BEHAVIOUR & INFORMATION TECHNOLOGY, 2017
https://doi.org/10.1080/0144929X.2017.1352028

Taylor & Francis
Taylor & Francis Group

Old risks, new challenges: exploring differences in security between home computer and mobile device use

Tanya McGill[a] and Nik Thompson[b]

[a]School of Engineering and Information Technology, Murdoch University, Perth, Australia; [b]School of Information Systems, Curtin University, Perth, Australia

ABSTRACT

Home users are particularly vulnerable to information security threats as they must make decisions about how to protect themselves, often with little knowledge of the technology. Furthermore, information for home users tends to focus on the traditional PC and may downplay threats faced on mobile devices, transforming well-known and old risks into new challenges for information security. To address the need for more behavioural information security research that focusses on mobile devices, this paper reports on the first large-scale study comparing security perceptions and behaviours on home computer and mobile devices. Data from 629 users revealed that in addition to differences in information security behaviour, the following security-related perceptions all differ significantly between home computer and mobile device use: perceived severity, security self-efficacy, response efficacy, response cost, descriptive norm, psychological ownership and intention to perform security behaviours. In each case, the direction of the difference was such that mobile devices were more likely to be at risk than a home computer. The practical implications of these differences are discussed.

ARTICLE HISTORY
Received 21 January 2016
Accepted 3 July 2017

KEYWORDS
Information security behaviours; mobile device security; home computer security; human factors; smartphone; mobile

1. Introduction

Personal computing users face numerous security threats (Jeske and van Schaik 2017; White 2015) and need to regularly make decisions regarding security measures to protect themselves. Not only do home users not normally have easy access to security training and information technology (IT) support to help with these decisions, but they have relatively low levels of information security awareness (Öğütçü, Testik, and Chouseinoglou 2016) and erroneous perceptions that their information is not important enough to be targeted (Alsaleh, Alomar, and Alarifi 2017; Sasse, Brostoff, and Weirich 2001) and that they are less vulnerable to risks than others are (West 2008). Issues associated with personal IT use are important not just for the users themselves but also for organisations, given the potential for harm to corporate as well as personal information. This is particularly relevant as many people now bring work home and may hold organisational data on their home computers and mobile devices, placing these data at risk of a security breach with substantial impact (Das and Khan 2016; Jones and Chin 2015; Munch and Canales 2014; Mylonas, Kastania, and Gritzalis 2013).

Whilst personal computing was previously associated with desktop and laptop computers, ownership and use of tablets and smartphones is increasing along with their use to access and store important personal data, and for tasks such as shopping and banking (Dulaney et al. 2014; Jones and Chin 2015). Although research suggests that people have been less willing to make purchases or do banking 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, and 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, 2). With this shift comes the need for more research on the behavioural security implications of mobile device use. This need is urgent as research suggests that the security awareness of mobile users is limited (Das and Khan 2016; Mylonas et al. 2013; Mylonas, Kastania, and Gritzalis 2013; Vecchiato and Martins 2015) and that many either do not read security messages or ignore them (Harris, Chin, and Brookshire 2015; Kelley et al. 2012). The threats are, however, real. For example, the 2017 Symantec (2017) Internet security threat report noted that there were 18.4 million mobile malware detections in 2016, up by 105% from 2015, highlighting the risk to mobile device users. There is also evidence that the security software that mobile device users use (such as anti-malware

CONTACT Tanya McGill t.mcgill@murdoch.edu.au

apps) may not be sufficiently effective (Faruki et al. 2014; Rastogi, Chen, and Jiang 2014). Finally, vendors may recommend different security controls for mobile platforms, for instance, Google executives stating that antivirus is not needed on their mobile OS, Android (Ludwig 2014). Such statements are potentially damaging, and may create new challenges by undermining what knowledge home users may have about well-known, old risks.

The research described in this paper aims to address the need for more behavioural security research that focusses on mobile devices (Crossler and Bélanger 2014) and presents the findings of a large-scale study comparing the security perceptions and behaviours associated with home computer use with those of mobile device use. Analysis of data from a sample of 629 adult users based in the United States sheds light on key factors that have been shown to influence security behaviours in order to answer the overall research question: '*What are the differences in security-related perceptions between home computer and mobile contexts?*'

2. Literature review

With the realisation that technological solutions alone are not sufficient to protect information and software (Sasse, Brostoff, and Weirich 2001), research has sought to understand user information security behaviour in order to foster improvements in it. Much of this research has focused on understanding users' intentions to perform security behaviours, and specific factors have been shown to influence these intentions and/or actual security behaviours, across a range of domains, but primarily in organisational settings.

The factors that are proposed to be important in determining information security behaviour largely derive from theoretical frameworks from health behaviour research (e.g. Protection Motivation Theory (PMT); Rogers 1975, 1983) that have been adapted and extended in various ways to reflect the security domain (e.g. Anderson and Agarwal 2010; Crossler and Bélanger 2014; Ifinedo 2012; Vance, Siponen, and Pahnila 2012). The review of the literature below introduces the key factors believed to be associated with home user IT security behaviour that are investigated in this study. It then discusses relevant research on their potential impact on security intentions and behaviour. It includes research from both organisational and home user domains, and highlights where mobile devices have been considered in the research. It also discusses why differences in security perceptions between home computers and mobile devices may be important.

2.1. Influences on IT security behaviour: organisational versus home computing domains

The factors that have been most commonly researched and shown to influence organisational security behavioural intentions or behaviour derive from the PMT (Rogers 1975, 1983) and include: *perceived vulnerability* to the threat (Ifinedo 2012; Siponen, Mahmood, and Pahnila 2014; Workman, Bommer, and Straub 2008), *perceived severity* of the threat (Siponen, Mahmood, and Pahnila 2014; Vance, Siponen, and Pahnila 2012), security *self-efficacy* (Bulgurcu, Cavusoglu, and Benbasat 2010; Herath and Rao 2009; Siponen, Mahmood, and Pahnila 2014; Vance, Siponen, and Pahnila 2012), perceived effectiveness of the response (*response efficacy*) (Siponen, Mahmood, and Pahnila 2014; Vance, Siponen, and Pahnila 2012) and the cost associated with taking protective action (*response cost*) (Vance, Siponen, and Pahnila 2012).

Many of the same factors also appear to be important in the home user domain (Anderson and Agarwal 2010; Liang and Xue 2010; Mwagwabi, McGill, and Dixon 2014; Woon, Tan, and Low 2005; Zhang and McDowell 2009); however, some differences in influences from those in the organisational security domain have been postulated, and are believed to be associated with more emotional responses to the threats (Liang and Xue 2010; Mwagwabi, McGill, and Dixon 2014; Zhang and McDowell 2009). Additional factors have also been identified as particularly relevant to the home user domain and these include *psychological ownership* (Anderson and Agarwal 2010), *subjective norm* (Anderson and Agarwal 2010; Ng and Rahim 2005) and *descriptive norm* (Anderson and Agarwal 2010; Tu et al. 2015). The above factors are all relevant to personal information security, but little is known about their relative importance for mobile device security. Tu et al. (2015) and Dang-Pham and Pittayachawan (2015) have conducted studies on the role of factors identified in PMT (Rogers 1975, 1983) on aspects of mobile device security, but do not include comparisons with home computer security. It is therefore important to determine their relevance in understanding differences in security perceptions and behaviours between home computer use and mobile device use. Each of these factors was therefore selected as potentially differing between home computer and mobile contexts, and investigated in this study. The remainder of this section discusses each of these factors. This discussion is organised by factor, and includes the source and the justification for the importance of each.

2.2. Threat appraisal factors

Perceived vulnerability to threat refers to users' subjectively estimated probability that a security threat exists,

and it is considered to be a key determinant of security motivation in PMT (Rogers 1975, 1983). Whilst level of perceived vulnerability to threats has been shown to positively influence security behaviour in organisational settings (Ifinedo 2012; Siponen, Mahmood, and Pahnila 2014; Workman, Bommer, and Straub 2008), there have been mixed findings about its role in personal information security behaviour. For example, although Liang and Xue (2010) found a positive influence on security behaviour to avoid spyware threats, Crossler (2010) found that perceived vulnerability unexpectedly had a negative influence on backup behaviour, and perceived vulnerability did not influence either home wireless security (Woon, Tan, and Low 2005) or password behaviour (Zhang and McDowell 2009) in other studies. Therefore, further research is required into the role of perceived vulnerability in different personal computing contexts such as mobile device use.

Perceived severity is also proposed as a key determination of security motivation in PMT (Rogers 1975, 1983), forming part of threat appraisal. In the personal computing context, perceived severity refers to the degree to which users believe that harm (e.g. financial or psychological) would occur if they were the victim of a security event. These severity perceptions have been shown to influence security intentions and behaviour either directly (Crossler and Bélanger 2014; Woon, Tan, and Low 2005) or indirectly via fear (also referred to as perceived threat) (Boss et al. 2015; Liang and Xue 2010; Mwagwabi, McGill, and Dixon 2014). For example, Crossler and Bélanger (2014) identified its effect using a unified measure of security behaviour of home users, and called for greater understanding of security in a mobile environment. The perceived severity of information security threats is therefore important to consider in the context of the increased use of smartphones and tablets.

2.3. Coping appraisal factors

Coping appraisal is a major component of PMT (Rogers 1975, 1983) and is also believed to play an important role in users' security behaviour. Coping appraisal involves both assessment of one's own ability to take protective action (self-efficacy; also referred to as perceived behavioural control in the Theory of Planned Behaviour (TPB); Ajzen 1991) and assessment of the effectiveness of available protective measures (response efficacy). In addition, assessment of response cost, which relates to perceptions of the costs (monetary or otherwise) associated with taking protective action, is also believed to play a role in coping appraisal. Both security self-efficacy and perceptions of response efficacy have been shown, in the personal computing context, to positively influence intention to protect against device theft (Tu et al. 2015), intention to use anti-spyware software (Liang and Xue 2010), intention to use strong passwords (Mwagwabi, McGill, and Dixon 2014), enabling of firewalls (Woon, Tan, and Low 2005) and performance of frequent backups (Crossler 2010). Perceptions of response cost have also been shown to play an important role in the personal computing context, such that increases in perceived response cost negatively influence users' intentions to perform security behaviours (Liang and Xue 2010; Mwagwabi, McGill, and Dixon 2014; Woon, Tan, and Low 2005). As mobile technology is relatively new to many personal computing users and is changing rapidly, differences in users' perceptions of their own ability to protect their devices, the cost of doing so and concerns about the effectiveness of the available modes of protection may be important.

2.4. Subjective and descriptive norms

Subjective norm refers to a user's beliefs as to whether others want them to perform behaviour, and is a key determinant of behavioural intention in the TPB (Ajzen 1991). Descriptive norm refers to what a user believes most other people do, in this case to protect their devices, and has been shown to be an additional predictor of behavioural intention beyond the TPB variables (Rivis and Sheeran 2003). There has been little research on the role of subjective norm or descriptive norm in information security behaviour, but Anderson and Agarwal (2010) included both in their study of home computer user security behaviour and found that subjective norm influenced intention to perform security-related behaviours on home computers, and that descriptive norm influenced intention to perform security behaviours relating to the Internet. Tu et al. (2015) explored the role of social influences in protection against mobile 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. In a qualitative study of smartphone users, Alsaleh, Alomar, and Alarifi (2017) also noted that social triggers influence security behaviours.

When devices are owned by individuals rather than their employer, adoption of security measures may require more self-reliance than in an organisational situation where technical support is supplied. Home users do not typically receive any formal security training and their learning tends to be based on information sources such as friends and family, previous personal experience, and the media and Internet (Furnell, Bryant, and Phippen 2007). This potentially makes subjective norm and descriptive norm important in the personal computing

context, and any differences in users' levels of them with respect to their home computers and their mobile devices may have impacts on their security behaviour.

2.5. Psychological ownership

Psychological ownership refers to the relationship between an individual and an object, in which the object is experienced as connected with the self (Pierce, Kostova, and Dirks 2003); therefore in the personal computing context this involves feelings of ownership for devices and their software and information. Devices are generally bought by the user, and often become central in their lives as sources of entertainment, communication and control over household expenditure, etc. Therefore, it is relevant to investigate how this centrality might play a role in information security behaviour. Anderson and Agarwal (2010) explored the role of psychological ownership of home computers and found that the extent of feelings of psychological ownership weakly influenced intention to perform security behaviours; however more research is needed to understand the role of psychological ownership in security behaviour, including how it differs between devices, as no previous work has addressed this.

3. Research questions and hypotheses

The research described in this paper is designed to compare security perceptions and behaviours relating to home computer use with those associated with mobile device use in order to identify differences that may have implications for securing home users' devices, software and data. Home computers are considered in this study to include both desktop and laptop machines. Whilst laptops provide greater flexibility in locations used, they offer essentially the same functionality as desktops and offer the same operating environments, and thus the needed security behaviour is largely the same. Smartphones and tablets differ from home computers in that they provide a touchscreen interface and utilise apps from an app-store rather than regular 'boxed' software. Thus some of the actions needed to protect these devices differ from those needed to protect home computers. There are also devices that overlap these two categories (e.g. Microsoft Surface Pro), but these are not included in the study. The research question addressed in this study was:

> What are the differences in security-related perceptions between home computer and mobile contexts?

Different perspectives have been taken with respect to relative levels of perceived vulnerability when using mobile devices. Several studies have reported that mobile device users do not understand the risks associated with personal computing on mobile devices (Imgraben, Engelbrecht, and Choo 2014; Wood et al. 2015), suggesting that perceived vulnerability would be lower for mobile devices than for home computers. This is supported by the results of a study on smartphone security by Alsaleh, Alomar, and Alarifi (2017), who found that many users felt that the risks associated with lack of protective behaviour were not severe, and that the likelihood of being exposed to privacy or security threats by sharing passwords was low.

However, Chin et al. (2012) hypothesised that people would be more worried about security on their smartphone than on their home computer, arguing that this is related to the reluctance to use smartphones for sensitive transactions that their study and other studies have identified (e.g. Shaikh and Karjaluoto 2015). Chin et al. (2012), however, found no difference in levels of perceived vulnerability when using smartphones compared to when using laptops. They explored this result further via interviews and reported that while having less experience and knowledge about using smartphones for computing purposes made users feel more vulnerable, this was balanced by less awareness of smartphones being hacked, and not generally performing sensitive tasks on their smartphones. Given this balance of differing contributors to perceived vulnerability, we proposed that:

> H1: Perceived vulnerability to information security threats will not differ between mobile devices and home computers.

Home computers have been considered by the majority of personal users as the primary repository of their important information (Chin et al. 2012). This may be a matter of habit, or influenced by risk assessments (Chin et al. 2012), such that users believe it is safer to keep the storage of important information on home computers rather than mobile devices. In a study by Egelman et al. (2014) the second most common reason 500 smartphone users gave for not locking their devices was that 'no one would care what was on their phone'; this suggests that many users consider the severity of information security threats to the device to be relatively low, possibly because of usage patterns. It is therefore hypothesised that the severity of a potential security threat is likely to be perceived as lower for mobile devices than for home computers.

> H2: Perceived severity of information security threats will be lower for mobile devices than for home computers.

A study by Botha, Furnell, and Clarke (2009) found that that security for mobile devices suffers from usability

issues and limitations that make it difficult for users to achieve the same level of protection that they have for their home computers, and users report that the inconvenience of mobile device security is a reason for not adequately protecting their device (Karatzouni et al. 2007). It seems likely that this is still the case, with users having less awareness of how to protect their mobile devices, both because they have less experience with them and because the devices are evolving more rapidly than their home computers (Kelley et al. 2012; Mylonas, Kastania, and Gritzalis 2013). We therefore hypothesised that users will perceive the response cost involved in protecting their mobile devices as higher than that of protecting their home computers:

> H3: Response cost will be perceived as higher for mobile devices than for home computers.

Applications and data on mobile devices have been considered by researchers to be less well protected than on most home computers (Ben-Asher et al. 2011; Leavitt 2005), and personal users' perceptions of response efficacy are likely to echo this, with them holding stronger beliefs in the effectiveness of security measures for home computers than for mobile devices. For example, when users attempt to undertake security behaviours for a mobile device they discover that the reduced interface is associated with a greatly reduced set of security options and that features that a home computer user would expect are not available (Botha, Furnell, and Clarke 2009). Whilst not all of these features may be relevant in this environment, user perceptions are likely to be influenced, as indicated by a study where about 70% of mobile device users were found to be interested in increased security for their mobile device (Kowalski and Goldstein 2006). It is therefore hypothesised that:

> H4: Response efficacy will be perceived as lower for mobile devices than for home computers.

Users have long exhibited low levels of confidence in their ability to protect themselves in the personal computing domain (Furnell, Bryant, and Phippen 2007). However, because of users' generally longer experience with home computers and the greater stability and usability of approaches to home computer protection (Botha, Furnell, and Clarke 2009) as well as previous research highlighting the difficulty users have understanding smartphone permissions displays associated with mobile apps (Kelley et al. 2012) we hypothesised that:

> H5: Security self-efficacy will be lower for mobile devices than for home computers.

There has been less research on the roles of subjective norm or descriptive norm in information security behaviour than on PMT (Rogers 1975, 1983) factors. However, some authors suggest that these factors are particularly important in the context of personal computing (Anderson and Agarwal 2010; Tu et al. 2015), because the formal approaches to improving security behaviour that organisations implement are not found in the personal use sphere. Tu et al. (2015) argue that with respect to personally owned computing devices, peers and family are more likely to try to convince people to take protective action (subjective norm) for mobile devices, or indirectly signal to them that such measures are needed by taking this action themselves and sharing the information (descriptive norm). They argue that these social factors are particularly important for smartphones and tablets because of their highly visible nature and their use for social interactions, and that device risks and possible solutions will therefore emerge in social situations. We, however, argue that because of lack of awareness of the threats associated with these mobile devices and lack of awareness of users' vulnerability to these threats (Das and Khan 2016; Imgraben, Engelbrecht, and Choo 2014; Vecchiato and Martins 2015), levels of both subjective norm and descriptive norm will be lower for smartphones and tablets than for home computers, and it is therefore hypothesised that:

> H6: Users will experience lower levels of subjective norm with regards to mobile device security than home computer security.

> H7: Users will experience lower levels of descriptive norm with regards to mobile device security than home computer security.

In this study, psychological ownership refers to the extent to which a user feels ownership of hardware and the software and information it contains, such that it becomes an 'extension of the self' (McCracken 1986). Anderson and Agarwal (2010) proposed that psychological ownership of the Internet and of one's own computer are positively related to behavioural intentions to protect them. They found that home computer users had very high levels of psychological ownership for their computers and that this weakly influenced their intention to protect them.

There have been many reports of people's attachment to their smartphones, to the extent that many young people sleep next to them (Keller 2011), and Walsh et al. (2011) note both cognitive and behavioural aspects to this attachment and compare it to addiction. Gikas and Grant (2013, 24) argue that 'the mobile device has possibly merged with the identity of the student'. These apparent strong feelings of attachment to mobile devices suggest that levels of psychological ownership will be higher for mobile devices than for home computers. Therefore, it is hypothesised that:

H8: Users will display higher levels of psychological ownership with regards to their mobile devices than their home computers.

The problems with the security behaviour of home computer users have been widely reported (Howe et al. 2012) but less is known about the security behaviour of users of smartphones and tablets (Mylonas, Kastania, and Gritzalis 2013). Studies by Imgraben, Engelbrecht, and Choo (2014), Mylonas, Kastania, and Gritzalis (2013), Tu et al. (2015) and Vecchiato and Martins (2015), however, suggest that mobile device users may be even less likely and able to perform the behaviours needed to protect their devices and information. For example, almost half of those surveyed by Imgraben, Engelbrecht, and Choo (2014) did not use passwords to lock their devices and even fewer locked their SIM card. Less than 20% used encryption software. Mylonas, Kastania, and Gritzalis (2013) also found poor use of both vendor supplied (e.g. physical) security controls and third-party security controls (e.g. antivirus software) in mobile devices. Therefore it is hypothesised that:

H9: Users are less likely to intend to perform security behaviours on their mobile devices than their home computers.

H10: Users are less likely to perform security behaviours on their mobile devices than their home computers.

The factors and the direction of each of the hypotheses related to them are summarised in Figure 1.

4. Method

This study was designed to directly compare security perceptions and behaviours of users with respect to their home computers and their mobile devices. The target population for the study was users who use home computers and smartphones/tablets for personal use, and data were collected using an anonymous online questionnaire.

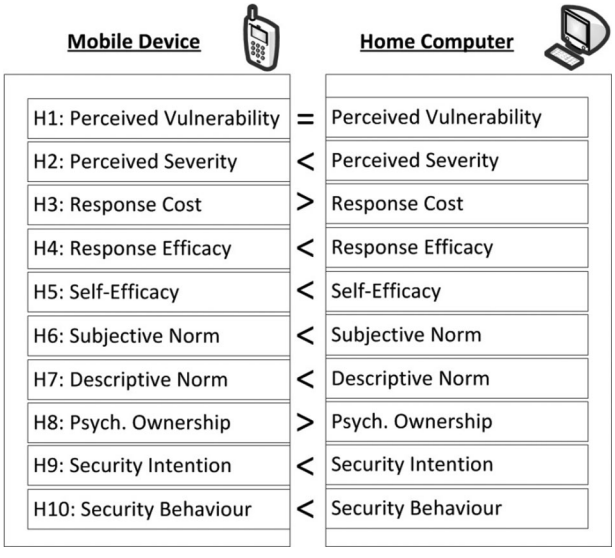

Figure 1. Summary of hypotheses.

4.1. Participants and procedures

We sought participants from a wide spectrum of backgrounds including gender, level of education, computer skills and computer security knowledge, and to do this used a third party recruiting company that, using census balanced random sampling, identified potential participants located in the United States. Participants were contacted via email and invited to voluntarily participate in the study by completing a questionnaire, which was hosted on SurveyMonkey. All participants were 18 or over and had both a home computer/laptop and a smartphone/tablet. All participants responded to background questions about both devices before being randomly allocated to answer questions about either their home computer/laptop use or their smartphone/tablet use.

4.2. Measurement

To ensure the validity of measurement, wherever possible the items used to measure the constructs were adapted for the home user domain from instruments used in previous behavioural security research, with new items developed as needed. The items to measure each construct were first pre-tested by two academics from the security area to establish content validity, and the full questionnaire was then pilot tested with several members of the target population and minor changes were made to the wording and to streamline the interface.

The first section of the questionnaire asked background demographic questions as well as about participants' previous information security training and their usage patterns on both their home computers and their mobile devices. The second section of the questionnaire asked about security perceptions and behaviours. The constructs measured were: perceived vulnerability, perceived severity, security self-efficacy, response efficacy, response cost, subjective norm, descriptive norm, psychological ownership, intention to perform security behaviours and security behaviour. Each participant only answered one set of questions as they were randomly assigned to answer questions regarding either their home computer/laptop or smartphone/tablet. The questions were kept consistent and varied only in the device referred to: either 'smartphone/tablet' or 'home computer/laptop'.

The items to measure each of the constructs of interest, apart from security behaviour, were measured on a

7-point Likert scale from 1 'Strongly Disagree' to 7 'Strongly Agree' (the appendix details the items used and their sources). Once data collection and preparation were completed, reliability testing was conducted to ensure that the items used to measure these constructs demonstrated sufficient internal consistency. All Cronbach's alphas were above 0.9, and the scales were thus found to be reliable (Nunnally 1978): perceived vulnerability $\alpha = 0.93$; perceived severity $\alpha = 0.94$; response cost $\alpha = 0.95$; response efficacy $\alpha = 0.94$; security self-efficacy $\alpha = 0.91$; subjective norm $\alpha = 0.95$; descriptive norm $\alpha = 0.95$; psychological ownership $\alpha = 0.93$; intention to perform security behaviours $\alpha = 0.96$. A summary measure of each of these constructs was then calculated for each respondent as the average of the responses to the items for that construct.

Security behaviour was measured using four items, each of which asked the participant about whether they performed a common specific security behaviour and was answered as 'Yes', 'No' or 'Unsure'. These items were chosen as representative of recommended personal use security behaviours and were analysed as separate variables rather than being combined to form a single measure of security behaviour.

4.3. Data preparation and analysis

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

As the data did not meet the assumption of normality, use of independent sample t-tests was not appropriate to test hypotheses H1–H9. Therefore, the alternative non-parametric Mann-Whitney *U* test was used. The Mann-Whitney *U* test tests the hypothesis that two independent samples are likely to derive from the same population, and does not require the assumption of normal distributions. For hypothesis H10, chi-square tests of independence were used to test for differences between home computers/laptops and smartphone/tablets for each of the types of security behaviour. An alpha level of 0.05 was used for all statistical tests.

Table 1. Background information about participants.

	Home computer/laptop respondents (%)	Smartphone/tablet respondents (%)
Gender		
Male	39.9	35.0
Female	60.1	65.0
Age		
18–24	2.5	3.0
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	24.3	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	18.6
Previous information security training		
Yes	20.2	17.6
No	79.8	82.4

5. Results

A total of 629 valid responses (62.5% female and 37.5% male) was obtained: 322 home computer/laptop respondents and 307 smartphone/tablet respondents. Table 1 provides background information about the two groups of participants in the study. The age spread in the groups differed from that of the US population at the time the data were 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 was, however, no significant difference between the two groups in terms of age ($\chi^2(6, N = 623) = 2.011$; $p = .919$) or gender ($\chi^2(1, N = 624) = 1.643$; $p = .200$).

Despite the majority of participants rating their skill with computers as good or excellent (64.7%), only 18.9% had previously received any information security training. Chi-square tests of independence revealed no significant differences between those who responded with respect to their home computer/laptop and those who responded with respect to their smartphone/tablet in either self-assessed computer skill ($\chi^2(4, N = 629) = 1.417$; $p = .841$) or whether they had received information security training ($\chi^2(1, N = 629) = 0.691$; $p = .406$).

The amount of time participants spent using the computing functionality of the different types of devices was also compared (see Table 2), with the computing functionality of smartphone/tablets defined to include all functionality except making phone calls. Participants were found to spend significantly longer each day

Table 2. Comparison of time spent per day using home computer/laptop versus smartphone/tablet.

Daily use	Home computer/laptop (%)	Smartphone/tablet (%)
1 hour or less	8.4	41.2
From 1 to 2 hours	18.0	25.3
From 2 to 3 hours	23.8	12.6
From 3 to 4 hours	17.5	8.9
From 4 to 5 hours	13.0	5.6
More than 5 hours	3.1	6.5

using their home computer than they did using the computing functionality of their smartphone/tablet ($\chi^2(25, N = 629) = 130.4$; $p < .001$). The most common amount of time spent using a home computer was two to three hours per day (23.8%, with 17.5% spending between three and four hours) and the most common amount of time spent using the computing functionality of smartphones and tablets was less than one hour per day (41.2%).

Users also differed in what they used their devices for (see Table 3). The most notable differences related to shopping and banking. Whilst 67.2% of participants used their home computer for online shopping only 24.0% purchased online using their smartphone/tablet. A similar pattern occurred for online banking with 61.2% of participants using their home computer for online banking, but only 21.9% of them doing it on their smartphone/tablet. The direction of these differences is consistent with those reported by Chin et al. (2012). The levels of use of mobile devices for banking, gaming and social media are lower than those reported by Imgraben, Engelbrecht, and Choo (2014), and this seems likely to be because their study involved a large proportion of university students and a younger age distribution.

Participants were also asked if they had installed any security software on their devices, and a large significant difference was found between device types ($\chi^2(4) = 124.68$, $p < .001$). Whilst 79.7% reported that they had installed security software on their home computer/laptop, only 25.3% had done so on their smartphone/tablet. This level of installation for home computers is relatively consistent with that reported in previous studies (Alsaleh, Alomar, and Alarifi 2017; Furnell, Bryant, and Phippen 2007; Milne, Labrecque, and Cromer 2009).

Table 4 provides descriptive information about each of the main constructs of interest relating to perceptions for both home computers/laptops and for smartphones/tablets. Each of the hypotheses was addressed by comparing perceptions regarding home computer security with those about smartphone/tablet security. As discussed above, the data did not meet the assumption of normality; therefore non-parametric Mann-Whitney U tests were conducted to evaluate hypotheses H1–H9.

Table 3. Comparison of types of use.

Device use	Home computer/ laptop (%)	Smartphone/tablet (%)
Shopping	67.2	24.0
Banking	61.2	21.9
Surfing the Internet	83.0	54.7
Email	92.4	69.3
Gaming	27.5	30.8
Messaging/video chat	15.9	26.4
Social media	49.8	41.8
Downloading or streaming video	22.4	14.5

Table 4. Descriptive statistics for key constructs and related hypothesis test results.

	Home computer/ laptop[a]		Smartphone/ tablet[b]			
	Mean	SD	Mean	SD	p	Accept?
(H1) Perceived vulnerability	4.74	1.29	4.67	1.39	.585	✗
(H2) Perceived severity	6.12	1.09	5.76	1.33	<.001	✓
(H3) Response cost	3.16	1.53	3.49	1.40	.003	✓
(H4) Response efficacy	5.19	1.19	4.90	1.27	.001	✓
(H5) Security self-efficacy	5.45	1.12	4.91	1.28	<.001	✓
(H6) Subjective norm	3.97	1.60	3.77	1.57	.167	✗
(H7) Descriptive norm	5.29	1.20	4.43	1.39	<.001	✓
(H8) Psychological ownership	5.36	1.12	4.64	1.39	<.001	✗
(H9) Intention to perform security behaviours	5.91	1.11	4.96	1.40	<.001	✓

[a] $n = 302$.
[b] $n = 307$.

As can be seen from Table 4, there was no significant difference in levels of perceived vulnerability to security threats for smartphone/tablets compared to home computers/laptops (Mdn 4.67 vs. 4.67; $U = 48{,}183$, $Z = -0.547$, $p = .585$). H1 was, therefore, not rejected: users experience similar levels of perceived vulnerability to security threats with respect to their mobile devices and their home computers. It was proposed that users would, however, have lower levels of perceived severity related to security threats to their smartphone/tablet than they would to those relating to their home computer. Mean levels of perceived severity were relatively high for both smartphones/tablets and home computers (5.76 vs. 6.12), but those for smartphones/tablets were significantly lower (Mdn 6.12 vs. 6; $U = 41{,}630$, $Z = -3.49$, $p < .001$). H2 was therefore supported.

Given the rapid evolution of mobile technology and the effort required to stay up to date with these developments, it was proposed that users would see the response cost associated with protecting their mobile devices as higher than that for protecting their home computers, and that the response efficacy would be lower. Consistent with this, response cost was significantly higher for smartphones/tablets than for home computers/laptops (Mean 3.49 vs. 3.16, Mdn 3.71 vs. 3.29; $U = 42{,}750$, $Z = -2.94$, $p = .003$) and levels of response efficacy were significantly lower for smartphones/tablets than for home computers/laptops (Mean 4.90 vs. 5.19, Mdn 5.00 vs. 5.00; $U = 41{,}975$, $Z = -3.29$, $p = .001$). Both H3 and H4 were therefore supported.

Consistent with these hypotheses, it was also proposed that users' security self-efficacy would be lower for mobile devices and higher for home computers, and this was found to be the case. Mean levels of security

self-efficacy were 4.91 for smartphones/tablet protection and 5.45 for home computer protection and this difference was significant (Mdn 5.50 vs. 5.50; $U = 36{,}912$, $Z = -5.50$, $p < .001$). H5 was therefore accepted.

It was hypothesised that users would experience lower levels of both subjective norm and descriptive norm with regards to mobile device security because of greater public awareness of the threats associated with home computer use (Imgraben, Engelbrecht, and Choo 2014). Contrary to expectations, there was no significant difference in levels of subjective norm for mobile device security and home computer security (Mean 3.99 vs. 3.97, Mdn 4.00 vs. 4.00; $U = 46{,}341$, $Z = -1.38$, $p = .585$), and H6 was therefore not supported. Levels of descriptive norm were, however, significantly lower for mobile device security (5.29 vs. 4.43); that is, users were less likely to believe that others protect their mobile devices than they were to believe that others protect their home computers (Mdn 4.25 vs. 5.25; $U = 30{,}816$, $Z = -8.21$, $p < .001$) and H7 was therefore supported.

H8 related to levels of psychological ownership for the two different types of devices, and it was hypothesised that users would display higher levels of psychological ownership with regards to their mobile devices. This hypothesis was not supported as the levels of psychological ownership were significantly lower for smartphones/tablets than for home computers/laptops (Mean 4.64 vs. 5.36, Mdn 4.57 vs. 5.57; $U = 34{,}347$, $Z = -6.63$, $p < .001$). Post-hoc analysis was undertaken to try to determine whether there was an age effect in this difference, and whilst those under 45 years of age did have significantly higher levels of psychological ownership of their mobile device than those 45 and over ($N = 305$, Mean 5.01 vs. 4.51, Mdn 5.00 vs. 4.43; $U = 7179$, $Z = -2.69$, $p = .007$), levels of psychological ownership of smartphones/tablets were still significantly lower than those for home computers/laptops in the under 45 age group ($N = 153$, Mean 5.01 vs. 5.46, Mdn 5.00 vs. 5.57; $U = 2313$, $Z = -2.22$, $p = .026$).

Given research highlighting low levels of engagement with security for mobile devices (Imgraben, Engelbrecht, and Choo 2014; Mylonas, Kastania, and Gritzalis 2013; Tu et al. 2015), and consistent with the other hypotheses about differences in factors believed to influence behavioural intentions, it was proposed that users would have lower levels of intention to secure their mobile devices than they would their home computers. This hypothesis (H9) was supported as intention to perform security behaviours was significantly lower for smartphones/tablets than for than for home computers/laptops (Mean 4.91 vs. 5.91, Mdn 5.00 vs. 6.00; $U = 29{,}374$, $Z = -8.90$, $p < .001$).

The final hypothesis (H10) relates to the information security behaviours undertaken by users, and it was hypothesised that users are less likely to perform security behaviours on their mobile devices than their home computers. Participants were asked about four specific behaviours and Table 5 summarises the extent to which the participants reported performing each of these behaviours for home computers/laptops and for smartphones/tablets. Chi-square tests of independence were used to test for differences in security behaviour.

As shown in Table 5, users were much more likely to be actively protecting their home computer/laptop than they were to be protecting their smartphone/tablet. Overall levels of backing up were relatively low with only 57.8% of the home computer users having recent backups and only 36.2% of the mobile device users having recent backups for their mobile device. This figure for mobile devices is relatively consistent with the 41% reported by Boyles, Smith, and Madden (2012). The proportion of those who kept backups was, however, significantly lower for mobile devices ($\chi^2(2, N = 629) = 31.9$, $p < .001$). It was also significantly lower for enabling automatic updating of software (68.0% vs. 54.4%, $\chi^2(2, N = 629) = 12.6$, $p = .023$).

The proportion of people who used security software (e.g. anti-virus/anti-malware) was reassuringly large for home computers (85.4%), but significantly lower for smartphones/tablets at only 44.6% ($\chi^2(2, N = 629) = 116.5$, $p < .001$). The final security measure included related to password use. Whilst 80.4% secured their home computer/laptop with a password, significantly fewer participants (59.0%) secured their smartphone/tablet in this way ($\chi^2(2, N = 629) = 35.4$, $p < .001$). This level of password protection of mobile devices is consistent with the 'close to half' not using passwords reported by Imgraben, Engelbrecht, and Choo (2014). Given these differences, H10 was supported; that is, users are less likely to perform security behaviours on their mobile device than their home computer. It was also interesting to note the percentages of participants who were unsure whether or not they had recent backups available (10.6% for home computers and 11.4% for smartphone/tablets),

Table 5. Comparison of security behaviour between home computers and mobile devices.

	Home computer/laptop			Smartphone/tablet		
	Yes (%)	No (%)	Unsure (%)	Yes (%)	No (%)	Unsure (%)
Have recent backups	57.8	31.7	10.6	36.2	52.4	11.4
Enabled automatic updating of software	68.0	23.9	8.1	54.4	32.6	13.0
Use security software	85.4	10.2	4.3	44.6	43.3	12.1
Device secured with password	80.4	15.8	3.7	59.0	35.5	5.5

whether they had enabled automatic updating of software (8.1% for home computers and 13% for smartphone/tablets) and whether or not they were using security software for their smartphone/tablet (12.1%). This uncertainty is consistent with results from Clarke et al. (2016), who found that over 20% of mobile device users did not know what security measures they were using.

6. Discussion

This research explored differences across device types in how personal computing users view security threats and their ability to protect against them, as well as their protective behaviour. In each case where there was a difference, the direction of the difference was such that it was likely to predispose personal computing users to be less likely to protect their mobile device than they would be to protect their home computer (according to theories such as PMT; Rogers 1975, 1983). These differences suggest that changing users' perceptions of threats and their perceptions of their ability to deal with them will be important in improving mobile device security.

Although users reported similar levels of perceived vulnerability for both types of device, they believed that the consequences of a breach would be more severe if it occurred on their home computer. As the results of this study and previous studies (Chin et al. 2012; Dulaney et al. 2014) show, many people are still reluctant to use their mobile devices for important transactions and it is hence understandable that for many the severity of a breach would be worse if it occurred on their home computer. However, this use pattern is changing, with younger users no longer so reluctant to use mobile devices for banking (Harris et al. 2016). Consistent with the results from Harris et al. (2016) and Alsaleh, Alomar, and Alarifi (2017), post hoc analysis of our data suggests that age is associated with willingness to use mobile devices to make financial transactions, with those under 45 years significantly more likely to use mobile devices for banking ($\chi^2(1,\ N = 623) = 9.39;\ p = .002$) and shopping ($\chi^2(1,\ N = 623) = 9.28;\ p = .002$). It appears likely that use of mobile devices for these kinds of transactions will normalise over time and it is important that perceptions of severity also shift accordingly, because of their potential impact on behaviour. Otherwise, users may face increased risk of security breaches if they continue to perceive the severity of security threats to mobile devices as relatively low.

The levels of factors associated with ability to cope with threats also differed between device types. Users had lower levels of belief in their ability to protect their mobile devices, believed that protective measures for mobile devices were less effective than those for home computers and that the costs associated with protecting mobile devices were higher. These findings are consistent with reports of users' lack of awareness of how to protect these devices (Das and Khan 2016; Mylonas, Kastania, and Gritzalis 2013; Vecchiato and Martins 2015) and of usability issues associated with protection measures for mobile devices (Botha, Furnell, and Clarke 2009; Kelley et al. 2012). As increasing numbers of users rely on mobile devices for their personal computing needs, it is important that they possess the knowledge, skills and confidence to be able to effectively protect themselves. Therefore, targeting usability in future product development could have immediate benefits. As Sobel and McGraw (2010) noted, there are market incentives for smart mobile device manufacturers and developers to do so.

It has been suggested that social influences on security behaviour are particularly important in the context of personal computing because users do not have access to the formal approaches to improving security that organisations implement (Anderson and Agarwal 2010; Tu et al. 2015). Contrary to expectations, no differences in levels of subjective norm were found; also average levels of subjective norm associated with both types of devices were relatively low. That is, users did not feel that others who are important to them held strong beliefs about the protective measures they should take for either type of device. In an organisational context, it has been suggested that organisations should task influential people with motivating and shaping the opinions of colleagues. This, however, is not possible in a home user environment.

There was, however, a difference in levels of descriptive norm, with users being more likely to believe that others implemented home computer security than mobile device security. These beliefs are consistent with our finding that lower levels of security actions are being taken for mobile devices than for home computers, and with previous research (Imgraben, Engelbrecht, and Choo 2014; Mylonas, Kastania, and Gritzalis 2013; Tu et al. 2015). Smartphones and tablets are highly visible because of their use in social settings, and Tu et al. (2015) argue that because of this, device risks will be discussed and possible solutions emerge. This, however, does not seem to be occurring to a great degree and suggests that users need to see others taking protective action and to hear them talk about it. If mobile device users hear their social group discussing information security threats and sharing knowledge about sources of information this should help bring both existing quality resources and new ones as they are developed into the broader consciousness.

Imgraben, Engelbrecht, and Choo (2014) identified the need for regular ongoing training programs for mobile device users to promote a culture of security. Whilst achievable within an organisation, this approach is less practical in the personal computing context, where users do not have easy access to training and where information sources tend to be informal (Furnell, Bryant, and Phippen 2007). Although user security education websites exist, they have had low levels of use (Howe et al. 2012). For security websites to be useful, mobile device users need to be aware of them, and engaging reminders such as Facebook's Privacy Dinosaur have the potential to influence personal users to protect their privacy when using mobile devices.

Much has been written about the strength of people's attachment to their smartphones (Gikas and Grant 2013; Keller 2011; Walsh et al. 2011) and we therefore incorrectly anticipated that users would have stronger levels of psychological ownership of their mobile devices. The higher levels of psychological ownership found for home computers are likely to be because these devices are the primary long-term repository of personal and financial information for many people and the device they most often use for important transactions. It is also possible that greater expenditure on home computers/laptops has contributed to greater psychological ownership, and this should be explored in future research. It seems likely that as the shift to mobile devices continues this will change and, consistent with the findings of Anderson and Agarwal (2010), increasing levels of psychological ownership associated with mobile devices should help to improve security behaviour in the future.

There are several limitations associated with this project. One limitation is that fear (an emotional feeling towards threat) was not included as one of the factors measured. Fear was included in the revised PMT (Rogers 1983) and although earlier behavioural security studies did not include it, a number of studies have explored its potential mediating role (e.g. Boss et al. 2015; Posey, Roberts, and Lowry 2015).

It should also be noted that participants were only recruited from the United States, thus limiting the ability to generalise more widely. They were also required to have both a home computer and a mobile device and this may have limited the participation of less wealthy personal computing users.

Crossler et al. (2013) called for more focus on actual behaviour as opposed to security intentions. The current study goes beyond intentions to actual behaviour but is limited by its reliance on self-report measures of behaviour with data collection at only a single point of time. Future research that combines multiple data collection points and direct measurement of behaviour will provide a more complete picture of information security behaviour using different device types.

7. Conclusion and future work

This study reports on a large-scale study to examine, if, and how, security perceptions and behaviours vary between home computer use and mobile device use. It addresses calls for increased research on mobile device security (Crossler and Bélanger 2014; Imgraben, Engelbrecht, and Choo 2014). The results of this study provide new evidence of major differences in how personal computing users perceive the threats associated with these devices and in perceptions associated with their ability to successfully protect their devices. This study has identified the need for mobile device users' perceptions of security threat severity to shift as patterns of use include more of the functions that have primarily been done on home computers. The study has also identified concerning differences in users' perceptions of their abilities to protect themselves; mobile devices users consider the costs of protecting themselves on these devices to be higher, and the efficacy of security solutions to be lower. Their security self-efficacy is also lower than with their home computers. Given these differences it is not surprising that less protective action is being taken with mobile devices. This paper discusses consequences of these differences and provides recommendations to address them in order to improve mobile device information security behaviour. Some of these recommendations flow from differences observed in descriptive norms. Users need to see others display protective behaviour and hear it discussed; therefore engendering a culture of discussion will be important.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Ajzen, I. 1991. "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* 50 (2): 179–211. doi:10.1016/0749-5978(91)90020-T

Alsaleh, M., N. Alomar, and A. Alarifi. 2017. "Smartphone Users: Understanding How Security Mechanisms are Perceived and New Persuasive Methods." *PLOS ONE* 12 (3): e0173284. doi:10.1371/journal.pone.0173284.

Anderson, C. L., and R. Agarwal. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioural Intentions." *MIS Quarterly* 34 (3): 613–643.

Ben-Asher, N., N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Moller. 2011. "On the Need for Different Security Methods on Mobile Phones." In *Proceedings of*

the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, 465–473. Stockholm, Sweden: ACM.

Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak. 2015. "What do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors." *MIS Quarterly* 39 (4): 837–864.

Botha, R. A., S. M. Furnell, and N. L. Clarke. 2009. "From Desktop to Mobile: Examining the Security Experience." *Computers & Security* 28 (3): 130–137.

Boyles, J. L., A. Smith, and M. Madden. 2012. *Privacy and Data Management on Mobile Devices*. Washington, DC: Pew Internet.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. "Information Security Awareness, Information Security Management, Compliance, Information Security Policy, Behavioral Issues of Information Security, Theory of Planned Behavior." *MIS Quarterly* 34 (3): 523–548.

Chin, E., A. P. Felt, V. Sekar, and D. Wagner. 2012. "Measuring User Confidence in Smartphone Security and Privacy." In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1–16. Washington, DC: ACM.

Clarke, N., J. Symes, H. Saevanee, and S. Furnell. 2016. "Awareness of Mobile Device Security: A Survey of User's Attitudes." *International Journal of Mobile Computing and Multimedia Communications* 7 (1): 15–31.

Crossler, R. E. 2010. "Protection Motivation Theory: Understanding Determinants to Backing up Personal Data." In *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS)*, 1–10. Kauai: IEEE.

Crossler, R. E., and F. Bélanger. 2014. "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument." *ACM SIGMIS Database* 45 (4): 51–71.

Crossler, R. E., A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. 2013. " Future Directions for Behavioral Information Security Research." *Computers & Security* 32: 90–101.

Dang-Pham, D., and S. Pittayachawan. 2015. "Comparing Intention to Avoid Malware Across Contexts in a BYOD-Enabled Australian University: A Protection Motivation Theory Approach." *Computers & Security* 48: 281–297. doi:10.1016/j.cose.2014.11.002

Das, A., and H. U. Khan. 2016. "Security Behaviors of Smartphone Users." *Information and Computer Security* 24 (1): 116–134.

Dulaney, K., V. L. Baker, R. Marshall, R. Cozza, T. Zimmerman, and D. A. Willis. 2014. *Predicts 2015: Mobile and Wireless*. Stamford, CT: Gartner.

Egelman, S., S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. 2014. "Are You Ready to Lock?" In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 750–761. Scottsdale: ACM.

Faruki, P., A. Bharmal, V. Laxmi, M. S. Gaur, M. Conti, and M. Rajarajan. 2014. "Evaluation of Android Anti-Malware Techniques Against Dalvik Bytecode Obfuscation." In *Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, 414–421. Beijing: IEEE.

Furnell, S. M., P. Bryant, and A. D. Phippen. 2007. "Assessing the Security Perceptions of Personal Internet Users." *Computers & Security* 26: 410–417.

Gikas, J., and M. M. Grant. 2013. "Mobile Computing Devices in Higher Education: Student Perspectives on Learning with Cellphones, Smartphones & Social media." *The Internet and Higher Education* 19: 18–26.

Harris, M. A., A. G. Chin, and R. Brookshire. 2015. "Mobile App Installation: The Role of Precautions and Desensitization." *Journal of International Technology and Information Management* 24 (4): 47–62.

Harris, M., K. C. Cox, C. F. Musgrove, and K. W. Ernstberger. 2016. "Consumer Preferences for Banking Technologies by Age Groups." *International Journal of Bank Marketing* 34 (4): 587–602.

Herath, T., and H. R. Rao. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." *European Journal of Information Systems* 18 (2): 106–125.

Howe, A. E., I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. 2012. "The Psychology of Security for the Home Computer User." In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, 209–223. San Francisco, CA: IEEE.

Huang, J. L., P. G. Curran, J. Keeney, E. M. Poposki, and R. P. DeShon. 2012. "Detecting and Deterring Insufficient Effort Responding to Surveys." *Journal of Business and Psychology* 27 (1): 99–114.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security* 31 (1): 83–95. doi:10.1016/j.cose.2011.10.007

Imgraben, J., A. Engelbrecht, and K.-K. R. Choo. 2014. "Always Connected, but are Smart Mobile Users Getting More Security Savvy? A Survey of Smart Mobile Device Users." *Behaviour & Information Technology* 33 (12): 1347–1360.

Jeske, D., and P. van Schaik. 2017. "Familiarity with Internet Threats: Beyond Awareness." *Computers & Security 66*, 129–141. doi:10.1016/j.cose.2017.01.010

Jones, B. H., and A. G. Chin. 2015. "On the Efficacy of Smartphone Security: A Critical Analysis of Modifications in Business Students' Practices Over Time." *International Journal of Information Management* 35 (5): 561–571.

Kaiser Family Foundation. 2016. *Population Distribution by Age* 2014. Accessed July 14, 2016. http://kff.org/other/state-indicator/distribution-by-age/.

Karatzouni, S., S. F. Furnell, N. L. Clarke, and R. A. Botha. 2007. "Perceptions of User Authentication on Mobile Devices." In *Proceedings of the 6th Annual ISOneWorld Conference*, 1–13. Las Vegas, NV: Information Institute.

Keller, J. 2011. "The Slow-Motion Mobile Campus." *The Chronicle of Higher Education*, May 8.

Kelley, P. G., S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall. 2012. "A Conundrum of Permissions: Installing Applications on an Android Smartphone." In *Financial Cryptography and Data Security*, 68–79. Berlin: Springer.

Kowalski, S., and M. Goldstein. 2006. "Consumers" Awareness of, Attitudes Towards and Adoption of Mobile Phone Security." In *Proceedings of the 20th International Symposium on Human Factors in Telecommunication*, 20–23. Sophia-Antipolis: HTF.

Leavitt, N. 2005. "Mobile Phones: The Next Frontier for Hackers?" *IEEE Computer* 38 (4): 20–23.

Liang, H., and Y. Xue. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective." *Journal of the Association for Information Systems* 11 (7): 394–413.

Ludwig, A. 2014."Keynote." Paper read at Google IO Developers Conference, at San Francisco, CA.

McCracken, G. 1986. "Culture and Consumption: A Theoretical Account of the Structure and Movement of the Cultural Meaning of Consumer Goods." *Journal of Consumer Research* 13: 71–84.

Milne, G. R., L. I. Labrecque, and C. Cromer. 2009. "Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices." *Journal of Consumer Affairs* 43 (3): 449–473.

Munch, B., and C. Canales. 2014. *Mobile Device Proliferation is Forcing Network Leaders to Redesign Enterprise Wireless LANs*. Stamford, CT: Gartner.

Mwagwabi, F., T. McGill, and M. Dixon. 2014. "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)*, 3188–3197. Hawaii: IEEE.

Mylonas, A., D. Gritzalis, B. Tsoumas, and T. Apostolopoulos. 2013. "A Qualitative Metrics Vector for the Awareness of Smartphone Security Users." In *Proceedings of the International Conference on Trust, Privacy and Security in Digital Business*, 173–184. Prague: Springer.

Mylonas, A., A. Kastania, and D. Gritzalis. 2013. "Delegate the Smartphone User? Security Awareness in Smartphone Platforms." *Computers & Security* 34: 47–66.

Ng, B. Y., and M. A. Rahim. 2005. "A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security." In *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, 234–247. Bangkok: AIS.

Nunnally, J. C. 1978. *Psychometric Theory*. 2nd ed. New York: McGraw-Hill.

Öğütçü, G., ÖM Testik, and O. Chouseinoglou. 2016. "Analysis of Personal Information Security Behavior and Awareness." *Computers & Security* 56: 83–93. doi:10.1016/j.cose.2015.10.002

Pierce, J. L., T. Kostova, and K. T. Dirks. 2003. "The State of Psychological Ownership: Integrating and Extending a Century of Research." *Review of General Psychology* 7 (1): 84–107.

Posey, C., T. Roberts, and P. B. Lowry. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets." *Journal of Management Information Systems* 32 (4): 179–214.

Rastogi, V., Y. Chen, and X. Jiang. 2014. "Catch Me If You Nan: Evaluating Android Anti-Malware Against Transformation Attacks." *IEEE Transactions on Information Forensics and Security* 9 (1): 99–108.

Rivis, A., and P. Sheeran. 2003. "Descriptive Norms as an Additional Predictor in the Theory of Planned Behaviour: A Meta-Analysis." *Current Psychology* 22 (3): 218–233.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change." *Journal of Psychology* 91 (1): 93–114.

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation." In *Social Psychophysiology*, edited by J. T. Cacioppo and R. E. Petty, 153–176. New York: Guilford Press.

Sasse, M., S. Brostoff, and D. Weirich. 2001. "Transforming the 'Weakest Link' – A Human/Computer Interaction Approach to Usable and Effective Security." *BT Technology Journal* 19 (3): 122–131.

Shaikh, A. A., and H. Karjaluoto. 2015. "Mobile Banking Adoption: A Literature Review." *Telematics and Informatics* 32 (1): 129–142.

Siponen, M., A. Mahmood, and S. Pahnila. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study." *Information & Management* 51 (2): 217–224. doi:10.1016/j.im.2013.08.006

Sobel, A. E., and G. McGraw. 2010. "Interview: Software Security in the Real World." *IEEE Computer* 43 (9): 47–53.

Symantec. 2017. *Internet Security Threat Report*. Symantec Corporation. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Taylor, S., and P. A. Todd. 1995. "Understanding Information Technology Usage: A Test of Competing Models." *Information Systems Research* 6 (2): 144–176.

Tu, Z., O. Turel, Y. Yuan, and N. Archer. 2015. "Learning to Cope With Information Security Risks Regarding Mobile Device Loss or Theft: An Empirical Examination." *Information & Management* 52 (4): 506–517. doi:10.1016/j.im.2015.03.002

Vance, A., M. Siponen, and S. Pahnila. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory." *Information & Management* 49 (3): 190–198.

Vecchiato, D., and E. Martins. 2015. "Experience Report: A Field Analysis of User-Defined Security Configurations of Android Devices." In *Proceedings of the 2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE)*, 314–323. Gaithersburg, MD: IEEE.

Walsh, S. P., K. M. White, S. Cox, and R. M. Young. 2011. "Keeping in Constant Touch: The Predictors of Young Australians' Mobile Phone Involvement." *Computers in Human Behavior* 27 (1): 333–342.

West, R. 2008. "The Psychology of Security." *Communications of the ACM* 51 (4): 34–40.

White, G. L. 2015. "Education and Prevention Relationships on Security Incidents for Home Computers." *Journal of Computer Information Systems* 55 (3): 29–37.

Wood, P., B. Nahorney, K. Chandrasekar, S. Wallace, and K. Haley. 2015. *Symantec Internet Security Threat Report*. Symantec Corporation. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

Woon, I., G. Tan, and R. Low. 2005. "A Protection Motivation Theory Approach to Home Wireless Security." In *Proceedings of the Twenty-Sixth International Conference on Information Systems*, 367–380. Las Vegas: AIS.

Workman, M., W. H. Bommer, and D. Straub. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test." *Computers in Human Behavior* 24 (6): 2799–2816.

Zhang, L., and W. C. McDowell. 2009. "Am I Really at Risk? Determinants of Online Users" Intentions to use Strong Passwords." *Journal of Internet Commerce* 8 (3): 180–197.

Appendix. Items used to measure constructs (where device was either 'smartphone/tablet' or 'home computer/laptop')

Construct	Items
Perceived severity (Ifinedo 2012; Woon, Tan, and Low 2005; Workman, Bommer, and Straub 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, Mahmood, and Pahnila 2014; Woon, Tan, and Low 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 are vulnerable to security breaches
	I could fall victim to a malicious attack if I fail to follow good security practices
Response cost (Woon, Tan, and Low 2005; Workman, Bommer, and Straub 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, Tan, and Low 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
Security 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 behaviour 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 personalised my *device* to better suit the way I use it
	I see my *device* as an extension of myself
Intention to perform security behaviours (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 behaviour (developed using the format of Liang and Xue 2010)	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