaluation.

For developers and security professionals, there are two main practical implications from the research findings. First, it may be inadvisable to assume that any security knowledge or background developed by users in a home computer context will immediately translate to equivalent behavior in a mobile environment. All aspects of the computing experience, including user experience, software design and interface development should be adequately grounded in the appropriate target platform to ensure that results are as predicted and that users are not unwittingly exposed to increased risks.

Second, the research finding that users may have incomplete or inadequately developed normative beliefs is something that may be addressed practically. The potential for social norms to be targeted to improve security behavior has been demonstrated (Herath and Rao, 2009; Ifinedo, 2014), and in a personal computing security context, a positive step would be simply to advance from one-sided user guidance material toward communities of practice, combining the benefits of the shared pool of knowledge, with the social normative influence providing an extra boost to productive behaviors. The communication capabilities of any home computer or mobile platform provide ample functionality for interaction between users. However, what is lacking is a move from silos of knowledge like web forums, to fully integrated, real-time interaction, possibly frequented and mediated by representatives from vendors or other experts to reinforce positive behavior.

7. Conclusion

Personal computing users are vulnerable to information security threats as they need to independently make decisions about how to protect themselves, often with little knowledge of the technology involved or understanding of the implications. Whilst personal computing has previously been primarily associated with desktop and laptop computers, with the growth in use of tablets and smartphones to access and store important personal and financial information (Dulaney et al., 2014) there is a need for more information security research that focuses on security behavior associated with different device types. The study described in this paper attempts to improve understanding of personal computing security behavior by proposing and testing a model of personal computing security behavior that extends PMT (Rogers, 1975, 1983), to incorporate previous findings on the roles of psychological ownership and social influence (Anderson and Agarwal, 2010; Tu et al., 2015) and to explicitly include security behavior. We also believe that it is the first study to explicitly compare model performance over different device types, with the model being tested separately with home computer users and mobile device users in order to explore whether the determinants of personal computing security behavior differ between home computer and mobile device use.

The results of the study show that perceived vulnerability, self-efficacy, response cost, descriptive norm and psychological ownership all were important in determining personal computing security intentions and behavior for both home computer users and mobile device users. However, perceived severity was only found to play a role in mobile device security behavior and neither response efficacy nor subjective norm influenced security intentions for either type of user. These findings have both practical implications and implications for future research into personal computing behavior.

Appendix A

Table A1 – Items used to measure constructs (where *device* was either "smartphone / tablet" or "home computer / laptop").

Construct	Items
Prior experience (Mwagwabi et al., 2014)	Have you ever experienced a security breach (e.g. had your email account, online shopping account or banking account hacked into)? If yes, please indicate the degree to which that experience affected you (e.g. in terms of lost data, lost time, monetary losses, identify theft etc.)
Perceived severity (Ifinedo, 2012; Woon et al., 2005; Workman et al., 2008)	A security breach on my *device* would be a serious problem for me
	Loss of information resulting from hacking would be a serious problem for me
	Having my confidential information on my *device* accessed by someone without my consent or knowledge would be a serious problem for me.
	Having someone successfully attack and damage my *device* would be very problematic for me
	I view information security attacks on me as harmful
	I believe that protecting the information on my *device* is important
Perceived vulnerability (Ifinedo, 2012; Siponen et al., 2014; Woon et al., 2005)	I could be subject to a serious information security threat
	I am facing more and more information security threats
	I feel that my *device* could be vulnerable to a security threat
	It is likely that my *device* will be compromised in the future
	My information and data is vulnerable to security breaches:
	I could fall victim to a malicious attack if I fail to follow good security practices
Response cost (Woon et al., 2005; Workman et al., 2008)	Taking security measures inconveniences me
	There are too many overheads associated with taking security measures to protect my *device*
	Taking security measures would require considerable investment of effort
	Implementing security measures on my *device* would be time consuming
	The cost of implementing recommended security measures exceeds the benefits
	The impact of security measures on my productivity exceeds the benefits
Response efficacy (Woon et al., 2005)	Enabling security measures on my *device* will prevent security breaches
	Implementing security measures on my *device* is an effective way to prevent hackers
	Enabling security measures on my *device* will prevent hackers from stealing my identity
	The preventative measures available to stop people from getting confidential personal or financial information on my *device* are effective
Self-efficacy (Anderson and Agarwal, 2010)	I feel comfortable taking measures to secure my *device*
	Taking the necessary security measures is entirely under my control
	I have the resources and the knowledge to take the necessary security measures
	Taking the necessary security measures is easy
	I can protect my *device* by myself
	I can enable security measures on my *device*
Subjective norm (Adapted from Taylor and Todd, 1995)	Friends who influence my behavior think that I should take measures to secure my *device*
	Significant others who are important to me think that I should take measures to secure my primary *device*
	My peers think that I should take security measures on my primary *device*
Descriptive norm (Anderson and Agarwal, 2010)	I believe other people implement security measures on their *devices*
	I believe the majority of people implement security measures on their *devices* to help protect the Internet
	I am convinced other people take security measures on their *devices*
	It is likely that the majority of home computer users take security measures to protect themselves from an attack by hackers
Psychological ownership (Newly developed)	I feel a high degree of ownership for my *device* and its contents
	The information stored in my *device* is very important to me.
	I personally invested a lot in my *device* (e.g. time, effort, money)
	I personally invested a lot in the software/applications on my *device* (e.g. time, effort, money)
	When I think about it, I see an extension of my life in my *device*
	I have personalized my *device* to better suit the way I use it
	I see my *device* as an extension of myself
Security intentions (Adapted from Taylor and Todd, 1995)	I am likely to take security measures on my *device*
	It is possible that I will take security measures to protect my *device*
	I am certain that I will take security measures to protect my *device*
	It is my intention to take measures to protect my *device*
Security behavior (Developed using format of Liang and Xue, 2010)	I have installed security software on my *device*
	I have recent backups of my *device*
	I have enabled automatic updating of my computer software
	I use security software (anti-virus/anti malware)
	My *device* is secured by a password

Appendix B

Table B1 – Descriptive statistics and item loadings

	Home Computers			Mobile Devices		
Item	Mean	SD	Loading	Mean	SD	Loading
PE	1.13	1.48	-	1.09	1.44	-
PV1	4.83	1.51	.87	4.72	1.62	.85
PV2	4.40	1.63	.85	4.42	1.65	.89
PV3	4.71	1.58	.92	4.79	1.65	.91
PV4	4.41	1.47	.88	4.25	1.59	.85
PV5	4.49	1.49	.90	4.52	1.65	.89
PV6	5.61	1.42	.67	5.35	1.47	.80
PS1	5.93	1.36	.88	5.34	1.69	.87
PS2	5.87	1.42	.88	5.58	1.61	.91
PS3	6.11	1.26	.92	5.67	1.63	.91
PS4	6.12	1.24	.90	5.81	1.55	.93
PS5	6.29	1.10	.88	6.19	1.17	.83
PS6	6.40	.98	.84	6.01	1.32	.88
RC1	3.20	1.84	.85	3.30	1.66	.84
RC2	3.18	1.73	.86	3.51	1.57	.88
RC3	2.98	1.71	.91	3.36	1.60	.91
RC4	3.31	1.79	.87	3.61	1.65	.85
RC5	3.43	1.75	.86	3.69	1.57	.88
RC6	2.97	1.80	.87	3.49	1.66	.88
RC7	3.06	1.78	.88	3.47	1.54	.85
RE1	5.18	1.35	.93	4.89	1.33	.92
RE2	5.42	1.23	.92	5.05	1.29	.95
RE3	5.04	1.38	.91	4.83	1.41	.94
RE4	5.13	1.25	.91	4.81	1.40	.94
SE1	5.80	1.25	.85	5.18	1.37	.82
SE2	5.77	1.23	.85	5.39	1.38	.77
SE3	5.46	1.37	.90	4.77	1.62	.89
SE4	5.23	1.38	.82	4.64	1.55	.89
SE5	4.97	1.58	.62	4.56	1.65	.80
SE6	5.51	1.42	.84	4.92	1.54	.88
DN1	5.37	1.26	.89	4.58	1.44	.88
DN2	5.30	1.33	.94	4.40	1.55	.93
DN3	5.25	1.33	.93	4.39	1.53	.95
DN4	5.25	1.35	.91	4.35	1.54	.91
SN1	3.88	1.70	.92	3.70	1.61	.96
SN2	4.07	1.70	.95	3.85	1.69	.96
SN3	3.94	1.70	.95	3.77	1.59	.97
PO1	5.84	1.21	.83	5.31	1.41	.74
PO2	5.90	1.15	.83	5.28	1.53	.82
PO3	5.44	1.34	.89	4.86	1.66	.88
PO4	5.08	1.47	.79	4.15	1.80	.84
PO5	5.02	1.50	.79	4.13	1.83	.87
PO6	5.34	1.37	.81	4.68	1.66	.79
PO7	4.89	1.58	.73	4.04	1.85	.83
SI1	5.92	1.17	.94	4.94	1.44	.95
SI2	5.86	1.19	.95	5.09	1.37	.92
SI3	5.93	1.16	.95	4.84	1.57	.96
SI4	5.92	1.18	.93	4.96	1.53	.96
SB	3.72	1.33	-	2.20	1.60	-

Note: PE = prior experience, PV = perceived vulnerability, PS = perceived severity, RC = response cost, RE = response efficacy, SE = self-efficacy, DN = descriptive norm, SN = subjective norm, PO = psychological ownership, SI = security intentions, SB = security behavior.

Table B2 – Correlation between constructs and square-root of AVEs on diagonal (home computers).

	PE	SB	PV	PS	RC	RE	SE	DN	SN	PO	SI
PE	-										
SB	−.08	-									
PV	.22	.00	**.85**								
PS	−.02	.06	.38	**.88**							
RC	.15	−.19	.28	−.12	**.87**						
RE	−.06	.13	−.01	.24	−.19	**.92**					
SE	−.07	.35	.03	.28	−.33	.64	**.82**				
DN	−.07	.13	.27	.30	−.16	.35	.30	**.91**			
SN	.19	.03	.47	.22	.32	.09	.08	.27	**.94**		
PO	.02	.22	.28	.51	−.19	.47	.60	.36	.26	**.81**	
SI	−.10	.34	.22	.37	−.34	.50	.63	.52	.17	.62	**.94**

Note: PE = prior experience, PV = perceived vulnerability, PS = perceived severity, RC = response cost, RE = response efficacy, SE = self-efficacy, DN = descriptive norm, SN = subjective norm, PO = psychological ownership, SI = security intentions, SB = security behavior.

Table B3 – Correlation between constructs and square-root of AVEs on diagonal (mobile devices).

	PE	SB	PV	PS	RC	RE	SE	DN	SN	PO	SI
PE	-										
SB	−.03	-									
PV	.18	.14	**.86**								
PS	.10	.25	.52	**.89**							
RC	.24	−.17	.14	−.10	**.87**						
RE	.03	.38	.28	.43	−.09	**.94**					
SE	−.04	.45	.22	.30	−.23	.62	**.84**				
DN	.03	.24	.28	.26	.07	.48	.44	**.92**			
SN	.17	.19	.43	.35	.16	.36	.28	.48	**.96**		
PO	.10	.45	.41	.61	−.09	.58	.48	.34	.43	**.82**	
SI	.05	.47	.46	.54	−.19	.59	.62	.45	.39	.64	**.95**

Note: PE = prior experience, PV = perceived vulnerability, PS = perceived severity, RC = response cost, RE = response efficacy, SE = self-efficacy, DN = descriptive norm, SN = subjective norm, PO = psychological ownership, SI = security intentions, SB = security behavior.

REFERENCES

Abraham CS, Sheeran P, Abrams D, Spears R. Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of HIV infection. Psychol Health 1994;9(4):253–72.

Ajzen I. The theory of planned behavior. Organ Behav Hum Decis Process 1991;50(2):179–211. http://dx.doi.org/10.1016/0749-5978(91)90020-T.

Ajzen I, Fishbein M. Understanding attitudes and predicting social behaviour. Englewood Cliffs: Prentice-Hall; 1980.

Ajzen I, Brown TC, Carvajal F. Explaining the discrepancy between intentions and actions: the case of hypothetical bias in contingent valuation. Person Social Psychol Bull 2004;30(9):1108–21.

Anderson BB, Vance A, Jenkins JL, Kirwan CB, Bjornn D. It all blurs together: How the effects of habituation generalize across system notifications and security warnings. In: Davis FD, Riedl R, vom Brocke J, Léger P-M, Randolph AB, editors. Information systems and neuroscience. Cham: Springer International Publishing; 2017. p. 43–9.

Anderson CL, Agarwal R. Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions. MIS Quart 2010;34(3):613–43.

Androulidakis II. A multinational survey on users' practices, perceptions, and awareness regarding mobile phone security. In: Mobile phone security and forensics: a practical approach. Cham: Springer International Publishing; 2016. p. 15–28.

Bagozzi RP. Measurement and meaning in information systems and organizational research: methodological and philosophical foundations. MIS Quart 2011;35(2):261–92.

Barclay D, Higgins C, Thompson R. The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration. Technol Stud 1995;2(2):285–309.

Beaglehole EP. A study in social psychology. London: George Allen and Unwin; 1932.

Boss SR. Control, perceived risk and information security precautions: External and internal motivations for security behavior [Ph.D. thesis]. University of Pittsburgh; 2007.

Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quart 2015;39(4):837–64.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quart 2010;34(3):523–48.

Chenoweth T, Minch R, Gattiker T. Application of protection motivation theory to adoption of protective technologies. In: Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS'09): IEEE; 2009.

Chin E, Felt AP, Sekar V, Wagner D. Measuring user confidence in smartphone security and privacy. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. Washington, D.C.: ACM; 2012. p. 1–16.

Chin WW. Commentary: issues and opinion on structural equation modeling. MIS Quart 1998;22(1):vii–xvi.

Cichy P, Salge T-O, Kohli R. Extending the privacy calculus: The role of psychological ownership. In: Proceedings of the Thirty Fifth International Conference on Information Systems. Auckland, NZ; 2014.

Claar CL, Johnson J. Analyzing home PC security adoption behavior. J Comput Inform Syst 2012;52(4):20–9. doi:10.1080/08874417.2012.11645573.

Crossler RE. Protection motivation theory: Understanding determinants to backing up personal data. In: Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS): IEEE; 2010. p. 1–10.

Crossler RE, Bélanger F. An extended perspective on individual security behaviors: protection motivation theory and a Unified Security Practices (USP) instrument. Data Base Adv Inform Syst 2014;45(4):51–71.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur 2013;32:90–101.

Crossler RE, Long JH, Loraas TM, Trinkle BS. Understanding compliance with BYOD (bring your own device) policies utilizing protection motivation theory: bridging the intention-behavior gap. J Inform Syst 2014;28(1):209–26.

Dang-Pham D, Pittayachawan S. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach. Comput Secur 2015;48:281–97. http://dx.doi.org/10.1016/j.cose.2014.11.002.

Dulaney K, Baker VL, Marshall R, Cozza R, Zimmerman T, Willis DA. Predicts 2015: Mobile and Wireless: Gartner Inc; 2014.

Dupuis MJ, Crossler RE, Endicott-Popovsky B. Measuring the human factor in information security and privacy. In: Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS): IEEE; 2016. p. 3676–85.

Egelman S, Peer E. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems: ACM; 2015. p. 2873–82.

Facebook. Android App help; 2016. Available from: https://www.facebook.com/help/android-app/339147412905600. [Accessed 7 October 2016].

Furnell SM, Bryant P, Phippen AD. Assessing the security perceptions of personal Internet users. Comput Secur 2007;26:410–17.

Gefen D, Straub D. A practical guide to factorial validity using PLS-Graph: tutorial and annotated example. Commun Assoc Inform Syst 2005;16(1):91–109.

Geisser S. The predictive sample reuse method with applications. J Am Stat Assoc 1975;70(350):320–8.

Godlove T. Examination of the factors that influence teleworkers' willingness to comply with information security guidelines. Inform Secur J Global Perspect 2012;21(4):216–29.

Google Inc. Android Security Architecture; 2016. Available from: https://developer.android.com/guide/topics/security/permissions.html. [Accessed 7 October 2016].

Hair JF, Hult GTM, Ringle CM, Sarstedt M. A primer on partial least squares structural equation modeling (PLS-SEM). Thousand Oaks, CA: Sage; 2014.

Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inform Syst 2009;18(2):106–25. doi:10.1057/ejis.2009.6.

Herath T, Chen R, Wang J, Banjara K, Wilbur J, Rao HR. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Inform Syst J 2014;24(1):61–84.

Howe AE, Ray I, Roberts M, Urbanska M, Byrne Z. The psychology of security for the home computer user. In: Proceedings of the 2012 IEEE Symposium on Security and Privacy: IEEE; 2012. p. 209–23.

Huang JL, Curran PG, Keeney J, Poposki EM, DeShon RP. Detecting and deterring insufficient effort responding to surveys. J Bus Psychol 2012;27(1):99–114.

Hulland J. Use of partial least squares (PLS) in strategic management research: a review of four recent studies. Strat Manage J 1999;20(2):195–204.

Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83–95. http://dx.doi.org/10.1016/j.cose.2011.10.007.

Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inform Manage 2014;51(1):69–79. http://dx.doi.org/10.1016/j.im.2013.10.001.

Imgraben J, Engelbrecht A, Choo K-KR. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. Behav Inform Technol 2014;33(12):1347–60. doi:10.1080/0144929X.2014.934286.

Jenkins JL, Grimes M, Proudfoot JG, Lowry PB. Improving password cybersecurity through inexpensive and minimally invasive means: detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. Inform Technol Dev 2014;20(2):196–213.

Johnston A, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Quart 2010;34(3):549–66.

Johnston AC, Warkentin M, Siponen M. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Quart 2015;39(1):113–34.

Kaiser Family Foundation. Population Distribution by Age; 2014. Available from: http://kff.org/other/state-indicator/distribution-by-age/. [Accessed 14 July 2016].

Kaspersky Labs. IT Threat Evolution in Q1 2016; 2016. Available from: https://securelist.com/files/2016/05/Q1_2016_MW_report_FINAL_eng.pdf. [Accessed 7 October 2016].

Keil M, Tan BC, Wei K, Saarinen T, Tuunainen V, Wassenaar A. A cross-cultural study on escalation of commitment behavior in software projects. MIS Quart 2000;24(2):299–325.

Kelley T, Camp LJ, Lien S, Stebila D. Self-identified experts lost on the interwebs: the importance of treating all results as learning experiences. In: Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results: ACM; 2012. p. 47–54.

LaRose R, Rifon NJ, Enbody R. Promoting personal responsibility for Internet safety. Commun ACM 2008;51(3):71–6. doi:10.1145/1325555.1325569.

Lee D, Larose R, Rifon N. Keeping our network safe: a model of online protection behaviour. Behav Inform Technol 2008;27(5):445–54.

Li Y, Siponen M. A call for research on home users' information security behaviour. In: Proceedings of the 15th Pacific Asia Conference on Information Systems (PACIS 2011); 2011.

Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J Assoc Inform Syst 2010;11(7):394–413.

Maddux JE, Rogers RW. Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. J Exp Soc Psychol 1983;19(5):469–79.

McCracken G. Culture and consumption: a theoretical account of the structure and movement of the cultural meaning of consumer goods. J Consum Res 1986;13:71–84.

Mwagwabi F, McGill T, Dixon M. Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In: Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS): IEEE; 2014. p. 3188–97.

Mylonas A, Kastania A, Gritzalis D. Delegate the smartphone user? Security awareness in smartphone platforms. Comput Secur 2013;34:47–66.

Ng B-Y, Kankanhalli A, Xu YC. Studying users' computer security behavior: a health belief perspective. Decision Support Syst 2009;46(4):815–25.

Pierce JL, Kostova T, Dirks KT. The state of psychological ownership: integrating and extending a century of research. Rev Gen Psychol 2003;7(1):84–107. doi:10.1037/1089-2680.7.1.84.

Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology 2003;88(5):879–903.

Posey C, Roberts T, Lowry PB. The impact of organizational commitment on insiders' motivation to protect organizational information assets. J Manage Inform Syst 2015;32(4):179–214.

Rettie R. Connectedness, awareness and social presence. Paper presented at the 6th International Presence Workshop, Aalborg, Denmark; 2003.

Ringle CM, Wende S, Will S. SmartPLS 2.0 (M3) Beta. Hamburg; 2005. Available from: http://www.smartpls.de. [Accessed 2 April 2016].

Rivis A, Sheeran P. Descriptive norms as an additional predictor in the theory of planned behaviour: a meta-analysis. Curr Psychol 2003;22(3):218–33.

Rogers RW. A protection motivation theory of fear appeals and attitude change. J Psychol 1975;91(1):93–114.

Rogers RW. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo JT, Petty RE, editors. Social psychophysiology. New York: Guilford Press; 1983. p. 153–76.

Sheeran P. Intention – behavior relations: a conceptual and empirical review. Eur Rev Social Psychol 2002;12(1):1–36. doi:10.1080/14792772143000003.

Sheeran P, Orbell S. Augmenting the theory of planned behavior: roles for anticipated regret and descriptive norms. J Appl Soc Psychol 1999;29(10):2107–42.

Shropshire J, Warkentin M, Sharma S. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comput Secur 2015;49:177–91. http://dx.doi.org/10.1016/j.cose.2015.01.002.

Siponen M, Mahmood A, Pahnila S. Employees' adherence to information security policies: an exploratory field study. Inform Manage 2014;51(2):217–24. http://dx.doi.org/10.1016/j.im.2013.08.006.

Sommestad T, Hallberg J. A review of the theory of planned behaviour in the context of information security policy compliance. Security and Privacy Protection in Information Processing Systems (pp. 257–271): Springer; 2013.

Sommestad T, Karlzén H, Hallberg J. A meta-analysis of studies on protection motivation theory and information security behaviour. Int J Inform Secur Priv 2015;9(1):26–46.

Stone M. Cross-validatory choice and assessment of statistical predictions. Journal of the Royal Statistical Society. Series B 1974;36(2):111–47.

Symantec Security Response. IoT devices being increasingly used for DDoS attacks; 2016.

Taylor S, Todd PA. Understanding information technology usage: a test of competing models. Inform Syst Res 1995;6(2):144–76.

Tsai HS, Jiang M, Alhabash S, LaRose R, Rifon NJ, Cotten SR. Understanding online safety behaviors: a protection motivation theory perspective. Comput Secur 2016;59:138–50.

Tu Z, Turel O, Yuan Y, Archer N. Learning to cope with information security risks regarding mobile device loss or theft: an empirical examination. Inform Manage 2015;52(4):506–17. http://dx.doi.org/10.1016/j.im.2015.03.002.

Van Dyne L, Pierce JL. Psychological ownership and feelings of possession: three field studies predicting employee attitudes and organizational citizenship behavior. J Org Behav 2004;25(4):439–59.

Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Inform Manage 2012;49(3):190–8.

Weinstein ND, Lyon JE, Rothman AJ, Cuite CL. Changes in perceived vulnerability following natural disaster. J Soc Clin Psychol 2000;19(3):372–95.

West R. The psychology of security. Commun ACM 2008;51(4):34–40.

Winkler I. Winkler: The Real Problems With Cloud Computing. csoonline.com; 2009. Available from: http://www.csoonline.com/article/2124281/cloud-security/winkler--the-real-problems-with-cloud-computing.html. [Accessed 7 October 2016].

Wood P, Nahorney B, Chandrasekar K, Wallace S, Haley K. Symantec Internet security threat report; 2015. Available from: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf. [Accessed 7 October 2016].

Wood W, Quinn JM, Kashy DA. Habits in everyday life: thought, emotion, and action. J Pers Soc Psychol 2002;83(6):1281–97.

Woon I, Tan G, Low R. A protection motivation theory approach to home wireless security. In: Proceedings of the Twenty-Sixth International Conference on Information Systems. Las Vegas; 2005. p. 367–80.

Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput Human Behav 2008;24(6):2799–816.

Zhang L, McDowell WC. Am I really at risk? Determinants of online users' intentions to use strong passwords. J Internet Commerce 2009;8(3):180–97.

Nik Thompson is a Senior Lecturer in the School of Information Systems at Curtin University, Australia. He holds MSc and PhD degrees and works in the area of Computer Security and Information Systems. His research interests include affective computing, human-computer interaction and information security.

Tanya Jane McGill is an Associate Professor in Information Technology at Murdoch University in Western Australia. She has a PhD from Murdoch University. Her major research interests include information system security, technology adoption, e-learning and ICT education. Her work has appeared in various journals including *Computers & Education, Decision Support Systems*, *Behaviour and Information Technology*, *Journal of Computer Assisted Learning*, and *Journal of Organizational and End User Computing*.

Xuequn (Alex) Wang is a Lecturer at Murdoch University. He received his PhD in Information Systems from Washington State University. His research interests include knowledge management, online communities, and idea generation. His research has appeared (or is forthcoming) in Communications of the Association for Information Systems, Journal of Organizational Computing and Electronic Commerce, Behaviour & Information Technology, Journal of Computer Information Systems, and Journal of Knowledge Management.