Protection Motivation Theory and Smartphone Security Behaviour: A qualitative investigation

[redacted]

This report is submitted in partial fulfilment

of the degree

of Master of Psychology (Organisational and Human Factors)

School of Psychology

University of Adelaide

October 2019

Literature Review Word Count: 4883

Research Report Word Count: 7682

Table of Contents

Declaration

This report contains no material which has been accepted for the award of any other degree or diploma in any University, and, to the best of my knowledge, this report contains no materials previously published except where due reference is made.

I give permission for the digital version of my thesis to be made available on the web, via the University’s digital research repository, the Library Search and also through web search engines, unless permission has been granted by the School to restrict access for a period of time.

[redacted]

October 2019

Acknowledgements

To my supervisors Kathryn Parsons, Dragana Calic and Clemence Due, I would like to sincerely thank you all for your continued support and encouragement throughout this year. You provided me with expertise, energy and passion for research that inspired me to delve deeper into my own research. I am truly grateful to have had the opportunity to work with you all this year.

I owe enormous gratitude to my parents, Louise and Wayne, along with my siblings, Harry, Josh and Hamish for their continued encouragement, and to my beautiful friends whose continued support and reassurance was unwavering. I could not have come this far without you all.

To my classmates, thank you for making the last two years more enjoyable than I could have asked for. Finally, I would like to acknowledge the invaluable contribution of the participants in this study. Without your perspectives this research would not have been possible.

List of Tables

Research Report

List of Figures

Literature Review

Research Report

Literature Review

Word count: 4883

Abstract

This review provides an initial assessment of the literature on smartphone reliance and the lack of good security behaviours displayed on smartphones within the general population. Protection Motivation Theory (PMT) is commonly used within information security contexts to investigate why someone might chose to engage in risky smartphone behaviour. There is theoretical support for PMT within both organisational and home settings. However, there is a lack of research within the PMT and smartphone context; therefore, an empirical investigation is warranted. Given the findings of this review, future research should examine user behaviour on smartphones across contexts.

Keywords: Information Security, Protection Motivation Theory, Smartphones

Introduction

Understanding human interaction with technology, and more specifically the proliferation of smartphone devices has presented a whole host of new challenges for user information security (Mylonas, Gritzalis, Tsoumas, & Apostolopoulos, 2013). Safeguarding people against the dangers these technologies may impose on everyday lives is essential. There has been rapid development into the user-experience of smartphone devices, providing intuitive operating systems and with that, methods to protect the user against threats (Das & Khan, 2015). However, as well designed as some smartphone device security systems may be, they require interaction with people who may not be as knowledgeable about security or are often not as vigilant as they should be (Allam, Flowerday & Flowerday, 2014). People are notorious for being the weak link in this process (Winnefeld, Kirchhoff, & Upton, 2015). Despite the simplicity of some security features available on smartphone devices, a human user who ignores these will ultimately fail to protect the system and themselves. For example, users can require a code or biometric to access their smartphone, but many people fail to use these simple security features. Consequently, it is important, to investigate the user relationship with, as well as their attitude and perceptions toward protecting that smartphone device, and the information it may contain. In the interest of brevity, ‘smartphone device’ will be referred to as ‘smartphone’ throughout the remainder of this review.

Modern day smartphone reliance

The use of smartphones as a person’s sole device has seen a dramatic increase in recent years, often replacing rather than complementing other technological devices such as laptops and personal computers (PC’s) (Verkijika, 2018). It has been predicted that the number of smartphone users in the world will surpass the 2.5 billion mark in 2019 (Statista, 2016). A smartphone is described as an internet enabled device that is complimented by intuitively designed interfaces and continuously advancing operating systems (Verkijika, 2018; Wang, Xiang, & Fesenmaier, 2014). The rapid innovation in technology means that the smartphone offers features beyond the traditional texting and telephoning functions (Clarke, Symes, Saevanee & Furnell, 2016). Smartphones offer users all the functionality and capability they once had via PC, now accessible in one's pocket and for a much lower cost (Haris, Haddadi, & Hui, 2014). This has greatly enhanced user productivity and efficiency when performing daily tasks such as email, social media, banking, calendar management, online shopping, navigation, and even entertainment such as watching YouTube videos and movies (Clarke et al., 2016; Das & Khan, 2015). Smartphones also include functions to aid the creation, sharing and consumption of content, making them more powerful than PC's have been in the past ten years (Das & Khan, 2016). Similarly, this surge in smartphone adoption has been reflected within the organisational setting, enabling a new level of operational efficiency, benefitting employers by having a constantly connected workforce (Allam, Flowerday, & Flowerday, 2014). More recently, smartphones can perform wireless payments, replacing the conventional debit or credit card which ultimately could eliminate the need to carry a wallet altogether (Clarke et al., 2016; McGill & Thompson, 2017). To utilise many of the smartphone features to their full potential, users are required to disclose their personal information such as names, addresses, financial and other sensitive information, wearable tracking device data, location, email addresses and photos to name a few. Smartphones therefore are multipurpose, servicing the users' personal as well as professional endeavours, and as a direct result, tremendous amounts of private, sensitive and confidential information is often stored and processed on smartphones (Alsaleh, Alomar, & Alarifi, 2017). Therefore, while smartphones and their versatile functions enable users to have a truly wireless, and connected lifestyle, they also pose significant security and privacy threats (Torre, Sanchez, Koceva, & Adorni, 2018).

Smartphone security

User information privacy is defined as the interest one has in controlling or influencing the management and usage of sensitive data about themselves (Chen & Li, 2017). This includes the user's willingness to disclose personal and sensitive information. This is particularly pertinent to smartphone use as numerous smartphone functions are dependent on users' personal and sensitive information, and people are often largely unaware of the extent to which they have allowed their information to be accessed and shared to third parties (Alsaleh et al., 2017). More than ever before, mobile services are collecting and analysing user information, often without the user being aware they have provided informed consent. Therefore, arguably the biggest concern to information security is the lack of control over the use and access of private information (Chen & Li, 2017).

Information security is concerned with the protection of information systems (IS) from unauthorised access and disclosure of information, which provides confidentiality and integrity of technology to the user, ultimately preventing misuse of information (Ophoff & Robinson, 2014). Historically, smartphones have been one of the most valuable items targeted in theft and robberies (Clarke et al., 2016). This was due to the high value of the hardware itself. Now, however, the increased functionality of smartphones, and especially the sensitive and other information that may be stored on these smartphones represents a more superior target (Verkijika, 2018). The theft or access to a smartphone could enable various fraudulent purposes such as stolen identities, online purchases, blackmail, extortion and the re-sell value of the hardware (Clarke et al., 2016). Smartphones are an attractive target, and there are many ways that hackers can install malware onto a victims device, gaining unauthorised access to sensitive information (Alsaleh et al., 2017).

Not only is the theft or physical loss of a smartphone a threat to user security and privacy, it is also common that users have unknowingly downloaded malware onto their smartphones through seemingly harmless functions, such as by downloading a mobile application (app) or using public Wi-Fi (Alsaleh et al., 2017). For example, McGill and Thompson (2017) found over 18 million mobile malware detections in 2016, an increase of 105% compared to the previous year. The same research found that smartphone vulnerabilities had experienced a growth of 32% in that same year. More recent research detected over 8.5 million malicious smartphone installation packages, 128,886 smartphone banking trojans and 261,214 ransomware trojans (Verkijika, 2018).

With all this information, one might assume that users would exercise extreme caution when operating and securing their smartphones, however research has found the opposite. Users are generally nonchalant in their attitudes and behaviours towards smartphones and information security (Clarke et al., 2016). Current research suggests that smartphone users are largely unaware of their susceptibility (Hewitt, Dolezel & McLeod, 2017). Further to this, many users tend to ignore security mechanisms or feel that they are generally ineffective in preventing or reducing the dangers and threats associated with using smartphones (Kusyanti & Puspa, 2018; Mylonas, Kastania, & Gritzalis, 2013). For example, one study on behaviour related to app downloads investigated whether the user considered security while choosing to download apps. They found that users were unable to comprehend selected permissions when downloading apps and the risks related to this decision, choosing to ignore security messaging (Mylonas et al., 2013). Not only is this concerning for achieving good information systems security (ISS) in the general population, but it may be even more concerning for organisations whose employees have access to personal and sensitive client or organisational information who are often not adequately skilled to ensure good security settings on their smartphones (Allam et al., 2014).

ISS research has focussed less attention the human factors involved, compared to technical aspects, such as the design and structure of protection software and firewalls

(Ophoff & Robinson, 2014). Despite human users playing a significant role in the security ecosystem, their part is often undervalued and research into user behaviour is not as extensive as the research into the technology aspect of security models (Mylonas et al., 2013). It must be understood that for the most part, humans are predominately the weak link in this scenario as their actions directly influence the strength of their security and privacy (Winnefeld et al., 2015). The most complex security systems and processes still need to be actioned by the human operator. Relevant specifically to smartphones, it is the case that people often fail to secure their smartphone and information appropriately, leaving their personal and sensitive information in the reach of those with malicious intentions (Leavitt, 2011). Other investigations have also found that users often download third-party apps from unregistered or unofficial channels (i.e., pirated apps) which have been notoriously difficult to regulate (Chen & Li, 2017; Kusyanti & Puspa, 2018; Leavitt, 2011). An investigation into these unregulated app platforms found that 82 percent of these malicious apps have the ability to send, receive and collect short messages, often without the user's knowledge. In addition to this, mobile viruses, phishing links and other malicious malware are real threats to user security and privacy (Chen & Li, 2017).

To prevent these threats from becoming real scenarios, the user must action information security behaviours to protect their data and therefore privacy. These can include, however are not limited to; using passcodes, backing up data, and not connecting to public Wi-Fi (Alsaleh et al., 2017; Haris et al., 2014). However, research suggests that user attitude toward these behaviours is incredibly lax. Take app permissions as mentioned previously, the smartphone user must accept an app permission prior to the download. Research into this protective behaviour found that users often do not read app permissions, however, also found that users were often unaware of dangers in accepting permissions and the extent of access they might be allowing to sensitive information (Haris et al., 2014). This has been found to go so far as apps having the ability to take users' photos without their permission (Kusyanti & Puspa, 2018).

Previous studies have found that even people who have fallen victim to a mobile security related incident still fail to secure their smartphones with something as simple as a passcode or pin (Clarke et al., 2016). Research has highlighted a disconnect between user desire for security, compared to the effort required to install and manage reliable security controls (Clarke, et al., 2016).

Protection Motivation Theory

A growing body of literature has focussed on why people might act in a dissonant manner and chose not to protect themselves against threat or danger. This research is based on understanding attitudes, motivations, intentions and adoption of behaviours towards protecting one's information security.

The literature that has investigated ISS behaviours, and the motivation behind performing these behaviours, has been dominated by *Protection Motivation Theory* (PMT), with the intention to explain the common disparity between what a user thinks or knows that they should do, compared to what they actually do (Rogers, 1975). PMT has become a leading model used by researchers in understanding ISS behaviours. This includes on a desktop computer (Anderson & Agarwal, 2010; Hanus & Wu, 2016) on a smartphone (Tu, Turel, Yuan, & Archer, 2015; Verkijika, 2018), in organisational (Ifinedo, 2011; Vance, Siponen, & Pahnila, 2012) personal (Thompson, McGill, & Wang, 2017) and in Bring Your Own Device (BYOD) settings (Dang-Pham & Pittayachawan, 2015; Hovav & Putri, 2016). Research into specific behaviours such as using strong passwords (Zhang & McDowell, 2009), downloading apps (Kusyanti & Puspa, 2018), and using anti-viral software (Tsai et al., 2016) have also utilised the theory.

The model, first coined in 1975 by Rogers, has been applied to numerous studies to understand protective behaviour, predominately related to health (Milne, Sheeran, & Orbell, 2000). The initial model was guided by the research of fear appeals, and developed based on expectancy-value theory (Floyd, Prentice-Dunn, & Rogers, 2000; Rogers, 1975). According to the original theory, “a fear appeal is an informative communication about a threat to an individual’s well-being” (Milne et al., 2000, p. 107). It was understood that fear-appeals could encourage change in attitudes and therefore in behaviours, however it was unknown how and why this change occurred. This idea motivated Rogers’ research, and the initial theory operationalised the components of a fear appeal, consisting of: perceived severity, perceived vulnerability, response efficacy and response cost, initiating what is referred to as a ‘cognitive mediating process’ (Maddux & Rogers, 1983; Rogers, 1975). The modern-day theory of PMT consists of two cognitive processes, the threat-appraisal and the coping-appraisal. The threat-appraisal process considers the likelihood and impact of the risk, while the coping-appraisal process considers the effectiveness of the adaptive response and the individual’s ability to perform this behaviour (Verkijika, 2018). The original theory was eventually broadened to include the components of ‘perceived reward’ and ‘self-efficacy’, how these fit within the theory will be explained in more detail below (Rogers, 1983; Maddux & Rogers, 1983).

Since its initial coining, the core concepts of PMT have remained robust (Martens, De Wolf, & De Marez, 2019). Essentially, it suggests that a threat-appraisal occurs first, which evaluates the components of a fear appeal that arise when an individual feels threatened, so that when an individual is faced with a risk, their behaviour in response to that risk is motivated by the appraisal processes (Floyd et al., 2000; Milne et al., 2000; Verkijika, 2018). The coping-appraisal process then requires the individual to assess the protective behaviour or adaptive response in order to minimise the threat, this process can be visualised in *Figure 1*. Each of the components within the model will be explained below.

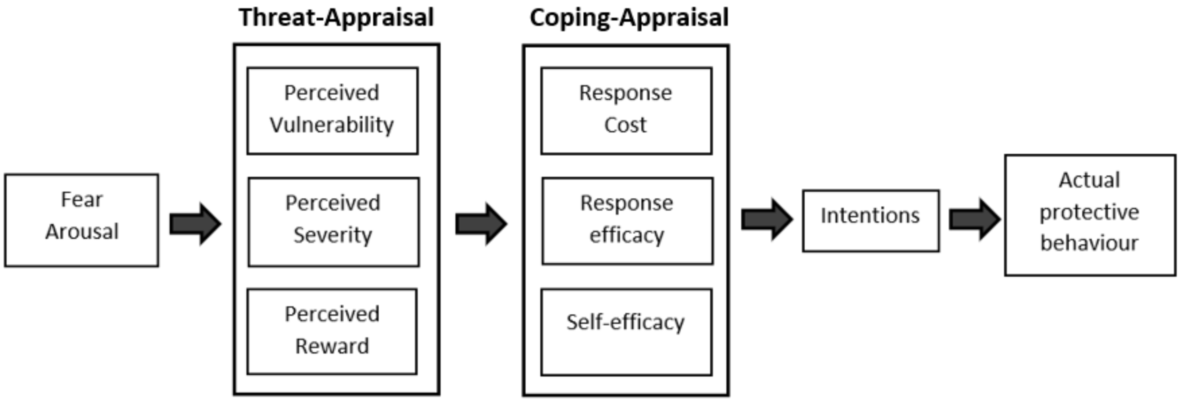


Figure 1. Diagram of Protection Motivation Theory

1. *Perceived severity* is the magnitude, or how serious the individual judges the threat to be (Milne et al., 2000; Vance et al., 2012). In other words, how detrimental the user perceives consequences of the threat to be (Verkijika, 2018). For example, Reeves, Parsons and Calic (2017) found that when asked about mobile computing/IoT, employees who felt more personally at risk (e.g., of reprimand, reduced productivity, personal data loss) were more likely to avoid behaviours that may lead to the risk event.

2. *Perceived vulnerability* regards an individual's level of personal susceptibility to a threat, or their perception of the probability of the threat actually occurring (Liang & Xue, 2010; Milne et al., 2000). With regards to smartphone security, this concerns a user's perception or belief around the likelihood that their device is inclined to a security threat (Verkijika, 2018).

3. *Perceived reward* regards any benefit to the user, whether it be intrinsic or extrinsic, that motivates the user to continue or even increase the maladaptive response,

disregarding the protective behaviour, such as downloading free pirated apps and ignoring privacy statements (Vance et al., 2012).

4. *Response efficacy* refers to an individual's belief that the coping response or protective behaviour is actually capable of reducing the threat (Milne et al., 2000). In terms of smartphone security, it is the extent to which an individual perceives that behaving securely effectively minimises the risk of a threat occurring (Verkijika, 2018).

5. *Response cost* refers to the perceived cost associated with implementing the protective behaviour (Vance et al., 2012). In other words how costly, whether it be monetary, time, or effort that performing the adaptive response is likely to afford (Milne et al., 2000).

6. *Self -efficacy* refers to an individual's level of perceived skill or ability in performing the protective behaviour (Verkijika, 2018). This can be conceptualised as ability or autonomy. Ability refers to how capable or competent the individual feels, and autonomy refers to an individual's capacity to protect themselves against a security threat on their smartphone (Sommestad, Karlzén, & Hallberg, 2015a; Vance et al., 2012).

In sum, the theory suggests that if vulnerability and severity are high, reward, fear and cost are low, and both efficacies are also high, the individual is likely to protect themselves against a potential threat. More often than not, these variables are assessed by measuring intentions to adopt, through observing actual behaviour or self-reported behaviour (Tu, Yuan, & Archer, 2014).

Protection Motivation Theory and Information Security

As discussed previously, there is a substantial body of literature exploring PMT in a range of contexts, including how the different PMT factors are linked to information security behaviours (Blythe, Coventry & Little, 2015; Sommestad et al., 2015a). It has been applied to a range of common information security contexts (Tsai et al., 2016), populations (Dang-Pham & Pittayachawan, 2015; Verkijika, 2018), devices (Anderson & Agarwal, 2010), and settings (Herath & Rao, 2009; Lee & Larsen, 2009; Siponen, Adam Mahmood, & Pahnila, 2014). Much of the earliest research concentrated on investigating desktop computers and employee policy compliance (Ifinedo, 2011; Johnston & Warkentin, 2010).

It is important to note that although the majority of previous research has focused on work or organisational contexts, there has been some disagreement that the conclusions drawn within this setting are applicable to the home context (Dang-Pham & Pittayachawan, 2015). Throughout the literature there is evidence to suggest that perception and therefore response to threats are not the same across different contexts and settings. As has been suggested within the literature, applying PMT to an organisational context implies that fear is influencing behaviour, and that users perceive organisational risk at the same level as personal risk. This is, however, not always the case - how an individual perceives organisational information and assets as personally important or relevant will vary (Hovav & Putri, 2016). This has been found to directly influence actual performed behaviour, Dang-Pham & Pittayachawan (2015) found a difference in protective behaviours on the same device when the setting was at university or at home. For example, students were more likely to avoid malicious websites at home due to a lack of confidence in home security settings, whereas they were more likely to physically lock and securely store the device at university due to a higher risk of theft and loss. The relevance of the copying-appraisal variables within the organisational setting have been questioned, due to behaviours being mandatory

(Sommestad et al., 2015a; Verkijika, 2018). Therefore cost, ability, and effectiveness of response are not always relevant to an employee who is mandated by policy. More recent criticisms are that home users may not have access to the same security training or support within the home context, that they rely on ill-informed information sourced from family and friends, that there is a greater requirement for self-reliance, and that they perceive their personal information as not important enough to be targeted (Anderson & Agarwal, 2010; McGill & Thompson, 2017). The importance of understanding and educating the home user has become even more apparent, as the translation of behaviours, and use of personal devices within the organisational context has potential dangers for organisational privacy and security. More importantly, the rapid adoption of smartphones within both personal and organisational contexts encourages that research focus on this user relationship, an idea explored below. Although the PMT has been used to examine information security behaviours in both organisational and home contexts, as discussed in the next sections, to date the findings have been mixed, and no study has yet to compare smartphone security behaviour in work and home contexts.

PMT and information security behaviour online

Some of the earliest PMT research into information security behaviour looked at user protection behaviours online. One of the initial studies found consistency with PMT, in that perceived vulnerability to virus threats, response efficacy of virus protection and self-efficacy in identifying and correctly installing the anti-viral protection were all found to be significant predictors of behavioural intentions to adopt protective behaviours. Perceived severity did not have a significant influence on this population. This was justified in that severity has little influence if an individual doesn’t believe they are vulnerable to that threat in the first instance (Lee, Larose, & Rifon, 2008). In a similar study, Zhang & McDowell (2009) investigated college students’ intentions to use strong passwords online. This study found that fear arousal, response cost and response efficacy were significantly related to user intention towards protective behaviour. In this instance, factors in the coping appraisal process were more important than those in the threat appraisal process. The authors suggest this might be because when creating a password there is no immediate visible threat, therefore risk is hypothetical, and this lessened the motivation to protect (Zhang & McDowell, 2009). In more recent research, Tsai et al. (2016) similarly investigated internet users safety precautions. The PMT model explained 29% of variance in security intentions, which increased to 43% with the inclusion of additional variables. The study found response efficacy to be the most stable predictor, along with response cost having a significant negative relationship with intention as PMT suggests (Tsai et al., 2016).

PMT and information security in organisational settings

A large portion of the research on PMT and Information Security has been in an organisational context, often investigating employee compliance towards security policies. Vance et al. (2012) found perceived severity to have a significant positive impact on employees' intention to comply with information security policies, as is supported by several studies investigating PMT and employee policy compliance (Herath & Rao, 2009b; Lee & Larsen, 2009; Siponen et al., 2014). While there is some evidence suggesting that perceived vulnerability might influence employee intentions to comply with security policies (Lee & Larsen, 2009; Siponen et al., 2014), there is also evidence that suggests it is not a significant predictor (Herath & Rao, 2009b; Ifinedo, 2011; Vance et al., 2012). Ifinedo (2012) found response efficacy to have the strongest effect on compliance, meaning employees were motivated to adhere to policies if they believed there were high expected returns by doing so, with support in the literature for this (Herath & Rao, 2009b; Lee & Larsen, 2009). Conversely, Ifinedo (2012) did not find response cost to have a significant relationship, suggesting this might be due to differing perspectives on costliness of a response. The component of perceived reward has been a variable of interest included within this population setting, however Vance (2012) was the only study to find a significant negative relationship, which is consistent with PMT. Most stable of these findings has been that self-efficacy is consistently shown to influence employee intentions to comply with security policies of their organisations (Herath & Rao, 2009b; Lee & Larsen, 2009; Siponen et al., 2014; Vance et al., 2012).

PMT and information security behaviour in personal settings

A change in research focus has seen some of the most recent PMT studies into information security investigating user motivations, intentions and behaviours within the home setting. The findings within this context are arguably more consistent. Perceived severity was found to have a significant positive relationship with security behaviours in a number of studies (Anderson & Agarwal, 2010; Liang & Xue, 2009; Crossler & Bélanger, 2014; Martens et al., 2019). Similarly, there is consistent evidence for perceived vulnerability having a significant effect on protective behaviours (Anderson & Agarwal, 2010; Liang & Xue, 2010; Martens et al., 2019; Thompson et al., 2017). Despite this, Hanus & Wu (2016) did not find the same support, suggesting that vulnerability infers that the user is aware that a threat exists, which is often not the case especially in the home setting. Similarly, response efficacy has good support within the home context (Anderson & Agarwal, 2010; Crossler & Bélanger, 2014; Hanus & Wu, 2016; Liang & Xue, 2010; Martens et al., 2019). There were a number of studies that excluded response cost as a variable of interest, as it is suggested security behaviours are not costly (Zhang & McDowell, 2009). Despite this, the studies that did consider response cost found support for its inclusion (Hanus & Wu, 2016; Liang & Xue, 2010; Thompson et al., 2017). Self-efficacy also had consistent support within the literature (Anderson & Agarwal, 2010; Crossler & Bélanger, 2014; Hanus & Wu, 2016; Liang & Xue, 2010; Thompson et al., 2017). Although Martens et al. (2019) did not find the same support, they argued that this might be due to level of digital skill, suggesting that the previous literature has used population samples that are often highly educated (i.e. university students). Perceived reward was excluded as a potential variable in all the aforementioned studies.

PMT and ISS Behaviour on smartphones

As outlined initially, the emergence of smartphones within both organisational and home contexts has become increasingly apparent. PMT has more recently been utilised to examine why smartphone users may chose not to adopt protective behaviours. User relationship with a smartphone has looked at theft or loss (Tu et al., 2014), app permissions (Kusyanti & Puspa, 2018), general smartphone security (Verkijika, 2018), and comparisons between smartphone and PC behaviours (McGill & Thompson, 2017; Thompson et al., 2017). The findings across these contexts have been inconsistent. Perceived severity and perceived vulnerability have support within the literature (Thompson et al., 2017; Tu et al., 2015; Verkijika, 2018). This suggests that smartphone users will use protective behaviours if they feel vulnerable to threats and if the threat has severe consequences. Although not in line with the broader information security literature, there is a lack of evidence for response cost and efficacy within the mobile and smartphone context specifically (Thompson et al., 2017).. This suggests that the effectiveness and the cost of smartphone protective behaviours may not influence protective behaviour (Verijjika, 2018). Finally, in line with other information security research, self-efficacy has the most support within the PMT smartphone literature (Kusyanti & Puspa, 2018; Thompson et al., 2017; Tu et al., 2014; Verkijika, 2018). Interestingly, in a comparison study between users of both mobile devices and PC's, users had lower self-efficacy on their mobile phones compared to their PC's. They also believed that protective measures were less effective and more costly to perform on their mobile phones compared to PC's (McGill & Thompson, 2017). These findings suggest that due to the relative recency and rapid adoption of smartphone usage, users may lack awareness in how to appropriately and effectively protect their smartphones (McGill & Thompson, 2017). The importance of understanding and educating the home user has become increasingly apparent, as the translation of behaviours, and use of personal devices within the organisational context has potential dangers for organisational privacy and security. This confirms the need to educate users on the importance of knowledge, skill and confidence in effectively protecting their smartphones.

Additional Variables

The current evidence suggests that PMT constructs on average account for between .34 and .50 of the variance in that particular population (Sommestad et al., 2015a; Thompson et al., 2017). Like within any research context, it is important not to limit exploration, or to only consider one particular model or theory. For this reason, it is important to note that multiple studies throughout the literature have considered and found significant evidence for a variety of additional variables. These include; subjective norm (Anderson & Agarwal, 2010; Herath & Rao, 2009; Ifinedo, 2011; Martens et al., 2019; McGill & Thompson, 2017; Tsai et al., 2016), descriptive norm (Anderson & Agarwal, 2010; Herath & Rao, 2009; Thompson et al., 2017), psychological ownership (Anderson & Agarwal, 2010; Thompson et al., 2017), social influence (Johnston & Warkentin, 2010; Lee & Larsen, 2009; Tu et al., 2014), habit strength (Kusyanti & Puspa, 2018; Tsai et al., 2016; Vance et al., 2012), anticipated regret (Sommestad, Karlzén, & Hallberg, 2015b; Verkijika, 2018). Again, a majority of these identified factors have been identified as relevant within organisational and personal computer contexts, however little is known about their importance within the smartphone security setting (McGill & Thompson, 2017).

Discussion

In this review, we provide a detailed overview into the sudden dependence in smartphones, we identify that users are not protecting their smartphones appropriately, and we look at PMT as a model of explaining information security and smartphone behaviour. In this section, we briefly discuss the theoretical and applied implications of this review and propose a way forward.

Limitations and Implications

Referring to the evidence outlined above, it is clear there is still research to be done in understanding smartphone user security behaviour. It is understood that people do not behave safely on smartphones (Alsaleh et al., 2017; Chen & Li, 2017; Thompson & McGill, 2017). However, to explain this, there are still gaps that exist within the PMT literature. Most notably a lack of understanding into smartphone specific security behaviours and a lack of understanding to the extent of behaviour transfer between organisational and home settings. It is interesting then to consider the comparison in behaviour of a smartphone user across the organisational and personal contexts. Given the argument that coping-appraisal variables are not relevant to the organisational setting emphasises the need to understand whether smartphone users behave in the same way across contexts. Increasingly organisations are providing work-supplied smartphones to assist employees in their roles, and quite commonly these individuals will also own and regularly use a smartphone for personal and work use (Allam et al., 2014; Clarke et al., 2016; Hewitt et al., 2017). The degree to which organisational policies and procedures taught and practiced within the workplace then transfer to the use of a personal smartphone is unknown. If individuals behave unsafely on their personal smartphone devices in the workplace, this can expose the organisation to security risks that it does not have the ability or authority to prevent or protect as it is the individual’s personal device. This may be particularly true for smaller organisations that do not have the resources to educate employees on safe smartphone use.

Future Research Directions

Future research into smartphone security behaviour should endeavour to understand how people behave on their devices across contexts. The use of PMT in examining this comparison will inform how to best educate both home and organisational smartphone users. This investigation will expose whether training and education within the workplace setting transfers to the home setting. This will then inform researchers of the most effective way to educate smartphone users, especially if this training is required to be different depending on the context. This should aid in the overarching goal of achieving an effective level of security behaviours and awareness in the general population.

References

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*(C), 56-65. doi:10.1016/j.cose.2014.01.005

Alsaleh, M., Alomar, N., & Alarifi, A. (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. , & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions.(Report). *MIS Quarterly*, *34*(3), 613. doi:10.2307/25750694

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. *Symposium on Usable Privacy and Security, 1*, 103-122

Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behavior A technology threat avoidance perspective. *Information and Computer Security*, *25*(3), 330-344. doi:10.1108/ICS-04-2016-0027

Clarke, N., Symes, J., Saevanee, H., & Furnell, S. (2016) Awareness of Mobile Device Security: A survey of User's Attitudes. *International Journal of Mobile Computing and Multimedia Communications, 7*(1), 15-31. doi: 10.4018/IJMCMC.2016010102

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, *45*(4), 51-71. doi:10.1145/2691517.2691521

Dang-Pham, D., & Pittayachawan, S. (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

D'arcy, J., Hovav, A. & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20* (1), 79-98.

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security, 24*(1), 116-134. doi:10.1108/ICS-04-2015-0018

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta- Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology, 30*(2), 407.

Hanus, B., & Wu, Y. a. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management, 33*(1). doi:10.1080/10580530.2015.1117842

Haris, M., Haddadi, H., & Hui, P. (2014). Privacy Leakage in Mobile Computing: Tools, Methods, and Characteristics.

Herath, T. & Rao, H.R. (2009a). Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47* (2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106. doi:10.1057/ejis.2009.6

Hewitt, B., Dolezel, D., & McLeod, A. (2017). Mobile Device Security: Perspectives of Future Healthcare Workers. *Perspectives in Health Information Management, 14*, 1-8.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. Pervasive and Mobile Computing, 32, 35-49. doi:10.1016/j.pmcj.2016.06.007

Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1). doi:10.1016/j.cose.2011.10.007

Johnston, A., & Warkentin, M. (2010). FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY. MIS Quarterly, 34(3), 549. doi:10.2307/25750691

Kusyanti, A., & Puspa, H. (2018). An Empirical Study of App Permissions: A User Protection Motivation Behaviour. *International Journal of Advanced Computer Science and Applications*, 9(11). doi:10.14569/IJACSA.2018.091116

Leavitt, N. (2011). Mobile Security: Finally a Serious Problem? Computer, 44(6), 11-14. doi:10.1109/MC.2011.184

Lee, Larose, & Rifon. (2008). Keeping Our Network Safe: A Model of Online Protection Behaviour. Behaviour & Information Technology, 27(5), 445-454. doi:10.1080/01449290600879344

Lee, & Larsen. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems, 18(2), 177-187. doi:10.1057/ejis.2009.11

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. MIS Q., 33(1), 71-90. doi:10.2307/20650279

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. J. Assoc. Inf. Syst., 11(7), 394-413.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469-479. doi:10.1016/0022-1031(83)90023-9

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Computers in Human Behavior, 92, 139-150. doi:10.1016/j.chb.2018.11.002

McGill, T., & Thompson, N. (2017). Old risks, new challenges: exploring differences in security between home computer and mobile device use. Behaviour & Information Technology, 36(11), 1111-1124. doi:10.1080/0144929x.2017.1352028 y1 - 2017

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. Journal of Applied Social Psychology, 30(1), 106-143. doi:10.1111/j.1559-1816.2000.tb02308.x

Mylonas, A., Gritzalis, D., Tsoumas, B., & Apostolopoulos, T. (2013). A qualitative metrics vector for the awareness of smartphone security users. In (Vol. 8058, pp. 173-184).

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. Comput. Secur., 34(C), 47-66. doi:10.1016/j.cose.2012.11.004

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18* (2), 126-139.

Ophoff, J., & Robinson, M. (2014). Exploring end-user smartphone security awareness within a South African context. In (pp. 1-7).

Reeves, A., Parsons, K., & Calic, D. (2017). *Securing mobile devices: evaluating the relationship between risk perception, organisational commitment and information security awareness*. Paper presented at the International Symposium on Human Aspects of Information Security & Assurance (HAISA), Adelaide, Australia, 145-155. Editors: Steven Furnell, Nathan Clarke.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803

Rogers, R. W. (1983). *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, NY: Guilford Press; p. 153–75.

Siponen, M., Mahmood, M. A., & Pahnila, S. (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

Sommestad, T., Karlzén, H., & Hallberg, J. (2015a). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy (IJISP), 9(1), 26-46. doi:10.4018/IJISP.2015010102

Sommestad, T., Karlzén, H., & Hallberg, J. (2015b). The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information & Computer Security, 23(2), 200-217. doi:10.1108/ICS-04-2014-0025

Statista. (2016, 07/06/2016). Smartphone users worldwide 2014-2020. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. Computers & Security, 70, 376-391. doi:10.1016/j.cose.2017.07.003

Torre, I., Sanchez, O. R., Koceva, F., & Adorni, G. (2018). Supporting users to take informed decisions on privacy settings of personal devices. Personal and Ubiquitous Computing, 22(2), 345-364. doi:10.1007/s00779-017-1068-3

Tsai, H.-Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. Computers & Security, 59, 138-150. doi:10.1016/j.cose.2016.02.009

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. Information & Management, 52(4), 506. doi:10.1016/j.im.2015.03.002

Tu, Z., Yuan, Y., & Archer, N. (2014). Understanding user behaviour in coping with security threats of mobile device loss and theft. Int. J. of Mobile Communications, 12(6). doi:10.1504/IJMC.2014.064915

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), 190-198. doi:10.1016/j.im.2012.04.002

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. Computers & Security, 77, 860-870. doi:10.1016/j.cose.2018.03.008

Wang, D., Xiang, Z., & Fesenmaier, D. R. (2014). Adapting to the mobile world: A model of smartphone use. Annals of Tourism Research, 48, 11-26. doi:10.1016/j.annals.2014.04.008

Winnefeld, S. J. A., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity’s human factor: Lessons from the pentagon. Harvard Business Review, 2015(September), <xocs:firstpage xmlns:xocs=""/>.

Zhang, L., & McDowell, W. C. (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. Journal of Internet Commerce, 8(3-4), 180-197. doi:10.1080/15332860903467508

Research Report

Word count: 7682

Protection Motivation Theory and Smartphone Security Behaviour: A qualitative investigation

[redacted]

Affiliation: The University of Adelaide

Postal address: The University of Adelaide
SA 5005
AUSTRALIA

Email address: a1647943@student.adelaide.edu.au

Declarations of interest: none

Abstract

The use of smartphones as a person's sole device has seen a dramatic increase in recent years, as has concern for smartphone security. Protection Motivation Theory (PMT) used to investigate smartphone security behaviour has received preliminary support; however, the display of consistent behaviour across contexts is yet to be empirically explored. Therefore, this study examined smartphone security attitudes, motivations and behaviour on both personal and work devices. Ten working Australians participated in semi-structured interviews and the data was analysed using deductive and inductive thematic analysis, guided by PMT to explore the comparisons between personal and work devices. Results suggest that perceived vulnerability, perceived reward, response cost, self-efficacy and social influence largely contributed to a lack of protective behaviour displayed on personal smartphones. Despite the safe behaviour displayed on work smartphones, it is suggested these behaviours were motivated by organisational controls, rather than being intrinsically motivated. The findings of this research have applied implications for education programs within both home and workplace contexts. Future research should aim to improve current training and education so that skills and protective behaviours are transferred across contexts, as users understand the benefit to not only their organisation but to their individual safety.

Keywords: Smartphone, Smartphone Devices, Protection Motivation Theory, Information systems, Security behaviour

1. Introduction

Smartphone use has proliferated throughout our everyday, private and work lives. Smartphone security is a growing concern. To further this body of research, we explore smartphone users' attitudes, perceptions and behaviours towards the security of their work provided and personal smartphone devices. The use of smartphones as a person's sole device has seen a dramatic increase in recent years and this has introduced a whole host of new challenges for user information security (Mylonas, Gritzalis, Tsoumas, & Apostolopoulos, 2013; Verijika, 2018; Allam, Flowerday & Flowerday, 2014). A smartphone is defined as an internet enabled device that is complimented by intuitively designed interfaces and continuously advancing operating systems (Verkijika, 2018; Wang, Xiang, & Fesenmaier, 2014; Clarke, Symes, Saevanee & Furnell, 2016; Haris, Haddadi, & Hui, 2014). It has been predicted that the number of smartphone users in the world will surpass the 2.5 billion mark in 2019 (Statista, 2016). The introduction of smartphones has greatly enhanced user productivity and efficiency when performing daily tasks including functions to aid the creation, sharing and consumption of content such as emails, social media, navigation and online banking. Current smartphones are now more powerful than PC's have been in the past ten years (Das & Khan, 2016). Similarly, this surge in smartphone adoption has been reflected within the organisational setting, enabling a new level of operational efficiency, benefitting employers by having a constantly connected workforce (Allam, Flowerday, & Flowerday, 2014). However, to utilise many of the smartphone features, users are required to disclose their personal information such as names, addresses, financial and other sensitive details (Alsaleh, Alomar, & Alarifi, 2017). Therefore, while smartphones and their versatile functions enable users to have a truly wireless, and connected lifestyle, they also pose significant security and privacy threats (Torre, Sanchez, Koceva, & Adorni, 2018).

1.1 Smartphone security

Due to the degree of sensitive information stored on smartphone devices, the theft of or access to a smartphone could result in stolen identities, blackmail, extortion and the re-sell value of the hardware (Chen & Li, 2017; Ophoff & Robinson, 2014; Alsaleh et al., 2017; Clarke et al., 2016). There are also many ways that hackers can install malware onto a victim's device, gaining unauthorised access to sensitive information (Alsaleh et al., 2017). Alarmingly, McGill &Thompson (2017) found over 18 million mobile malware detections in 2016, an increase of 105% compared to the previous year. The same research found that smartphone vulnerabilities had experienced a growth of 32% in that same year. More recent research detected over 8.5 million malicious smartphone installation packages, 128,886 smartphone banking trojans and 261,214 ransomware trojans (Verkijika, 2018).

Given the obvious frequency and gravity of these threats, one might assume that users would exercise extreme caution when operating and securing their smartphones. However, research has found the opposite. Users are generally nonchalant in their attitudes and behaviours towards smartphones and information security (Clarke et al., 2016). Current research suggests that smartphone users are largely unaware of their susceptibility, and many users tend to ignore security mechanisms or feel that they are generally ineffective in preventing or reducing the dangers and threats when using smartphones (Kusyanti & Puspa, 2018; Mylonas, Kastania, & Gritzalis, 2013; Hewitt, Dolezel & McLeod, 2017). Previous studies have found that even people who have fallen victim to a mobile security related incident still fail to secure their smartphones with something as simple as a passcode or pin (Clarke et al., 2016).

Despite smartphone users playing a significant role in the security ecosystem, their part is often undervalued and the research into user behaviour is not as extensive as the research into the technology aspect of security models (Mylonas et al., 2013, Ophoff &

Robinson, 2014). It must be understood that, for the most part, humans are considered to be the weak link in this scenario as their actions directly influence the strength of their security and privacy (Winnefeld et al., 2015). Research has highlighted a disconnect between user desire for security, compared to the effort required to install and manage reliable security controls (Clarke, et al., 2016). Not only is this concerning for achieving good information systems security (ISS) in the general population, but it may be even more concerning for organisations whose employees have access to personal and sensitive client or organisational information who are often not adequately skilled to ensure good security settings on their smartphones (Allam et al., 2014).

1.2 Protection Motivation Theory

A growing body of literature has focussed on why people might act in a dissonant manner and chose not to protect themselves against threat or danger. This research is based on understanding attitudes, motivations, intentions and adoption of behaviours towards protecting one's information security. This literature has been dominated by the Protection Motivation Theory (PMT), which can explain the common disparity between what a user thinks or knows they should do and their actual behaviour (Rogers, 1975).

The model, first coined in 1975 by Rogers, has been applied to numerous studies to understand protective behaviour, predominately related to health (Milne, Sheeran, & Orbell, 2000). PMT consists of two cognitive processes, the *threat-appraisal* and the *coping-appraisal*, depicted in Figure 1. The threat-appraisal process considers the likelihood and impact of the risk, while the coping-appraisal process considers the effectiveness of the adaptive response and the individual's ability to perform this behaviour. (Rogers, 1983; Maddux & Rogers, 1983; Floyd et al., 2000; Milne et al., 2000; Verkijika, 2018). Each of the components within the model will be explained below.

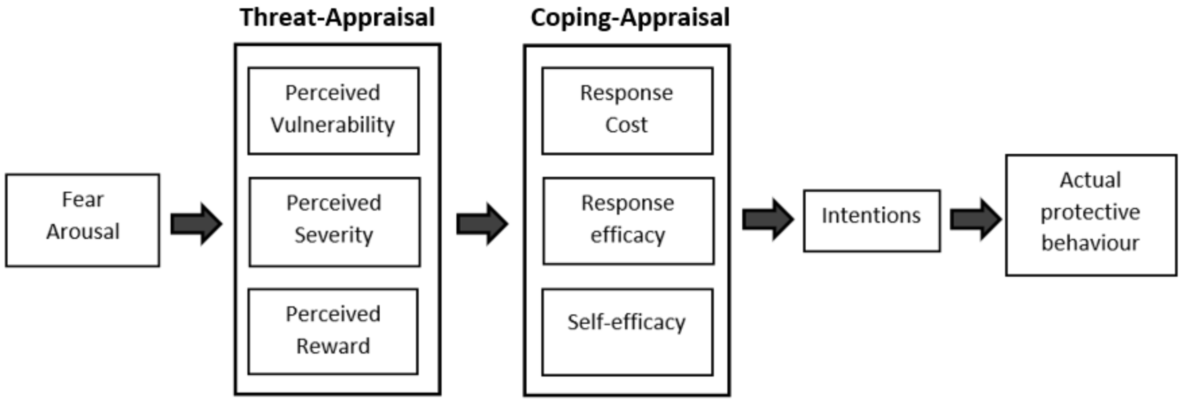


Figure 1. Diagram of Protection Motivation Theory

7. *Perceived severity* is the magnitude, or how serious the individual judges the threat to be (Milne et al., 2000; Vance et al., 2012). In other words, how detrimental the user perceives consequences of the threat to be (Verkijika, 2018). For example, Reeves, Parsons and Calic (2017) found that when asked about mobile computing/IoT, employees who felt more personally at risk (e.g., of reprimand, reduced productivity, personal data loss) were more likely to avoid behaviours that may lead to the risk event.

8. *Perceived vulnerability* is the extent to which an individual believes they are susceptible to a threat, or their perception of the probability of the threat actually occurring (Liang & Xue, 2010; Milne et al., 2000). With regards to smartphone security, this concerns a user's perception or belief around the likelihood of their device being compromised (Verkijika, 2018).

9. *Perceived reward* regards any benefit to the user, whether it be intrinsic or extrinsic, that motivates the user to continue or even increase the maladaptive response, disregarding the protective behaviour, such as downloading free pirated apps (Vance et al., 2012).

10. *Response efficacy* refers to an individual's belief that the coping response or protective behaviour is actually capable of reducing the threat (Milne et al., 2000). In terms of smartphone security, it is the extent to which an individual perceives that behaving securely effectively minimises the risk of a threat occurring (Verkijika, 2018).

11. *Response cost* refers to the perceived cost associated with implementing the protective behaviour (Vance et al., 2012). These can include money, time or effort exerted to perform the protective behaviour (Milne et al., 2000).

12. *Self -efficacy* is an individual's level of perceived skill or ability in performing the protective behaviour (Verkijika, 2018). This can be conceptualised as ability or autonomy. Ability refers to how capable or competent the individual feels, and autonomy refers to an individual's capacity to protect themselves against a security threat on their smartphone (Sommestad, Karlzén, & Hallberg, 2015a; Vance et al., 2012).

More often than not, these variables are assessed by measuring intentions to adopt through observing actual behaviour or self-reported behaviour (Tu, Yuan, & Archer, 2014).

1.3 Previous research: PMT and Information Security

As discussed previously, there is a substantial body of literature exploring PMT in a range of contexts, including how the different PMT factors are linked to information security behaviours (Blythe, Coventry & Little, 2015; Sommestad et al., 2015a). It has been applied to a range of common information security contexts (Tsai et al., 2016), populations (Dang-Pham & Pittayachawan, 2015; Verkijika, 2018), devices (Anderson & Agarwal, 2010), and settings (Herath & Rao, 2009b; Lee & Larsen, 2009; Siponen, Adam Mahmood, & Pahnila, 2014).

It is important to note that although the majority of previous research has focused on work or organisational contexts, there has been some disagreement that the conclusions drawn within this setting are applicable to the home context (Dang-Pham & Pittayachawan, 2015). It has been suggested within the literature, that applying PMT to an organisational context implies that fear is influencing behaviour, and that users perceive organisational risk at the same level as personal risk (Hovav & Putri, 2016). The relevance of the coping-appraisal variables within the organisational setting have also been questioned, due to behaviours being mandatory (Sommestad et al., 2015a; Verkijika, 2018). More recent criticisms are that home users may not have access to the same security training or support within the home context, that they rely on ill-informed information sourced from family and friends, that there is a greater requirement for self-reliance, and that they perceive their personal information as not important enough to be targeted (Anderson & Agarwal, 2010; McGill & Thompson, 2017). Although the PMT has been used to examine information security behaviours in both organisational and home contexts, as discussed in the next sections, to date the findings have been mixed, and no study has yet to compare smartphone security behaviour in work and home contexts.

1.3.1 PMT and Information security in organisational settings

A large portion of the research on PMT and information security has been in an organisational context, often investigating employee compliance towards security policies. Vance et al. (2012) found perceived severity to have a significant positive impact on employees' intention to comply with information security policies, as is supported by several studies investigating PMT and employee policy compliance (Herath & Rao, 2009b; Lee & Larsen, 2009; Siponen et al., 2014). While there is some evidence suggesting that perceived vulnerability might influence employee intentions to comply with security policies (Lee & Larsen, 2009; Siponen et al., 2014), there is also evidence that suggests it is not a significant predictor (Herath & Rao, 2009b; Ifinedo, 2011; Vance et al., 2012). Ifinedo (2012) found response efficacy to have the strongest effect on compliance, meaning employees were motivated to adhere to policies if they believed there were high expected returns by doing so, with support in the literature for this (Herath & Rao, 2009b; Lee & Larsen, 2009). Conversely, Ifinedo (2012) did not find response cost to have a significant relationship, suggesting this might be due to differing perspectives on costliness of a response. The component of perceived reward has been a variable of interest included within this population setting, however Vance (2012) was the only study to find a significant negative relationship, which is consistent with PMT. Most stable of these findings has been that self-efficacy is consistently shown to influence employee intentions to comply with security policies of their organisations (Herath & Rao, 2009b; Lee & Larsen, 2009; Siponen et al., 2014; Vance et al., 2012).

1.3.2 PMT and information security in personal settings

A change in research focus has seen some of the most recent PMT studies into information security investigating user motivations, intentions and behaviours within the home setting. The findings within this context are arguably more consistent. Perceived severity was found to have a significant positive relationship with security behaviours in a number of studies (Anderson & Agarwal, 2010; Liang & Xue, 2009; Crossler & Bélanger, 2014; Martens et al., 2019). Similarly, there is consistent evidence for perceived vulnerability having a significant effect on protective behaviours (Anderson & Agarwal, 2010; Liang & Xue, 2010; Martens et al., 2019; Thompson et al., 2017). Despite this, Hanus & Wu (2016) did not find the same support, suggesting that vulnerability infers that the user is aware that a threat exists, which is often not the case especially in the home setting. Similarly, response efficacy has good support within the home context (Anderson & Agarwal, 2010; Crossler & Bélanger, 2014; Hanus & Wu, 2016; Liang & Xue, 2010; Martens et al., 2019). There were a number of studies that excluded response cost as a variable of interest, as it is suggested security behaviours are not costly (Zhang & McDowell, 2009). Despite this, the studies that did consider response cost found support for its inclusion (Hanus & Wu, 2016; Liang & Xue, 2010; Thompson et al., 2017). Self-efficacy also had consistent support within the literature (Anderson & Agarwal, 2010; Crossler & Bélanger, 2014; Hanus & Wu, 2016; Liang & Xue, 2010; Thompson et al., 2017). Although Martens et al. (2019) did not find the same support, they argued that this might be due to level of digital skill, suggesting that the previous literature has used population samples that are often highly educated (i.e. university students). Perceived reward was excluded as a potential variable in all the aforementioned studies.

1.3.3 PMT and ISS behaviour on smartphones

As outlined initially, the emergence of smartphones within both organisational and home contexts has become increasingly apparent. PMT has more recently been utilised to examine why smartphone users may chose not to adopt protective behaviours. User relationship with a smartphone has looked at theft or loss (Tu et al., 2014), app permissions (Kusyanti & Puspa, 2018), general smartphone security (Verkijika, 2018), and comparisons between smartphone and PC behaviours (McGill & Thompson, 2017; Thompson et al., 2017). The findings across these contexts have been inconsistent. Perceived severity and perceived vulnerability have support within the literature (Thompson et al., 2017; Tu et al., 2015; Verkijika, 2018). This suggests that smartphone users will use protective behaviours if they feel vulnerable to threats and if the threat has severe consequences. Although not in line with the broader information security literature, there is a lack of evidence for response cost and efficacy within the mobile and smartphone context specifically (Thompson et al., 2017). This suggests that the effectiveness and the cost of smartphone protective behaviours may not influence protective behaviour (Verijjika, 2018). Finally, in line with other information security research, self-efficacy has the most support within the PMT smartphone literature

(Kusyanti & Puspa, 2018; Thompson et al., 2017; Tu et al., 2014; Verkijika, 2018). Interestingly, in a comparison study between users of both mobile devices and PC's, users had lower self-efficacy on their mobile phones compared to their PC's. They also believed that protective measures were less effective and more costly to perform on their mobile phones compared to PC's (McGill & Thompson, 2017). These findings suggest that due to the relative recency and rapid adoption of smartphone usage, users may lack awareness in how to appropriately and effectively protect their smartphones (McGill & Thompson, 2017). The importance of understanding and educating the home user has become increasingly apparent, as the translation of behaviours, and use of personal devices within the organisational context has potential dangers for organisational privacy and security. This confirms the need to educate users on the importance of knowledge, skill and confidence in effectively protecting their smartphones.

1.4 Additional Variables

The current evidence suggests that PMT constructs on average account for between 34 and 50 percent of the variance (Sommestad et al., 2015a; Thompson et al., 2017). Like within any research context, it is important not to limit exploration, or to only consider one particular model or theory. For this reason, it is important to note that multiple studies throughout the literature have considered and found significant evidence for a variety of additional variables. These include; subjective norms (Anderson & Agarwal, 2010; Herath & Rao, 2009b; Ifinedo, 2011; Martens et al., 2019; McGill & Thompson, 2017; Tsai et al., 2016), descriptive norms (Anderson & Agarwal, 2010; Herath & Rao, 2009b; Thompson et al., 2017), psychological ownership (Anderson & Agarwal, 2010; Thompson et al., 2017), social influence (Johnston & Warkentin, 2010; Lee & Larsen, 2009; Tu et al., 2014), habit strength (Kusyanti & Puspa, 2018; Tsai et al., 2016; Vance et al., 2012), and anticipated regret (Sommestad, Karlzén, & Hallberg, 2015b; Verkijika, 2018). Again, a majority of these factors have been identified as relevant within organisational and personal computer contexts, however little is known about their importance within the smartphone security setting (McGill & Thompson, 2017).

1.5 Study aims

Referring to the evidence outlined above, it is clear there is still research to be done in understanding smartphone user security behaviour. Most notably, there is a lack of understanding of smartphone specific security behaviours and a lack of understanding about the extent of behaviour transfer between organisational and home settings. It is interesting then to consider the comparison in behaviour of a smartphone user across the organisational and personal contexts. For example, it is unknown whether organisational policies and procedures taught and practiced within the workplace transfer to the use of a personal smartphone. Therefore, the aim of this study is to understand how people behave on smartphone devices across contexts, and whether context influences behaviour on smartphone devices.

Specifically, the research questions were as follows: 1) to what extent do participants use the same security behaviours on smartphones regardless of context? And 2) can PMT be used to explore this comparison?

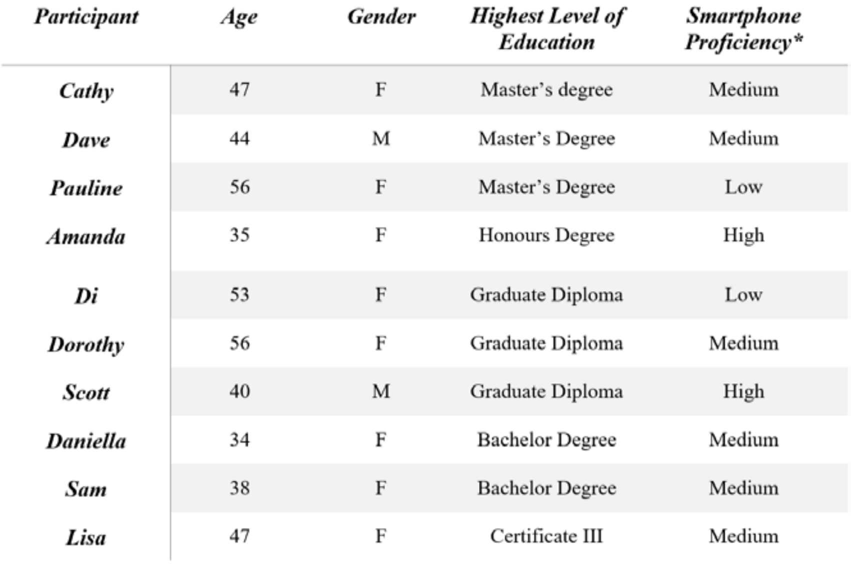
2. Method

Data collection involved qualitative interviews. Data was collected over a three-month period, May through August 2019. Ethics approval was granted in May 2019 by the Human Research Ethics Subcommittee of the University of Adelaide School of Psychology (H-2019-45).

2.1 Participants

A total of ten (8 females, 2 males) working Australians volunteered to participate in the interviews, ranging from 34 to 56 years of age (*M* = 45, *SD* = 7.81). Basic participant demographics are summarised in Table 1. Participants were given pseudonyms, and any identifying information discussed by participants was de-identified. Participants were all employed by and recruited from an Australian insurance company. All were employed full-time at the time of the interview, in various roles across the business, with a mix of internal and external customer facing roles. Participants were required to be over the age of 18, currently employed by the selected Australian insurance company, had a smartphone device supplied to them by the organisation to assist in their duties at work, and also a personal phone owned by the individual for use outside of work.

Table 1. *Participant Demographics*



Participant	*Age*	*Gender*	*Highest Level of Education*	*Smartphone Proficiency**
Cathy	47	F	Master's degree	Medium
Dave	44	M	Master's Degree	Medium
Pauline	56	F	Master's Degree	Low
Amanda	35	F	Honours Degree	High
Di	53	F	Graduate Diploma	Low
Dorothy	56	F	Graduate Diploma	Medium
Scott	40	M	Graduate Diploma	High
Daniella	34	F	Bachelor Degree	Medium
Sam	38	F	Bachelor Degree	Medium
Lisa	47	F	Certificate III	Medium

**Smartphone proficiency is self-reported level of skill and experience*

2.2 Procedure

Participants were recruited internally through the organisation. Advertisements were made on the organisation's intranet page, with reminders through the regular intranet updates email chain. This recruitment strategy meant that no direct recruitment approaches were made, therefore there was no coercion to participate. The advertisement directed eligible participants to contact the researcher via email or telephone if they were interested in being interviewed. Once the participant had made contact with the researcher, they were sent a participant information sheet (Appendix B) and a one-on-one interview time was arranged. Written informed consent (Appendix C) occurred at the beginning of each interview. Interviews were conducted in a secluded location within the organisation, with approval of the participant.

Interviews were semi-structured, with open-ended questions to avoid biased answers (Potter & Hepburn, 2005). Loosely based on questions from Dang-Pham and Pittayachawan (2015), Thompson et al. (2017) and Verijika (2018), the interview questions referred to how dual smartphone owners used both devices in daily activities, the differences and similarities in use and in regard to protective behaviour (questions attached in Appendix D). All interviews were audio recorded and transcribed verbatim by the researcher, using the orthographic method advised by Braun and Clarke (2006).

Data saturation, as outlined by Guest, Bunce and Johnson (2006), was reached between the eighth and ninth interviews. However, the additional interview was conducted to ensure that saturation had occurred. Interviews lasted between 16 and 34 minutes (*M* = 25.8, *SD* = 5.82). A summary of the preliminary themes was emailed to the participants for review and reflection, following Tracy' (2010) recommendation to conduct member checking. One participant responded to say they were satisfied with the suggested results.

2.3 Analysis

Thematic analysis was used to analyse the data, combining both inductive and deductive approaches. This meant analysis was both guided by the components of PMT, as defined by Rogers (1983), but was also flexible and explorative, identifying themes which did not neatly fit within the theory. This mixed approach enabled a robust and rigorous analysis of the comparison between protective smartphone behaviour (Fereday & Muir-Cochrane, 2006). Throughout the research process, the data was analysed sequentially so that each interview conducted would influence the next. After each interview, potential themes were noted. This provided the researcher with a clearer idea of which domains seemed to be relevant to participants throughout the research process allowing for constant comparison between interviews (Tracy, 2010). This also helped to identify when data saturation had occurred (Braun & Clarke, 2013).

Analysis followed Braun and Clarke’s (2006; 2013) six-step guide to ensure quality and rigor of research. The first phase, familiarisation involved the researcher transcribing the interviews while noting preliminary themes. The next few phases involved generating initial codes, searching for themes and reviewing themes. This part of the analysis process was deductive, with the PMT used to guide the analysis. These themes were then reviewed against the data set as a whole. Data was then analysed inductively in order to identify themes across the data set which did not fit within PMT. At this stage, cross-checking of the themes with other researchers was employed, as encouraged by Pope and Mays (2006) to minimise researcher bias, ensuring research rigor and trustworthiness. Deductive analysis lead to the themes within PMT and inductive analysis identified the additional theme ‘social influence’, which were then named. The final stage of analysis involved the researcher selecting extracts from the data set that would provide vivid examples of the themes within the model of PMT, and the additional theme relating to social influence (Braun & Clarke, 2006; 2013).

3. Results

The main overarching theme identified from the data was that people behave more safely on their work smartphones compared to on their personal smartphones. Using PMT to explore this comparison, it seems that it is not as simple as just better behaviour. The primary finding indicates that participants did not ultimately know why they performed protective behaviours on their work smartphones, or how the behaviours benefitted their safety and security rather than their reputation within the workplace. It seems people were behaving better due to the organisational controls and monitoring that was in place to protect them, which do not exist within a personal setting.

To conceptualise this view, data was analysed according to the six components of the PMT extended model (Rogers, 1975, 1983; Maddux & Rogers, 1983). The higher sense of vulnerability, the presence of perceived reward and response cost and the higher need for self-efficacy within the personal setting were major themes. Inductive analysis provided the additional theme relevant to the construct ‘social influence’, which considers influences towards smartphone security behaviour external to the PMT model. The themes within this comparison will be explored in more detail below.

In this study, risky or maladaptive smartphone security behaviour included downloading third-party, unofficial or pirated apps, choosing not to read privacy statements, accepting all permissions, using public unsecure Wi-Fi, not using a passcode to lock the device, not backing up the devices data, inappropriate use of social media (e.g. such as using unsafe surveys without reading privacy agreements). This also included storing sensitive information on the smartphone without the correct precautions in place. Most significantly, participants unanimously reported behaving far safer on their work smartphones, in terms of refraining from almost all of the listed behaviours when compared to their personal smartphones. Applying the main factors within the PMT, the specific themes are explored below in greater detail.

3.1 Perceived Severity

When comparing attitudes, intentions and behaviours towards protecting smartphones, participants seemed to perceive a similar severity for their work and personal devices. Perception of severity was generally based on purpose of use, and nature of the information accessed or stored on the smartphone. Cathy expressed this in relation to her work smartphone:

> *I guess the reason why I don't put my mind to the work phone that often is because I don't access as many different apps and do as much personal activity with personal information and details through the work phone.*

Later in the interview, Cathy indicated that her personal smartphone would have more severe consequences due to the personal nature of information stored on the smartphone:

> *I'd say personal, yeah, because you've got a whole lot more stuff on there that impacts you and your family and that sort of thing.*

Aspects such as job role also seemed to influence perceptions of severity, as suggested by Dorothy:

> *…for me personally, I'd feel really horrible about client information being exposed because as a professional, that's part of our ethics, so that would make me really uncomfortable professionally… I'd feel terrible…the ramifications for client stuff is bigger than, for the client, than the ramifications, so the money, for me.*

This implies that the extent to which an individual feels personally responsible for the use of and information accessed on the device determines how severe they expect the threat to be. This was consistent amongst participants on both personal and work smartphones.

3.2 Perceived Vulnerability

A feeling of vulnerability, on the other hand, was perceived more frequently in relation to participants' personal compared to their work smartphones. When discussing the use of the work smartphone, participants indicated not feeling vulnerable because of their reliance and sense of trust in the technical support they received through the organisation, as described by Pauline:

> *I'm fairly IT not very literate, and so I am assuming that, well we get software updates, regularly, and that if I just keep those updates updated, that whatever security is needed behind this phone happens. So I'm just assuming that it's all secure, anti-virus, everything is done to this phone because it's a work phone, but I have no idea what it is, or what they do, so I'm just assuming IT keep it up to date.*

This was a feeling shared amongst most of the participants who would often describe the IT support as extremely skilled, capable and able to '*shutdown*' (Cathy, Dorothy, Scott, Di) or '*wipe*' (Amanda, Cathy, Dorothy, Di) devices and '*know exactly what to do'* (Dorothy, Daniella, Sam). As described by Pauline above, participants indicated that this perception of company security practices reduces the need for an individual's own capacity in protecting themselves.

3.3 Self-efficacy

Self-efficacy is conceptualised in terms of ability and autonomy (Sommestad, Karlzén, & Hallberg, 2015a; Vance et al., 2012). Ability is described as knowing how to do the behaviour, and autonomy is taking ownership and responsibility of that behaviour (as exemplified by Pauline, above). In the quote, below, Sam discussed her vulnerability and her lack of knowledge (i.e., ability) to protect her personal device:

> *Probably the work phone, because I can go to Peter, and I'll go Peter, I've lost the phone, and I'm sure he will work his magic around, I don't know, resolving all of that. I don't know, getting rid of all of that information on there, somehow. Whereas my personal phone, oh gosh, what could I do, I don't know, I don't have a lot of control over mine do I? No… I think, my work phone, IT department will sort it out for me, whereas my own phone, I have to do it myself and I wouldn't even know where to begin.*

Sam indicated feeling supported in a solution provided by the organisation's IT department. Therefore, there is no need for her to have any learnt problem-solving or coping strategies in place, and this is possibly why she didn't feel capable in protecting her personal smartphone. This suggests that participants do not have greater skill or ability to protect their work smartphones, but rather there is support available and there are stricter controls on use of smartphones. Participants often did not engage in risky behaviour on their work smartphones, as there was often no benefit in doing so. This included not connecting to unsecure Wi-Fi due to supplied data plans, also not having a need or want to engage with social media, and being advised against downloading additional apps (and therefore reading privacy statements). It wasn't expected by the organisation that employees would need to engage in this behaviour to help them do their job better, and it certainly wasn't something that participants wanted to have or do on their work smartphones, as expressed by Dave:

> *…because I use it so rarely, because I don't do any other app or personal activity on it, I believe that I would always be able to stand on my own two feet and*

> *say I'm not doing anything careless with it, because of my, as I said, minimalist approach with this [work phone].*

As Dave explained above, he is careful with his work smartphone use. Similarly, the majority of participants acknowledged they purposefully and consciously made the decision to behave safely on their work smartphone, as identified by Lisa:

> *…we've got really good things in place here. But because I'm only using it for work related things, I don't think I'm exposing the phone or anything that's on the phone in any way.*

There are clear differences between smartphones regarding what is expected or required from a user. Protective behaviours such as using a passcode and refraining from downloading unregistered apps were often mandatory on the work smartphone. However, some behaviours such as backing up the device data or downloading and updating anti-viral software were not the responsibility of the end-user and these behaviours were performed by the organisation, as Scott explained:

> *the work phone was nice because it happened for me type thing, so I didn't really have to do anything, the updates came through and everything was forced and messages would come out from the service desk to say 'run this update' and things like that, so it was a bit of less involvement, it was sort of done for you, so you know you could just 'it's broken fix it, send me a new one' whatever it is.*

However, this was not the case for personal devices, which required the user to take personal responsibility for all behaviours. This may have contributed to participants' inability to enact such protective behaviours on their personal smartphones.

3.4 Perceived Reward and Response Cost

Participants engaged in risky behaviour on their personal devices due to several reasons, but most specifically, the response cost associated with protective behaviours and the perceived reward associated with maladaptive responses. Often participants felt protective behaviours were '*too costly*' (Cathy, Sam), '*time-consuming'* (Daniella, Sam), '*inconvenient*' (Scott, Cathy, Dave) and '*boring*' (Lisa, Amanda, Daniella, Sam). As described by Lisa when justifying not reading privacy statements:

> *[Interviewer – what are you gaining by not reading it?] time, haha, time yeah… and a lot of it's, it's information overload, as well, like it's small print, you know and is this going to tell me anything that I'm not already assuming that you're going to be doing?*

Lisa identified the behaviour as not only costly, but also ineffective. Participants would often weigh up cost and gains of maladaptive behaviour, as Dave explained in regards to connecting to unsecure Wi-Fi:

> *...I know and accept the fact that nothing is for free and that absolutely, and it's the same for apps as well, nothing is ever for free and they are always collecting data and numbers and activity, from me. So I know that, I know that they are doing that, but that's the price I'm willing to pay because it means I can watch a movie on my phone while I'm waiting for a flight.*

Further, when discussing reward and cost, this was often in regard to access. Participants would use phrases such as '*tick the box*' (Dave, Daniella, Pauline) '*gain accessibility*' (Di, Scott) *'get access'* (Cathy), '*click the button*' (Lisa) '*it won't let me unless I do*' (Sam, Dorothy). It should be acknowledged, then, that participants commonly expressed being aware if they were doing the wrong thing, as explained by Daniella:

> *...probably another reason why I don't download things on my work phone as well because I'm not great at reading terms and conditions and I wouldn't want to put something on there that I haven't read.*

Therefore, participants seemed to be aware of maladaptive behaviours and restricted these on their work smartphones. However, that was not the case on their personal smartphones. For example, Daniella admitted to downloading numerous apps on her personal smartphone without reading the conditions or privacy statements:

> *…my personal phone I use all my apps, all my games… I probably should have read them, I kind of probably just accepted them, um as I do with most things.*

This might suggest the reason that participants lacked good behaviours on their personal devices was due to not having a complete awareness of the importance and effectiveness of behaviours in both the organisational and personal contexts. For example, participants were aware that connecting to unsecure Wi-Fi was not allowed on work phones for security reasons, but may not have been aware of the extent that this behaviour could also protect their personal smartphone devices.

3.5 Response Efficacy

Despite displaying generally poor security behaviours on personal smartphones, when participants did utilise a protective behaviour, they acknowledged that the behaviour was effective, as discussed by Lisa when asked why she used a code to lock her personal phone:

> *...it's just a good safeguard in case someone, you know I lose it, it's locked, so somebody can't, hopefully, access it.*

This was consistent amongst participants with regard to a variety of different behaviours (Amanda, Dorothy, Dave, Scott, Daniella). This suggests that to some extent training and educating have been effective, and may have transferred to personal contexts.

3.6 Social Influence

A concept that was beyond the scope of PMT was the role of social influence, subjective norm and descriptive norm. Each of these concepts have been used throughout previous literature as additional variables to supplement the explanatory power of a PMT model (Johnston & Warkentin, 2010; Lee & Larsen, 2009; Tu et al., 2014). These variables suggest that there is some form of social influence on behaviour. This was true in this study for both personal and work smartphones. When discussing the social impact on the use of their work smartphones participants used phrases such as *'being caught', 'being monitored', 'corporate policy', 'embarrassing', 'be careful', 'don't contradict the values', 'someone could potentially see it', 'security conscious'* and *'strict'* (Cathy, Scott, Daniella, Amanda, Dave, Pauline, Di, Sam). This suggests that participants were performing safely because it was expected from them and they wanted to do the right thing by the organisation, not necessarily because they were intrinsically motivated or because they thought that security is important, as described by Daniella:

> *I think with the work phone as well, is I guess it's not technically my property so at any time it can be accessed by IT so you know it's kind of like 'oh I'm just going to restrict the information on there', Number one, I don't ever want to contradict policy, and it's probably just easier, keeps it clean and keeps them very differentiated.*

The idea of social influence can also be used to describe participants' use of personal smartphones, and the justification/explanation that engaging in risky behaviour is ok because ‘*everybody does it’* (Scott, Dave, Daniella, Lisa, Di, Cathy, Dorothy, Sam), as expressed by Amanda:

> *I don’t know why I’ve accepted it, I think because I see everyone else using it and so it’s like, oh well, they think it’s fine, I’ll think it’s fine too…yeah, going by kind of herd mentality, and herd immunity and figuring if there are now hundreds of people doing it, then the chances of me being mucked over is lower because there’s 99 other people to pick.*

4. Discussion

A large body of literature explored aspects relating to PMT and information security behaviour. However, despite the rapid adoption of smartphones, there is limited literature exploring user security behaviour on smartphones, especially those with two devices. Therefore, the aim of this study was to explore and compare user security behaviour on smartphones in both the personal and workplace contexts. The following sections will discuss the study’s findings, applications, limitations and future directions.

4.1 Findings and Implications

A key finding that emerged from the data was that people behave safer on their work devices compared to their personal devices. This was often despite feeling far more vulnerable and incapable of protecting themselves on their personal smartphones. For example, all participants protected their work smartphones with a code, but this was not always the case on personal smartphones. Similarly, all participants refrained from downloading pirated or unofficial apps on their work devices, whereas many had these installed on their personal devices.

Using PMT to explore and thematically analyse this comparison, several themes were identified. The strongest themes were; a higher sense of vulnerability on personal devices; a higher need for self-efficacy on personal devices; the occurrence of perceived reward and response cost on personal devices. There were no differences in device use and perception regarding perceived severity and response efficacy. Inductive analysis identified the role of social influence on both personal and work smartphones.

Participants generally felt that their personal smartphones were far more vulnerable or more susceptible to a security threat. This finding is not surprising, with little support for perceived vulnerability within the PMT organisational literature (Herath & Rao, 2009b; Ifinedo, 2011; Vance et al., 2012). Participants felt less vulnerable on their work smartphones for several reasons. Firstly, participants often did very little activity on their work smartphones, besides the basic telephoning and email functions. It was also acknowledged participants did not engage in risky behaviour on their smartphones due to lack of need and policy. This was also influenced by the idea that engaging in risky behaviour was linked to punishment, rather than good protective behaviours being linked to benefits for the individual. Finally, the organisation took care of a majority of the security behaviours, leaving the participant feeling safe in the hands of IT. Participants did not have this safety-net on their personal phones, and frequently admitted to engaging in risky behaviour such as not reading privacy statements, and connecting to unsecure Wi-Fi.

In terms of self-efficacy, there was a higher need for this component in the personal smartphone context. This is interesting as previous literature identified a high need for self-efficacy within the organisational setting (Herath & Rao, 2009b; Lee & Larsen, 2009; Siponen et al., 2014; Vance et al., 2012). In this study, participants often considered themselves to be solely responsible for the protection and security of their personal smartphones. Participants often acknowledged that the work smartphones had systems of support and required less effort to maintain and look after. This meant participants did not have to practice all protective behaviours on their work smartphones, and therefore did not perform them on their personal smartphones either. It did not seem as though participants knew exactly how the organisation protected their smartphones; therefore, this limited their ability and autonomy to perform these behaviours themselves. From a practical perspective, it is suggested that if participants understood how the work smartphone was protected and why, this might increase protective behaviours in the personal context.

Participants often discussed perceived reward and response cost within the same nature. Despite being defined as separate components and within separate appraisal processes, these have often been operationalised as a single construct (Verijika, 2018; Thompson et al., 2017; Sommestad et al. 2015a). When using their personal smartphone, participants often perceived some reward as a result of performing risky behaviours such as connecting to unsecure Wi-Fi at airports. Similarly, the cost of performing protective behaviours was often a reason for not performing them on personal smartphone devices, such as backing up data or reading privacy statements, which were considered too time consuming and inconvenient. In sum, both these components combined led to participants justifying their poor security behaviour on personal smartphones. As has been suggested within previous literature, protective behaviours are often mandatory within a workplace, and therefore participants would not consider costs. Similarly, rewards may not have existed within this context, as performing risky behaviours such as downloading unregistered apps would have contradicted policy and ultimately could have led to dismissal. Rewards would not have out-weighed consequences within the work context.

The use of deductive analysis provided the final theme social influence. This concept has been identified within previous literature. This concept suggests that individual behaviour is unavoidably influenced by surrounding people (Tu et al., 2014). Inevitably, social networks play a major role in adoption of protective behaviour (Liang & Xue, 2009). Social influence can encourage compliance due to the need for getting approval, acceptance or the fear of punishment (Liang & Xue, 2009). This was certainly found within our data, in terms of performing protective behaviours on the work smartphone. However, social influence can also involve aligning one’s own values with that of the broader group, the consequence of which resulted in performing risky behaviours on personal smartphones that may have been recognised as socially desirable (Lee & Larsen, 2008, Liang & Xue, 2009).

4.1.1 Applied Implications

The themes identified within the data offer several applied implications, particularly to the broader aim of establishing good security behaviours and awareness in the general population. Firstly, it was not explicitly discussed by participants, but must be acknowledged that the ultimate consequence of performing risky or maladaptive behaviours on their work smartphones was dismissal from the workplace. The organisation had policies in place in regard to internet usage, smartphone usage and acceptable behaviour in the workplace. As mentioned throughout the analysis, and particularly in relation to social influence – participants may have behaved safely from fear of punishment or wanting to do the right thing (D’Arcy, Hovav & Galletta, 2009; Herath & Rao, 2009a; Myyry et al., 2009). From the perspective of the organisation, this might be considered as a successful outcome. However, this could mean that instead of using their work smartphones to do anything ‘riskier’, participants might perform this on their personal smartphones, and then connect this to the workplace via email or other means. This could inadvertently expose the organisation to risk they cannot control or avoid. Further, the lack of good security behaviour performed on personal smartphones could potentially result in malicious intent such as hacking or extortion. If a hacker was successful, they could potentially have access to the organisation if the individual had workplace information stored on their personal smartphone.

With these implications in mind, it must also be acknowledged that the participants within this study had participated in several technology and cyber-security trainings within their workplace. The results of this study would suggest that this training had been successful, as participants behaved safely on their work smartphones, complying with policy. It is interesting that this education and training was not displayed on personal smartphones. Traditionally PMT research within the organisational context has investigated and made suggestions for improving employee policy compliance (Ifinedo 2011, Vance et al., 2012; Siponen et al., 2014; Lee & Larsen, 2008; Herath & Rao, 2009b). This is not the findings of the current research, with employees behaving extremely compliantly. However, the lack of good behaviour performed regardless of context suggests that the training was not as effective as it could be. This might indicate that participants did not ultimately know why they performed particular behaviours, or how the behaviours benefitted their safety and security rather than their reputation within the workplace. The transfer of behaviour may not be occurring as the behaviours are not intrinsically motivated. For example, if a workplace brought in a new policy that everyone must walk 20,000 steps a day, employees would do this because it is a requirement and they want to do the right thing. However, if no other information is communicated about the benefits of walking 20,000 steps to overall health, as soon as employees left the workplace, it is unlikely they would continue this behaviour as it has no relevance to them outside of the workplace environment. This is the same within the smartphone and information security behaviour context.

4.2 Limitations and Future Directions

While this study has provided a useful insight into the relationship between organisational and personal smartphone security behaviour, it is not without its limitations. Firstly, the participant sample was limited to a single workplace, which may be subject to bias. Future research should attempt to triangulate results, possibly with other workplaces, and those who specialise in smartphone security and training (Tracey, 2010). In addition, the interviews were based on self-report and in aid of convenience, interviews were conducted within the workplace. It is possible then, despite being made aware of confidentiality, that participants avoided admitting some poor security behaviours performed on work-supplied smartphones. Finally, selection bias may have also influenced participation in the study. Specifically attracting those who were confident in their work smartphone usage, discouraging participation from those who behaved poorly.

Considering the results of this study, it is suggested that future research focus on tackling the education of personal smartphone security. PMT guided analysis enabled a direct comparison and exploration into which factors might influence adaptive and maladaptive security behaviour performed on both personal and work smartphones. It is however suggested that future research consider not only PMT, but variables beyond the theory such as the role of social influence which was evident within our data. Ultimately the goal of future research should be in improving current training and education so that skills and protective behaviours are transferred across contexts, as users understand the benefit to not only their organisation but to their individual safety. Future organisational education programs should emphasise the importance of security and secure behaviours within the home and personal context. However, it is important here to consider cyber fatigue and not overloading people with lots of different information on cyber-security (Reeves, 2019). This should be essential in the development of successful education programs.

4.3 Conclusion

This study examined the relationship between user behaviour on personal smartphones and work supplied smartphones. Results indicated that participants behaved safer on their work smartphones devices compared to their personal smartphone devices. It was found that perceived vulnerability, perceived reward, response cost, self-efficacy and social influence largely contributed to a lack of protective behaviour displayed on personal smartphones. These findings have important theoretical and applied implications.

Theoretically, while PMT was able to provide insight into the relationship, additional variables will aid this investigation. From an applied perspective, fear of penalty was linked to many of the themes, therefore it is suggested that education programs within organisations focus upon the benefits of protective behaviours to employees in both organisational and home contexts.

5. References

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42*(C), 56-65. doi:10.1016/j.cose.2014.01.005

Alsaleh, M., Alomar, N., & Alarifi, A. (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., & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643. doi:10.2307/25750694

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. doi:10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2013). *Successful Qualitative Research: A Practical Guide for Beginners.* London, England: SAGE Publications Ltd.

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. *Symposium on Usable Privacy and Security, 1*, 103-122

Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behaviour: A technology threat avoidance perspective. *Information and Computer Security*, *25*(3), 330-344. doi:10.1108/ICS-04-2016-0027

Clarke, N., Symes, J., Saevanee, H., & Furnell, S. (2016) Awareness of Mobile Device Security: A survey of User's Attitudes. *International Journal of Mobile Computing and Multimedia Communications, 7*(1), 15-31. doi: 10.4018/IJMCMC.2016010102

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, *45*(4), 51-71. doi:10.1145/2691517.2691521

Dang-Pham, D., & Pittayachawan, S. (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

D'arcy, J., Hovav, A. & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20* (1), 79-98.

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security, 24*(1), 116-134. doi:10.1108/ICS-04-2015-0018

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods, 5,* 80-92.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta- Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

Guest, G., Bunce, A., Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59-82. doi: 10.1177/1525822X05279903

Hanus, B., & Wu, Y. a. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2-16. doi:10.1080/10580530.2015.1117842

Haris, M., Haddadi, H., & Hui, P. (2014). Privacy Leakage in Mobile Computing: Tools, Methods, and Characteristics, 1-16.

Herath, T. & Rao, H.R. (2009a). Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-112. doi:10.1057/ejis.2009.6

Hewitt, B., Dolezel, D., & McLeod, A. (2017). Mobile Device Security: Perspectives of Future Healthcare Workers. *Perspectives in Health Information Management, 14,* 1-8.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, 35-49. doi:10.1016/j.pmcj.2016.06.007

Ifinedo, P. (2011). 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

Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34*(3), 549-566. doi:10.2307/25750691

Kusyanti, A., & Puspa, H. (2018). An Empirical Study of App Permissions: A User Protection Motivation Behaviour. *International Journal of Advanced Computer Science and Applications, 9*(11), 106-111. doi:10.14569/IJACSA.2018.091116

Leavitt, N. (2011). Mobile Security: Finally a Serious Problem? *Computer Society, 44*(6), 11-14. doi:10.1109/MC.2011.184

Lee, D., Larose, R., & Rifon, N. (2008). Keeping Our Network Safe: A Model of Online Protection Behaviour. *Behaviour & Information Technology, 27*(5), 445-454. doi:10.1080/01449290600879344

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187. doi:10.1057/ejis.2009.11

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly, 33*(1), 71-90. doi:10.2307/20650279

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *J. Assoc. Inf. Syst., 11*(7), 394-413.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. doi:10.1016/0022-1031(83)90023-9

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior, 92*, 139-150. doi:10.1016/j.chb.2018.11.002

McGill, T., & Thompson, N. (2017). Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology, 36*(11), 1111-1124. doi:10.1080/0144929x.2017.1352028 y1 - 2017

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology, 30*(1), 106-143. doi:10.1111/j.1559-1816.2000.tb02308.x

Mylonas, A., Gritzalis, D., Tsoumas, B., & Apostolopoulos, T. (2013). A qualitative metrics vector for the awareness of smartphone security users. *LNCS, 8058*, 173-184.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Comput. Secur., 34*(C), 47-66. doi:10.1016/j.cose.2012.11.004

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(2), 126-139.

Ophoff, J., & Robinson, M. (2014). Exploring end-user smartphone security awareness within a South African context. *IEEE, 978*(1), 1-7.

Pope, C., & Mays, N. (2006). *Qualitative Methods in health research*. Qualitative Research in health care (3rd ed.). Carlton, Victoria: Blackwell Publishing Ltd.

Potter, J., & Hepburn, A. (2005). Qualitative interviews in psychology: Problems and possibilities. *Qualitative Research in Psychology, 2*, 281-307. doi:10.1191/1478088705qp045oa

Reeves, A. (2019) *A model of Cyber Fatigue: Are you tired of cybersecurity?* Presented at Cyber Summer School, Adelaide, 21 March 2019.

Reeves, A., Parsons, K., & Calic, D. (2017). *Securing mobile devices: Evaluating the relationship between risk perception, organisational commitment and information security awareness.* Paper presented at the International Symposium on Human Aspects of Information Security & Assurance (HAISA), Adelaide, Australia.145-155, Editors: Steven Furnell, Nathan Clarke

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803

Rogers, R. W. (1983). *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, NY: Guilford Press; p. 153–75.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (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

Sommestad, T., Karlzén, H., & Hallberg, J. (2015a). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy, 9*(1), 26-46. doi:10.4018/IJISP.2015010102

Sommestad, T., Karlzén, H., & Hallberg, J. (2015b). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security, 23*(2), 200-217. doi:10.1108/ICS-04-2014-0025

Statista. (2016, 07/06/2016). Smartphone users worldwide 2014-2020. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70,* 376-391. doi:10.1016/j.cose.2017.07.003

Torre, I., Sanchez, O. R., Koceva, F., & Adorni, G. (2018). Supporting users to take informed decisions on privacy settings of personal devices. *Personal and Ubiquitous Computing, 22*(2), 345-364. doi:10.1007/s00779-017-1068-3

Tracy, S. J. (2010). Qualitative quality: Eight "big-tent" criteria for excellent qualitative research. *Qualitative Inquiry, 16,* 837-851. doi: 10.1177/1077800410383121

Tsai, H.-Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59,* 138-150. doi:10.1016/j.cose.2016.02.009

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management, 52*(4), 506. doi:10.1016/j.im.2015.03.002

Tu, Z., Yuan, Y., & Archer, N. (2014). Understanding user behaviour in coping with security threats of mobile device loss and theft. *Int. J. of Mobile Communications, 12*(6). doi:10.1504/IJMC.2014.064915

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198. doi:10.1016/j.im.2012.04.002

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security, 77,* 860-870. doi:10.1016/j.cose.2018.03.008

Wang, D., Xiang, Z., & Fesenmaier, D. R. (2014). Adapting to the mobile world: A model of smartphone use. *Annals of Tourism Research, 48,* 11-26. doi:10.1016/j.annals.2014.04.008

Winnefeld, S. J. A., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity’s human factor: Lessons from the pentagon. Harvard Business Review, 2015:86-95.

Zhang, L., & McDowell, W. C. (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. *Journal of Internet Commerce*, *8*(3-4), 180-197. doi:10.1080/15332860903467508

Appendices

Appendix A: Journal Guidelines for Submission

Computers in Human Behaviour

ELSEVIER

COMPUTERS IN HUMAN BEHAVIOR

AUTHOR INFORMATION PACK

DESCRIPTION

Computers in Human Behavior is a scholarly journal dedicated to examining the use of computers from a psychological perspective. Original theoretical works, research reports, literature reviews, software reviews, book reviews and announcements are published. The journal addresses both the use of computers in psychology, psychiatry and related disciplines as well as the psychological impact of computer use on individuals, groups and society. The former category includes articles exploring the use of computers for professional practice, training, research and theory development. The latter category includes articles dealing with the psychological effects of computers on phenomena such as human development, learning, cognition, personality, and social interactions. The journal addresses human interactions with computers, not computers per se. The computer is discussed only as a medium through which human behaviors are shaped and expressed. The primary message of most articles involves information about human behavior. Therefore, professionals with an interest in the psychological aspects of computer use, but with limited knowledge of computers, will find this journal of interest.

Benefits to authors

We also provide many author benefits, such as free PDFs, a liberal copyright policy, special discounts on Elsevier publications and much more. Please click here for more information on our author services. Please see our Guide for Authors for information on article submission. If you require any further information or help, please visit our Support Center

AUDIENCE

Psychologists, Cognitive Scientists, Educational Psychologists.

IMPACT FACTOR

2018: 4.306 © Clarivate Analytics Journal Citation Reports 2019

ABSTRACTING AND INDEXING

Psychology Abstracts

Current Contents - Social & Behavioral Sciences

PsycINFO

PsycLIT

Current Contents

Social Sciences Citation Index

Current Index to Journals in Education
International Bibliography of Periodical Literature
International Bibliography Book Reviews
Ergonomics Abstracts
Software Reviews on File
Computer Publishers & Publications
Engineering Index
COMPENDEX
Engineering Meetings
World Patent Information
Sociological Abstracts
Bioengineering Abstracts
Cambridge Scientific Abstracts
Embase
IBZ and IBR
Information Science Abstracts
Library and Information Science Abstracts
SSSA/CISA/ECA/ISMEC
Scopus
MathEduc

Scientific Board

GUIDE FOR AUTHORS

Your Paper Your Way

We now differentiate between the requirements for new and revised submissions. You may choose to submit your manuscript as a single Word or PDF file to be used in the refereeing process. Only when your paper is at the revision stage, will you be requested to put your paper in to a 'correct format' for acceptance and provide the items required for the publication of your article. To find out more, please visit the Preparation section below.

Submission checklist

You can use this list to carry out a final check of your submission before you send it to the journal for review. Please check the relevant section in this Guide for Authors for more details.

Ensure that the following items are present:

One author has been designated as the corresponding author with contact details:

1. E-mail address
2. Full postal address

All necessary files have been uploaded:

Manuscript:

1. Include keywords
2. All figures (include relevant captions)
3. All tables (including titles, description, footnotes)
4. Ensure all figure and table citations in the text match the files provided
5. Indicate clearly if color should be used for any figures in print

Graphical Abstracts / Highlights files (where applicable)

Supplemental files (where applicable)

Further considerations

6. Manuscript has been 'spell checked' and 'grammar checked'
7. All references mentioned in the Reference List are cited in the text, and vice versa
8. Permission has been obtained for use of copyrighted material from other sources (including the Internet)
9. A competing interests statement is provided, even if the authors have no competing interests to declare
10. Journal policies detailed in this guide have been reviewed
11. Referee suggestions and contact details provided, based on journal requirements

For further information, visit our Support Center.

SUBMISSIONS: BEFORE YOU BEGIN

Ethics in publishing

Please see our information pages on Ethics in publishing and Ethical guidelines for journal publication.

Studies in humans and animals

If the work involves the use of human subjects, the author should ensure that the work described has been carried out in accordance with The Code of Ethics of the World Medical Association (Declaration of Helsinki) for experiments involving humans. The manuscript should be in line with the Recommendations for the Conduct, Reporting, Editing and Publication of Scholarly Work in Medical Journals and aim for the inclusion of representative human populations (sex, age and ethnicity) as per those recommendations. The terms sex and gender should be used correctly.

Authors should include a statement in the manuscript that informed consent was obtained for experimentation with human subjects. The privacy rights of human subjects must always be observed.

All animal experiments should comply with the ARRIVE guidelines and should be carried out in accordance with the U.K. Animals (Scientific Procedures) Act, 1986 and associated guidelines, EU Directive 2010/63/EU for animal experiments, or the National Institutes of Health guide for the care and use of Laboratory animals (NIH Publications No. 8023, revised 1978) and the authors should clearly indicate in the manuscript that such guidelines have been followed. The sex of animals must be indicated, and where appropriate, the influence (or association) of sex on the results of the study.

Declaration of interest

All authors must disclose any financial and personal relationships with other people or organizations that could inappropriately influence (bias) their work. Examples of potential competing interests include employment, consultancies, stock ownership, honoraria, paid expert testimony, patent applications/registrations, and grants or other funding. Authors must disclose any interests in two places: 1. A summary declaration of interest statement in the title page file (if double-blind) or the manuscript file (if single-blind). If there are no interests to declare then please state this: 'Declarations of interest: none'. This summary statement will be ultimately published if the article is accepted. 2. Detailed disclosures as part of a separate Declaration of Interest form, which forms part of the journal's official records. It is important for potential interests to be declared in both places and that the information matches. More information.

Submission declaration and verification

Submission of an article implies that the work described has not been published previously (except in the form of an abstract, a published lecture or academic thesis, see 'Multiple, redundant or concurrent publication' for more information), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyrightholder. To verify originality, your article may be checked by the originality detection service Crossref Similarity Check.

Use of inclusive language

Inclusive language acknowledges diversity, conveys respect to all people, is sensitive to differences, and promotes equal opportunities. Articles should make no assumptions about the beliefs or commitments of any reader, should contain nothing which might imply that one individual is superior to another on the grounds of race, sex, culture or any other characteristic, and should use inclusive language throughout. Authors should ensure that writing is free from bias, for instance by using 'he or she', 'his/her' instead of 'he' or 'his', and by making use of job titles that are free of stereotyping (e.g. 'chairperson' instead of 'chairman' and 'flight attendant' instead of 'stewardess').

Changes to authorship

Authors are expected to consider carefully the list and order of authors before submitting their manuscript and provide the definitive list of authors at the time of the original submission. Any addition, deletion or rearrangement of author names in the authorship list should be made only before the manuscript has been accepted and only if approved by the journal Editor. To request such a change, the Editor must receive the following from the corresponding author: (a) the reason for the change in author list and (b) written confirmation (e-mail, letter) from all authors that they agree with the addition, removal or rearrangement. In the case of addition or removal of authors, this includes confirmation from the author being added or removed. Only in exceptional circumstances will the Editor consider the addition, deletion or rearrangement of authors after the manuscript has been accepted. While the Editor considers the request, publication of the manuscript will be suspended. If the manuscript has already been published in an online issue, any requests approved by the Editor will result in a corrigendum.

Copyright

Upon acceptance of an article, authors will be asked to complete a 'Journal Publishing Agreement' (see more information on this). An e-mail will be sent to the corresponding author confirming receipt of the manuscript together with a 'Journal Publishing Agreement' form or a link to the online version of this agreement. Subscribers may reproduce tables of contents or prepare lists of articles including abstracts for internal circulation within their institutions. Permission of the Publisher is required for resale or distribution outside the institution and for all other derivative works, including compilations and translations. If excerpts from other copyrighted works are included, the author(s) must obtain written permission from the copyright owners and credit the source(s) in the article. Elsevier has pre-printed forms for use by authors in these cases. For gold open access articles: Upon acceptance of an article, authors will be asked to complete an 'Exclusive License Agreement' (more information). Permitted third party reuse of gold open access articles is determined by the author's choice of user license. Author rights As an author you (or your employer or institution) have certain rights to reuse your work. More information.

Elsevier supports responsible sharing
Find out how you can share your research published in Elsevier journals.

Role of the funding source

You are requested to identify who provided financial support for the conduct of the research and/or preparation of the article and to briefly describe the role of the sponsor(s), if any, in study design; in the collection, analysis and interpretation of data; in the writing of the report; and in the decision to submit the article for publication. If the funding source(s) had no such involvement, then this should be stated.

Funding body agreements and policies
Elsevier has established a number of agreements with funding bodies which allow authors to comply with their funder's open access policies. Some funding bodies will reimburse the author for the gold open access publication fee. Details of existing agreements are available online.

Open access

This journal offers authors a choice in publishing their research:

Subscription

- Articles are made available to subscribers as well as developing countries and patient groups through our universal access programs.
- No open access publication fee payable by authors.
- The Author is entitled to post the accepted manuscript in their institution's repository and make this public after an embargo period (known as green Open Access). The published journal article cannot be shared publicly, for example on ResearchGate or Academia.edu, to ensure the sustainability of peer-reviewed research in journal publications. The embargo period for this journal can be found below. Gold open access
- Articles are freely available to both subscribers and the wider public with permitted reuse.
- A gold open access publication fee is payable by authors or on their behalf, e.g. by their research funder or institution. Regardless of how you choose to publish your article, the journal will apply the same peer review criteria and acceptance standards.

For gold open access articles, permitted third party (re)use is defined by the following

Creative

Commons user licenses:

Creative Commons Attribution (CC BY)
Let's others distribute and copy the article, create extracts, abstracts, and other revised versions, adaptations or derivative works of or from an article (such as a translation), include in a collective work (such as an anthology), text or data mine the article, even for commercial purposes, as long as they credit the author(s), do not represent the author as endorsing their

adaptation of the article, and do not modify the article in such a way as to damage the author's honor or reputation.

Creative Commons Attribution-NonCommercial-NoDerivs (CC BY-NC-ND)
For non-commercial purposes, lets others distribute and copy the article, and to include in a collective work (such as an anthology), as long as they credit the author(s) and provided they do not alter or modify the article. The gold open access publication fee for this journal is USD 2050, excluding taxes. Learn more about Elsevier's pricing policy: https://www.elsevier.com/openaccesspricing.

Green open access
Authors can share their research in a variety of different ways and Elsevier has a number of green open access options available. We recommend authors see our open access page for further information. Authors can also self-archive their manuscripts immediately and enable public access from their institution's repository after an embargo period. This is the version that has been accepted for publication and which typically includes author-incorporated changes suggested during submission, peer review and in editor-author communications. Embargo period: For subscription articles, an appropriate amount of time is needed for journals to deliver value to subscribing customers before an article becomes freely available to the public. This is the embargo period and it begins from the date the article is formally published online in its final and fully citable form. Find out more. This journal has an embargo period of 24 months.

Elsevier Researcher Academy
Researcher Academy is a free e-learning platform designed to support early and mid-career researchers throughout their research journey. The "Learn" environment at Researcher Academy offers several interactive modules, webinars, downloadable guides and resources to guide you through the process of writing for research and going through peer review. Feel free to use these free resources to improve your submission and navigate the publication process with ease.

Language (usage and editing services)
Please write your text in good English (American or British usage is accepted, but not a mixture of these). Authors who feel their English language manuscript may require editing to eliminate possible grammatical or spelling errors and to conform to correct scientific English may wish to use the English Language Editing service available from Elsevier's Author Services.

Submission

Our online submission system guides you stepwise through the process of entering your article details and uploading your files. The system converts your article files to a single PDF file used in the peer-review process. Editable files (e.g., Word, LaTeX) are required to typeset your article for final publication. All correspondence, including notification of the Editor's decision and requests for revision, is sent by e-mail.

Submit your article
Please submit your article via http://ees.elsevier.com/chb/

PREPARATION

NEW SUBMISSIONS

Submission to this journal proceeds totally online and you will be guided stepwise through the creation and uploading of your files. The system automatically converts your files to a single PDF file, which is used in the peer-review process. As part of the Your Paper Your Way service, you may choose to submit your manuscript as a single file to be used in the refereeing process. This can be a PDF file or a Word document, in any format or layout that can be used by referees to evaluate your manuscript. It should contain high enough quality figures for refereeing. If you prefer to do so, you may still provide all or some of the source files at the initial submission. Please note that individual figure files larger than 10 MB must be uploaded separately.

References
There are no strict requirements on reference formatting at submission. References can be in any style or format as long as the style is consistent. Where applicable, author(s) name(s), journal title/book title, chapter title/article title, year of publication, volume number/book chapter and the article number or pagination must be present. Use of DOI is highly encouraged. The reference style used by the journal will be applied to the accepted article by Elsevier at the proof stage. Note that missing data will be highlighted at proof stage for the author to correct.

Formatting requirements
There are no strict formatting requirements, but all manuscripts must contain the essential elements needed to convey your manuscript, for example Abstract, Keywords, Introduction, Materials and Methods, Results, Conclusions, Artwork and Tables with Captions. If your article includes any Videos and/or other Supplementary material, this should be included in your initial submission for peer review purposes. Divide the article into clearly defined sections.

Figures and tables embedded in text
Please ensure the figures and the tables included in the single file are placed next to the relevant text in the manuscript, rather than at the bottom or the top of the file. The corresponding caption should be placed directly below the figure or table.

Peer review

This journal operates a double-blind review process. All contributions will be initially assessed by the editor for suitability for the journal. Papers deemed suitable are then typically sent to a minimum of two independent expert reviewers to assess the scientific quality of the paper. The Editor is responsible for the final decision regarding acceptance or rejection of articles. The Editor's decision is final. More information on types of peer review.

Double-blind review

This journal uses double-blind review, which means the identities of the authors are concealed from the reviewers, and vice versa. More information is available on our website. To facilitate this, please include the following separately:

Title page (with author details): This should include the title, authors' names, affiliations, acknowledgements and any Declaration of Interest statement, and a complete address for the corresponding author including an e-mail address.

Blinded manuscript (no author details): The main body of the paper (including the references, figures, tables and any acknowledgements) should not include any identifying information, such as the authors' names or affiliations.

REVISED SUBMISSIONS

Use of word processing software
Regardless of the file format of the original submission, at revision you must provide us with an editable file of the entire article. Keep the layout of the text as simple as possible. Most formatting codes will be removed and replaced on processing the article. The electronic text should be prepared in a way very similar to that of conventional manuscripts (see also the Guide to Publishing with Elsevier). See also the section on Electronic artwork.

To avoid unnecessary errors, you are strongly advised to use the 'spell-check' and 'grammar check' functions of your word processor.

Article structure

Subdivision - numbered sections
Divide your article into clearly defined and numbered sections. Subsections should be numbered 1.1 (then 1.1.1, 1.1.2, ...), 1.2, etc. (the abstract is not included in section numbering). Use this numbering also for internal cross-referencing: do not just refer to 'the text'. Any subsection may be given a brief heading. Each heading should appear on its own separate line.

Introduction
State the objectives of the work and provide an adequate background, avoiding a detailed literature survey or a summary of the results. Material and methods Provide sufficient details to allow the work to be reproduced by an independent researcher. Methods that are already published should be summarized and indicated by a reference. If quoting directly from a previously published method, use quotation marks and also cite the source. Any modifications to existing methods should also be described.

Theory/calculation
A Theory section should extend, not repeat, the background to the article already dealt with in the Introduction and lay the foundation for further work. In contrast, a Calculation section represents a practical development from a theoretical basis.

Results
Results should be clear and concise.

Discussion
This should explore the significance of the results of the work, not repeat them. A combined Results and Discussion section is often appropriate. Avoid extensive citations and discussion of published literature.

Conclusions
The main conclusions of the study may be presented in a short Conclusions section, which may stand alone or form a subsection of a Discussion or Results and Discussion section.

Appendices
If there is more than one appendix, they should be identified as A, B, etc. Formulae and equations in appendices should be given separate numbering: Eq. (A.1), Eq. (A.2), etc.; in a subsequent appendix, Eq. (B.1) and so on. Similarly, for tables and figures: Table A.1; Fig. A.1, etc.

Essential title page information

- ***Title***. Concise and informative. Titles are often used in information-retrieval systems. Avoid abbreviations and formulae where possible
- ***Author names and affiliations***. Please clearly indicate the given name(s) and family name(s) of each author and check that all names are accurately spelled. You can add your name between parentheses in your own script behind the English transliteration. Present the authors' affiliation addresses (where the actual work was done) below the names. Indicate all affiliations with a lowercase superscript letter immediately after the author's name and in front of the appropriate address. Provide the full postal address of each affiliation, including the country name and, if available, the e-mail address of each author.

- ***Corresponding author.*** Clearly indicate who will handle correspondence at all stages of refereeing and publication, also post-publication. This responsibility includes answering any future queries about Methodology and Materials. Ensure that the e-mail address is given and that contact details are kept up to date by the corresponding author.
- ***Present/permanent address***. If an author has moved since the work described in the article was done, or was visiting at the time, a 'Present address' (or 'Permanent address') may be indicated as a footnote to that author's name. The address at which the author actually did the work must be retained as the main, affiliation address. Superscript Arabic numerals are used for such footnotes.

Highlights

Highlights are optional yet highly encouraged for this journal, as they increase the discoverability of your article via search engines. They consist of a short collection of bullet points that capture the novel results of your research as well as new methods that were used during the study (if any). Please have a look at the examples here: example Highlights. Highlights should be submitted in a separate editable file in the online submission system. Please use 'Highlights' in the file name and include 3 to 5 bullet points (maximum 85 characters, including spaces, per bullet point).

Abstract

A concise and factual abstract is required and should not be longer than 200 words. The abstract should state briefly the purpose of the research, the principal results and major conclusions. An abstract is often presented separately from the article, so it must be able to stand alone. For this reason, References should be avoided, but if essential, then cite the author(s) and year(s). Also, nonstandard or uncommon abbreviations should be avoided, but if essential they must be defined at their first mention in the abstract itself. graphical abstract Although a graphical abstract is optional, its use is encouraged as it draws more attention to the online article. The graphical abstract should summarize the contents of the article in a concise, pictorial form designed to capture the attention of a wide readership. Graphical abstracts should be submitted as a separate file in the online submission system. Image size: Please provide an image with a minimum of 531 × 1328 pixels (h × w) or proportionally more. The image should be readable at a size of 5 × 13 cm using a regular screen resolution of 96 dpi. Preferred file types: TIFF, EPS, PDF or MS Office files. You can view Example Graphical Abstracts on our information site. Authors can make use of Elsevier's Illustration Services to ensure the best presentation of their images and in accordance with all technical requirements.

Keywords

Immediately after the abstract, provide a maximum of 6 keywords, using American spelling and avoiding general and plural terms and multiple concepts (avoid, for example, 'and', 'of'). Be sparing with abbreviations: only abbreviations firmly established in the field may be eligible. These keywords will be used for indexing purposes.

Abbreviations

Define abbreviations that are not standard in this field in a footnote to be placed on the first page of the article. Such abbreviations that are unavoidable in the abstract must be defined at their first mention there, as well as in the footnote. Ensure consistency of abbreviations throughout the article.

Acknowledgements

Do not include acknowledgements on the title page, as a footnote to the title or otherwise. In a separate file to the manuscript, list those individuals who provided help during the research (e.g., providing language help, writing assistance or proof reading the article, etc.)

Formatting of funding sources List funding sources in this standard way to facilitate compliance to funder's requirements: Funding: This work was supported by the National Institutes of Health [grant numbers xxxx, yyyy]; the Bill & Melinda Gates Foundation, Seattle, WA [grant number zzzz]; and the United States Institutes of Peace [grant number aaaa]. It is not necessary to include detailed descriptions on the program or type of grants and awards. When funding is from a block grant or other resources available to a university, college, or other research institution, submit the name of the institute or organization that provided the funding. If no funding has been provided for the research, please include the following sentence: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Math formulae
Please submit math equations as editable text and not as images. Present simple formulae in line with normal text where possible and use the solidus (/) instead of a horizontal line for small fractional terms, e.g., X/Y. In principle, variables are to be presented in italics. Powers of e are often more conveniently denoted by exp. Number consecutively any equations that have to be displayed separately from the text (if referred to explicitly in the text).

Footnotes
Footnotes should be used sparingly. Number them consecutively throughout the article. Many word processors build footnotes into the text, and this feature may be used. Should this not be the case, indicate the position of footnotes in the text and present the footnotes themselves separately at the end of the article.

Artwork

Electronic artwork
General points

- Make sure you use uniform lettering and sizing of your original artwork.
- Preferred fonts: Arial (or Helvetica), Times New Roman (or Times), Symbol, Courier.
- Number the illustrations according to their sequence in the text.
- Use a logical naming convention for your artwork files.
- Indicate per figure if it is a single, 1.5 or 2-column fitting image. • For Word submissions only, you may still provide figures and their captions, and tables within a single file at the revision stage.
- Please note that individual figure files larger than 10 MB must be provided in separate source files.

A detailed guide on electronic artwork is available.
You are urged to visit this site; some excerpts from the detailed information are given here.

Formats
Regardless of the application used, when your electronic artwork is finalized, please 'save as' or convert the images to one of the following formats (note the resolution requirements for line drawings, halftones, and line/halftone combinations given below): EPS (or PDF): Vector drawings. Embed the font or save the text as 'graphics'. TIFF (or JPG): Color or grayscale photographs (halftones): always use a minimum of 300 dpi. TIFF (or JPG): Bitmapped line drawings: use a minimum of 1000 dpi. TIFF (or JPG): Combinations bitmapped line/half tone (color or grayscale): a minimum of 500 dpi is required.

Please do not:

- Supply files that are optimized for screen use (e.g., GIF, BMP, PICT, WPG); the resolution is too low.

- Supply files that are too low in resolution.
- Submit graphics that are disproportionately large for the content.

Color artwork
Please make sure that artwork files are in an acceptable format (TIFF (or JPEG), EPS (or PDF), or MS Office files) and with the correct resolution. If, together with your accepted article, you submit usable color figures then Elsevier will ensure, at no additional charge, that these figures will appear in color online (e.g., ScienceDirect and other sites) regardless of whether or not these illustrations are reproduced in color in the printed version. **For color reproduction in print, you will receive information regarding the costs from Elsevier after receipt of your accepted article. Please indicate your preference for color: in print or online only. Further information on the preparation of electronic artwork.**

Figure captions
Ensure that each illustration has a caption. A caption should comprise a brief title (not on the figure itself) and a description of the illustration. Keep text in the illustrations themselves to a minimum but explain all symbols and abbreviations used.

Tables

Please submit tables as editable text and not as images. Tables can be placed either next to the relevant text in the article, or on separate page(s) at the end. Number tables consecutively in accordance with their appearance in the text and place any table notes below the table body. Be sparing in the use of tables and ensure that the data presented in them do not duplicate results described elsewhere in the article. Please avoid using vertical rules and shading in table cells.

References

Citation in text
Please ensure that every reference cited in the text is also present in the reference list (and vice versa). Any references cited in the abstract must be given in full. Unpublished results and personal communications are not recommended in the reference list, but may be mentioned in the text. If these references are included in the reference list they should follow the standard reference style of the journal and should include a substitution of the publication date with either 'Unpublished results' or 'Personal communication'. Citation of a reference as 'in press' implies that the item has been accepted for publication.

Web references
As a minimum, the full URL should be given and the date when the reference was last accessed. Any further information, if known (DOI, author names, dates, reference to a source publication, etc.), should also be given. Web references can be listed separately (e.g., after the reference list) under a different heading if desired, or can be included in the reference list.

Data references
This journal encourages you to cite underlying or relevant datasets in your manuscript by citing them in your text and including a data reference in your Reference List. Data references should include the following elements: author name(s), dataset title, data repository, version (where available), year, and global persistent identifier. Add [dataset] immediately before the reference so we can properly identify it as a data reference. The [dataset] identifier will not appear in your published article.

eferences in a special issue
Please ensure that the words 'this issue' are added to any references in the list (and any citations in the text) to other articles in the same Special Issue.

Reference management software
Most Elsevier journals have their reference template available in many of the most popular reference management software products. These include all products that support Citation Style Language styles, such as Mendeley. Using citation plug-ins from these products, authors only need to select the appropriate journal template when preparing their article, after which citations and bibliographies will be automatically formatted in the journal's style. If no template is yet available for this journal, please follow the format of the sample references and citations as shown in this Guide. If you use reference management software, please ensure that you remove all field codes before submitting the electronic manuscript. More information on how to remove field codes from different reference management software. Users of Mendeley Desktop can easily install the reference style for this journal by clicking the following link: http://open.mendeley.com/use-citation-style/computers-in-human-behavior
When preparing your manuscript, you will then be able to select this style using the Mendeley plugins for Microsoft Word or LibreOffice.

Reference formatting
There are no strict requirements on reference formatting at submission. References can be in any style or format as long as the style is consistent. Where applicable, author(s) name(s), journal title/book title, chapter title/article title, year of publication, volume number/book chapter and the article number or pagination must be present. Use of DOI is highly encouraged. The reference style used by the journal will be applied to the accepted article by Elsevier at the proof stage. Note that missing data will be highlighted at proof stage for the author to correct. If you do wish to format the references yourself, they should be arranged according to the following examples:

Reference style
Text: Citations in the text should follow the referencing style used by the American Psychological Association. You are referred to the Publication Manual of the American Psychological Association, Sixth Edition, ISBN 978-1-4338-0561-5, copies of which may be ordered online or APA Order Dept., P.O.B. 2710, Hyattsville, MD 20784, USA or APA, 3 Henrietta Street, London, WC3E 8LU, UK.

List: references should be arranged first alphabetically and then further sorted chronologically if necessary. More than one reference from the same author(s) in the same year must be identified by the letters 'a', 'b', 'c', etc., placed after the year of publication.

Examples:
Reference to a journal publication: Van der Geer, J., Hanraads, J. A. J., & Lupton, R. A. (2010). The art of writing a scientific article. Journal of Scientific Communications, 163, 51–59. https://doi.org/10.1016/j.Sc.2010.00372.

Reference to a journal publication with an article number:
Van der Geer, J., Hanraads, J. A. J., & Lupton, R. A. (2018). The art of writing a scientific article. Heliyon, 19, e00205. https://doi.org/10.1016/j.heliyon.2018.e00205.
Reference to a book: Strunk, W., Jr., & White, E. B. (2000). The elements of style. (4th ed.). New York: Longman, (Chapter 4).

Reference to a chapter in an edited book:
Mettam, G. R., & Adams, L. B. (2009). How to prepare an electronic version of your article. In B. S. Jones, & R. Z. Smith (Eds.), Introduction to the electronic age (pp. 281–304). New York: E-Publishing Inc.

Reference to a website:

Cancer Research UK. Cancer statistics reports for the UK. (2003). http://www.cancerresearchuk.org/aboutcancer/statistics/cancerstatsreport/ Accessed 13 March 2003.

Reference to a dataset:
[dataset] Oguro, M., Imahiro, S., Saito, S., Nakashizuka, T. (2015). Mortality data for Japanese oak wilt disease and surrounding forest compositions. Mendeley Data, v1. https://doi.org/10.17632/xwj98nb39r.1

Reference to a conference paper or poster presentation: Engle, E.K., Cash, T.F., & Jarry, J.L. (2009, November). The Body Image Behaviours Inventory-3: Development and validation of the Body Image Compulsive Actions and Body Image Avoidance Scales.
Poster session presentation at the meeting of the Association for Behavioural and Cognitive Therapies, New York, NY.

Video

Elsevier accepts video material and animation sequences to support and enhance your scientific research. Authors who have video or animation files that they wish to submit with their article are strongly encouraged to include links to these within the body of the article. This can be done in the same way as a figure or table by referring to the video or animation content and noting in the body text where it should be placed. All submitted files should be properly labeled so that they directly relate to the video file's content. . In order to ensure that your video or animation material is directly usable, please provide the file in one of our recommended file formats with a preferred maximum size of 150 MB per file, 1 GB in total. Video and animation files supplied will be published online in the electronic version of your article in Elsevier Web products, including ScienceDirect. Please supply 'stills' with your files: you can choose any frame from the video or animation or make a separate image. These will be used instead of standard icons and will personalize the link to your video data. For more detailed instructions please visit our video instruction pages. Note: since video and animation cannot be embedded in the print version of the journal, please provide text for both the electronic and the print version for the portions of the article that refer to this content.

Data visualization

Include interactive data visualizations in your publication and let your readers interact and engage more closely with your research. Follow the instructions here to find out about available data visualization options and how to include them with your article.

Supplementary material

Supplementary material such as applications, images and sound clips, can be published with your article to enhance it. Submitted supplementary items are published exactly as they are received (Excel or PowerPoint files will appear as such online). Please submit your material together with the article and supply a concise, descriptive caption for each supplementary file. If you wish to make changes to supplementary material during any stage of the process, please make sure to provide an updated file. Do not annotate any corrections on a previous version. Please switch off the 'Track Changes' option in Microsoft Office files as these will appear in the published version.

Research data

This journal encourages and enables you to share data that supports your research publication where appropriate, and enables you to interlink the data with your published articles. Research data refers to the results of observations or experimentation that validate research findings. To facilitate reproducibility and data reuse, this journal also encourages you to share your software, code, models, algorithms, protocols, methods and other useful materials related to the project. Below are a number of ways in which you can associate data with your article or make a statement about the availability of your data when submitting your manuscript. If you are sharing data in one of these ways, you are encouraged to cite the data in your manuscript and reference list. Please refer to the "References" section for more information about data citation. For more information on depositing, sharing and using research data and other relevant research materials, visit the research data page.

Data linking

If you have made your research data available in a data repository, you can link your article directly to the dataset. Elsevier collaborates with a number of repositories to link articles on ScienceDirect with relevant repositories, giving readers access to underlying data that gives them a better understanding of the research described. There are different ways to link your datasets to your article. When available, you can directly link your dataset to your article by providing the relevant information in the submission system. For more information, visit the database linking page. For supported data repositories a repository banner will automatically appear next to your published
article on ScienceDirect. In addition, you can link to relevant data or entities through identifiers within the text of your manuscript, using the following format: Database: xxxx (e.g., TAIR: AT1G01020; CCDC: 734053; PDB: 1XFN).

Mendeley Data

This journal supports Mendeley Data, enabling you to deposit any research data (including raw and processed data, video, code, software, algorithms, protocols, and methods) associated with your manuscript in a free-to-use, open access repository. During the submission process, after uploading your manuscript, you will have the opportunity to upload your relevant datasets directly to Mendeley
Data. The datasets will be listed and directly accessible to readers next to your published article online. For more information, visit the Mendeley Data for journals page.

Data in Brief

You have the option of converting any or all parts of your supplementary or additional raw data into one or multiple data articles, a new kind of article that houses and describes your data. Data articles ensure that your data is actively reviewed, curated, formatted, indexed, given a DOI and publicly available to all upon publication. You are encouraged to submit your article for Data in Brief as an additional item directly alongside the revised version of your manuscript. If your research article is
accepted, your data article will automatically be transferred over to Data in Brief where it will be editorially reviewed and published in the open access data journal, Data in Brief. Please note an open access fee of 600 USD is payable for publication in Data in Brief. Full details can be found on the Data in Brief website. Please use this template to write your Data in Brief.

Data statement

To foster transparency, we encourage you to state the availability of your data in your submission. This may be a requirement of your funding body or institution. If your data is unavailable to access or unsuitable to post, you will have the opportunity to indicate why during the submission process, for example by stating that the research data is confidential. The statement will appear with your published article on ScienceDirect. For more information, visit the Data Statement page.

AFTER ACCEPTANCE

Online proof correction

Corresponding authors will receive an e-mail with a link to our online proofing system, allowing annotation and correction of proofs online. The environment is similar to MS Word: in addition to editing text, you can also comment on figures/tables and answer questions from the Copy Editor. Web-based proofing provides a faster and less error-prone

process by allowing you to directly type your corrections, eliminating the potential introduction of errors. If preferred, you can still choose to annotate and upload your edits on the PDF version. All instructions for proofing will be given in the e-mail we send to authors, including alternative methods to the online version and PDF. We will do everything possible to get your article published quickly and accurately. Please use this
proof only for checking the typesetting, editing, completeness and correctness of the text, tables and figures. Significant changes to the article as accepted for publication will only be considered at this stage with permission from the Editor. It is important to ensure that all corrections are sent back to us in one communication. Please check carefully before replying, as inclusion of any subsequent corrections cannot be guaranteed. Proofreading is solely your responsibility.

Offprints

The corresponding author will, at no cost, receive a customized Share Link providing 50 days free access to the final published version of the article on ScienceDirect. The Share Link can be used for sharing the article via any communication channel, including email and social media. For an extra charge, paper offprints can be ordered via the offprint order form which is sent once the article is accepted for publication. Both corresponding and co-authors may order offprints at any time via Elsevier's Author Services. Corresponding authors who have published their article gold open access do not receive a Share Link as their final published version of the article is available open access on ScienceDirect and can be shared through the article DOI link.

AUTHOR INQUIRIES

Visit the Elsevier Support Center to find the answers you need. Here you will find everything from
Frequently Asked Questions to ways to get in touch.

Appendix B: Participant Information Sheet

PARTICIPANT INFORMATION SHEET

PROJECT TITLE: Security awareness and behaviours in workers with dual device smartphones

HUMAN RESEARCH ETHICS COMMITTEE APPROVAL NUMBER: H-2019-45

PRINCIPAL INVESTIGATOR: Dr. Clemence Due

STUDENT RESEARCHER: Ms. Holly Mason

STUDENT'S DEGREE: Master of Psychology (Organisational and Human Factors)

Dear Participant,

You are invited to participate in the research project described below.

What is the project about?

You are being invited to take part in this study to increase the understanding of how people use smartphone devices, and in particular, dual devices, on an everyday basis. The aim of this study is to gain a clearer understanding of how people manage dual devices, to what extent tasks performed on either device might similar or different and how security behaviours might influence the performance of tasks, and everyday use of the devices. The study is interested in identifying the decision-making process and which factors might influence or motivate behavioural decisions. The study endeavours to understand the functionality of a dual device relationship.

Who is undertaking the project?

This project is being conducted by Dr. Clemence Due and Ms. Holly Mason. This research will form the basis for the degree of Master of Psychology (Organisational and Human Factors) at the University of Adelaide under the supervision of Dr. Clemence Due, Ms. Kathryn Parsons and Dr. Dragana Calic.

Why am I being invited to participate?

You are being invited to participate in this study as you fit the following criteria:

1. Are over the age of 18 and are fluent in English
2. Use both a personal and work-supplied smart phone device

What am I being invited to do?

If you wish to participate, you will be asked to spend approximately 30-60 minutes being interviewed about the everyday use of both your personal and work-supplied smartphone devices. Interviews will take place on the premises of your place of work, at a time that is convenient to you. If you would prefer, the interview location can be relocated to somewhere else in public setting such as the University of Adelaide.

The interview will be audio recorded so that an anonymous transcription can be made of the interview. An anonymous transcription is a written-out record of the interview that contains no identifying information.

How much time will my involvement in the project take?

You will be asked to spend approximately 30-60 minutes being interviewed.

Are there any risks associated with participating in this project?

The only risk identified by participating in this research is the risk of disclosing information about breach of company policy. However, this information will not be revealed to your employer as everything discussed is confidential and will be kept completely anonymous and un-identifiable. The name of the organisation will also not be disclosed at any point and will be referred to as an Australian insurance company in any subsequent reporting.

Despite the researcher currently completing a student placement on site, the employer will have no access to participant details, including who participated and what was discussed during the interviews. The results will be completely confidential. The research has no influence by anyone employed at the organisation, however an overview of results will be supplied to the organisation.

What are the potential benefits of the research project?

It is expected that the findings of the study will inform professionals in various domains including information and technology, human resources and security to better assess the benefits and areas for improvement for the use of dual devices by workers. This should serve to improve functionality and performance in roles and tasks. Further, the results aim to improve understanding of which factors may prevent or motivate someone performing certain tasks on a mobile device. Including tasks they may not perform, such as security protocols and storage of the device. The benefit of this should be to understand how we can better use and guide the use of smartphone devices personally, and in assisting and protect workers and their organisations.

Can I withdraw from the project?

Participation in this project is completely voluntary. If you agree to participate, you can withdraw from the study at any time. You do not have to answer all the questions and you may terminate the interview or choose to withdraw as a participant at any time up until the time Holly submits her thesis. It must be understood that participation or non-participation does not influence employment at the organisation.

What will happen to my information?

Confidentiality and privacy: Your name and any identifying information will remain anonymous and will not appear in any subsequent publications or reports that arise from the data. Only the named investigators above will have access to the interview transcripts for the purpose of analysis.

Storage: As per the University of Adelaide Human Research Ethics Committee guidelines de-identified transcripts of all interviews will be kept securely on a password secured computer in Dr Due's office in The School of Psychology for a period of seven years.

Publishing: The data will remain de-identified and every effort will be made to ensure anonymity in all reported results and publications. The data will be used in the researcher's Master of Psychology thesis as part of her coursework, and this could be potentially result in a publication or journal article. Extracts from interviews may be used, however these will be completely anonymous with the use of pseudonyms, any identifiable information will be excluded.

Sharing: Once interviews have been transcribed participants will have the opportunity to review their own transcript and the summary of themes produced by the analysis to confirm the researcher has a true and accurate representation of the data. A summary of the results will be provided to the organisation, as well as a presentation by the researcher, to inform the organisation of the findings of the research.

Your information will only be used as described in this participant information sheet and it will only be disclosed according to the consent provided, except as required by law.

Who do I contact if I have questions about the project?

[redacted]

What if I have a complaint or any concerns?

The study has been approved by the Human Research Ethics Committee at the University of Adelaide (approval number H-2019-45). This research project will be conducted according to the NHMRC National Statement on Ethical Conduct in Human Research 2007 (Updated 2018). If you have questions or problems associated with the practical aspects of your participation in the project, or wish to raise a concern or complaint about the project, then you should consult the Principal Investigator. If you wish to speak with an independent person regarding concerns or a complaint, the University's policy on research involving human participants, or your rights as a participant, please contact the Human Research Ethics Committee's Secretariat on:
Phone: +61 8 8313 6028

Email: hrec@adelaide.edu.au
Post: Level 4, Rundle Mall Plaza, 50 Rundle Mall, ADELAIDE SA 5000
Any complaint or concern will be treated in confidence and fully investigated. You will be informed of the outcome.

If I want to participate, what do I do?

If you would like to participate in this research, please contact Holly. She will be able to provide you with further information about the study, and can organise a time to meet for an interview.

Yours sincerely,

[redacted]

Appendix C: Participant consent form

Human Research Ethics Committee (HREC)

CONSENT FORM

1. I have read the attached Information Sheet and agree to take part in the following research project:

Title:	**Security awareness and behaviours in workers with dual device smartphones**
Ethics Approval Number:	**H-2019-45**

2. I have had the project, so far as it affects me, and the potential risks and burdens fully explained to my satisfaction by the research worker. I have had the opportunity to ask any questions I may have about the project and my participation. My consent is given freely.

3. I have been given the opportunity to have a member of my family or a friend present while the project was explained to me.

4. Although I understand the purpose of the research project is to improve the quality of health/medical care, it has also been explained that my involvement may not be of any benefit to me.

5. I agree to participate in the activities as outlined in the participant information sheet.

6. I agree to be:
   Audio recorded ☐ Yes ☐ No

7. I understand that as my participation is anonymous, I am free to withdraw from the project at any time up until submission of the thesis

8. I have been informed that the information gained in the project may be published in a journal article/thesis/conference presentations/report etc.

9. I have been informed that in the published materials I will not be identified, and my personal results will not be divulged.

10. I agree to my information being used for future research purposes as follows:
    - Research undertaken by these same researcher(s) Yes ☐ No ☐
    - Related research undertaken by any researcher(s) Yes ☐ No ☐
    - Any research undertaken by any researcher(s) Yes ☐ No ☐

11. I understand my information will only be disclosed according to the consent provided, except where disclosure is required by law.

12. I am aware that I should keep a copy of this Consent Form, when completed, and the attached Information Sheet.

Participant to complete:

Name: ______________________ Signature:________________________ Date: ____________________________

Researcher/Witness to complete:

I have described the nature of the research to ____

(print name of participant)

and in my opinion she/he understood the explanation.

Signature: ___________________ Position: _________________________ Date: ____________________________

Appendix D: Interview Schedule

1. Can you please briefly describe your role in the workplace and the tasks that you perform?

2. How does your work-supplied smartphone device assist you in performing your work duties?

3. Did/does your employer set any guidelines or requirements for work related smartphone usage?

Prompt

1. Any rules or restrictions?

2. Do you believe these to be effective?

3. Are they an inconvenience? Require a lot of effort? Time consuming? Effort exceeds benefits?

4. In what ways does your activity on your work device differ to your activity on your personal device?

Prompt

5. Is there a reason for this difference…for example, company policy, security or data stored on either phone?

6. Do you perform any tasks/actions on your work-supplied phone for personal use?

7. Do you worry about the security on and of your personal phone more or less than the security on and of your work-supplied phone?

Prompt

8. Are your security behaviours different on each phone as a direct result?

9. Do you deliberately not perform certain tasks/activities on either phone due to security? Due to policy?

10. What are you gaining by doing or not doing the same security behaviours?

11. What are you losing?

12. Do you back up either phone?

13. Have you downloaded apps on your work phone, or use social media? Is the app work-related or for personal use?

Prompt

14. Do you read the privacy statement? Free or paid?

15. Would you say that your security behaviours (the things you do to protect what you have on your phone) on your mobile phones is different compared to your security behaviours on a laptop or PC?

Prompt

16. Tasks you perform (finances), installation of security software, passwords, and physical security of device

17. How susceptible do you think you are to a security threat?

Prompt

18. Do you worry or think about security when performing activities on either phone?

19. Do you use public/free wifi?

20. Do you think that your security behaviours/actions effect your susceptibility?

21. I just want you to imagine for a second, what is the worst thing that could happen to your device?

Prompt

22. How likely do you think it is that this could actually happen?

23. Has something adverse happened before?

24. Are you aware of what security threats are out there? Do you think that you are susceptible/not susceptible to these threats?

Demographics

25. Age:

26. Gender:

27. Ethnicity:

28. Level of education:

29. Proficiency with IT/Technology/Smartphone use:

    Low/Med/High

30. English first language:

31. How long have you used smart phones?

32. What model is your work phone:

33. What model is your personal phone: