12-7-2022

A Separate Phone to Work and Play: Protection Motivation Theory and Smartphone Security Behaviour

Holly Mason
University of Adelaide, holly.mason@adelaide.edu.au

Kathryn Parsons
Defence Science and Technology Group, kathryn.parsons@defence.gov.au

Dragana Calic
Defence Science and Technology Group, dragana.pittas@defence.gov.au

Clemence Due
University of Adelaide, clemence.due@adelaide.edu.au

A Separate Phone to Work and Play: Protection Motivation Theory and Smartphone Security Behaviour

Holly Mason
University of Adelaide
Edinburgh, South Australia
Email: Holly.Mason@adelaide.edu.au

Kathryn Parsons
Defence Science and Technology (DST) Group
Edinburgh, South Australia
Email: Kathryn.Parsons@defence.gov.au

Dragana Calic
Defence Science and Technology (DST) Group
Edinburgh, South Australia
Email: Dragana.Calic@defence.gov.au

Clemence Due
University of Adelaide
Edinburgh, South Australia
Email: Clemence.Due@adelaide.edu.au

Abstract

Smartphone security is a growing concern. In this study, we use the Protection Motivation Theory (PMT) to explore users' attitudes, perceptions and behaviours towards the security of their work provided and personal smartphones. Australian employees from an insurance company participated in in-depth semi-structured interviews focussed on their behaviours. Data was analysed using deductive and inductive thematic analysis, guided by PMT to explore the comparisons between personal and work devices. The main overarching theme was that people behave more safely on their work smartphones compared to on their personal smartphones. Results suggest that perceived vulnerability, perceived reward, response cost, self-efficacy and social influence largely contributed to a lack of protective behaviours displayed when using personal smartphones. Despite the safe behaviour reported for work smartphones, these behaviours appear to be motivated by organisational controls, rather than intrinsically. This research has applied implications for education, relevant to both personal and workplace contexts.

Keywords Smartphone, Work smartphone, Personal smartphone, Protection Motivation Theory, Security behaviour.

1 Introduction

The use of smartphones as a person's sole device has seen a dramatic increase in recent years. The number of smartphone users in the world surpassed 6.5 billion in 2022 (O'Dea 2022). 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 engagement, navigation and online banking. Similarly, this surge in smartphone adoption has been reflected within organisational settings, enabling a new level of operational efficiency, benefitting employers by having an increasingly connected workforce (Allam et al. 2014). This has introduced a host of challenges for user information security (Allam et al. 2014; Verkijika 2018). For example, users are often required to disclose personal information such as names, addresses, financial and other sensitive details (Alsaleh et al. 2017). Therefore, while smartphones enable users to have a truly wireless, and connected lifestyle, they can also pose significant security and privacy threats (Torre et al. 2018).

This study will explore how people behave on smartphones across settings, and whether setting influences security behaviour. Specific research questions will focus on the extent to which people employ the same security behaviours regardless of setting; and, to what extent can Protective Motivation Theory (PMT) explain the use of smartphones across settings. Although PMT has been widely studied in relation to smartphones, the influence of settings has not been examined. Throughout the following sections, we present relevant literature outlining this important research gap.

1.1 Smartphone security

Due to the degree of sensitive information stored on smartphones, the theft of or access to a smartphone could result in stolen identities, blackmail, extortion and the re-sell of the hardware (Alsaleh et al. 2017; Clarke et al. 2016; Ophoff and Robinson 2014). 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). Recent research identified over 8.5 million malicious smartphone installation packages, 128,886 smartphone banking trojans and 261,214 ransomware trojans (Verkijika 2018).

Given these threats, one might assume that users would exercise extreme caution when operating and securing their smartphones. However, the opposite has been found. 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 tend to ignore security mechanisms or feel that they are generally ineffective in preventing or reducing the dangers and threats when using smartphones (Kusyanti and Catherina 2018; Wang et al. 2019). Not only is this concerning f the general population, but it may be even more concerning for organisations whose employees have access to personal and sensitive information who are often not adequately skilled to ensure good security 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 choose not to protect themselves against cyber security threat or danger. This literature has been dominated by the Protection Motivation Theory (PMT), which can be used to explain the common disparity between what a user thinks or knows they should do and their actual behaviour (Rogers 1975).

PMT consists of two cognitive processes, threat-appraisal and coping-appraisal, depicted in Figure 1. Threat-appraisal considers the likelihood and impact of the risk, while coping-appraisal considers the effectiveness of the adaptive response and the individual's ability to perform this behaviour (Milne et al. 2000; Rogers 1983; Verkijika 2018). Each component is explained below.

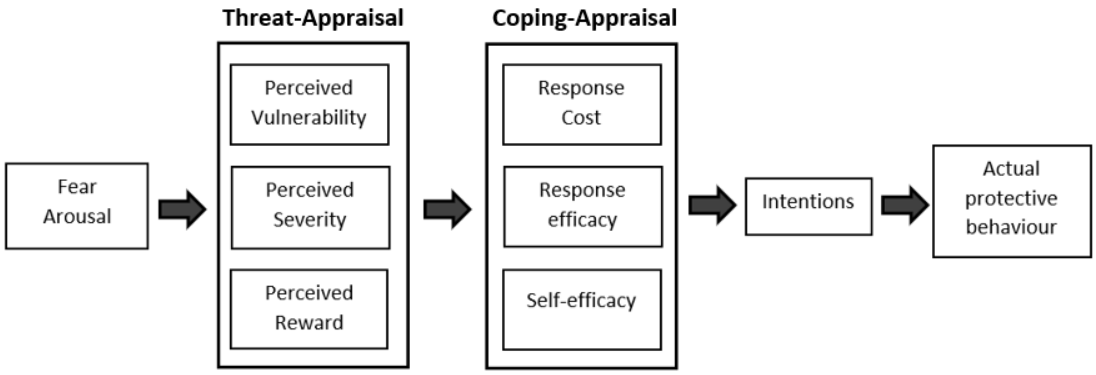

Figure 1. Diagram of Protection Motivation Theory

1. Perceived severity refers to how serious the individual views the threat or its consequences (Milne et al. 2000; Vance et al. 2012). For example, Reeves et al. (2017) found that when asked about mobile computing/IoT, employees who felt more personally at risk (e.g., of reprimand, personal data loss) were more likely to avoid behaviours that may lead to the risk event.
2. 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 and Xue 2010; Milne et al. 2000). With regards to smartphone security, this concerns a user's perception about the likelihood of their device being compromised (Verkijika 2018).
3. Perceived reward is associated with any perceived benefit to the user, such as saving time or money, that motivates them to continue or even increase their maladaptive response. This means they may disregard important protective behaviours (Vance et al. 2012).
4. Response efficacy refers to an individual's belief that the coping response or protective behaviour can help reduce 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). These can include money, time or effort required to perform protective behaviours (Milne et al. 2000)
6. Self-efficacy is an individual's level of perceived skill to perform the protective behaviour (Verkijika 2018). This can be conceptualised as ability or autonomy. Ability refers to how capable the individual feels, and autonomy refers to an individual's capacity to protect themselves against a smartphone security threat (Sommestad et al. 2015b).

Evidence suggests that PMT constructs on average account for between 34 and 50 percent of the variance in protective behaviour (Sommestad et al. 2015b; Thompson et al. 2017). For this reason, researchers have also found evidence for additional variables such as social influence (Johnston and Warkentin 2010; Lee and Larsen 2009; Tu et al. 2014). This allows for the fact that people may act safely because it is a social norm within a specific setting.

1.3 Previous research: PMT and information security

PMT has been applied to a range of information security populations (Dang-Pham and Pittayachawan 2015; Verkijika 2018), devices (Anderson and Agarwal 2010), and settings (Herath and Rao 2009; Lee and Larsen 2009; Siponen et al. 2014). The majority of research has focused on organisational contexts, and there has been some disagreement about the extent to which the findings are transferable to the personal context (Dang-Pham and Pittayachawan 2015).

It has been suggested that work and personal contexts may differ in regards to the level of personal risk, which may limit the applicability of PMT (Hovav and Putri 2016). The relevance of coping-appraisal within organisational settings have also been questioned, due to behaviours being mandatory (Sommestad et al. 2015b; Verkijika 2018). Recent criticisms are that home users do not have the same security training or support, that they rely on often inadequate 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 and Agarwal 2010; McGill and

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 compared smartphone security at 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 organisational contexts, often investigating employee compliance towards security policies. This research has commonly shown that perceived severity had a significant positive impact on employees' intention to comply with information security policies (Herath and Rao 2009; Lee and Larsen 2009; Siponen et al. 2014). Other findings are not as consistent. For example, while there is some evidence suggesting that perceived vulnerability might influence employee intentions to comply with security policies (Lee and Larsen 2009; Siponen et al. 2014), there is also evidence suggesting it is not a significant predictor (Ifinedo 2012; Vance et al. 2012). Response efficacy has been found to have the strongest effect on compliance, meaning that employees were motivated to adhere to policies if they believed there were high expected returns (Herath and Rao 2009; Ifinedo 2012; Lee and Larsen 2009). Perceived rewards have received support within organisational settings. However, Vance et al. (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 and Rao 2009; Lee and Larsen 2009; Siponen et al. 2014).

1.3.2 PMT and information security in personal settings

The findings within the personal context are more consistent. Perceived severity was found to have a significant positive relationship with security behaviours in a number of studies (Anderson and Agarwal 2010; Crossler and Bélanger 2014; Liang and Xue 2009; Martens et al. 2019). Similarly, there is consistent evidence for perceived vulnerability and response efficacy having a significant effect on protective behaviours (Anderson and Agarwal 2010; Crossler and Bélanger 2014; Hanus and Wu 2016; Liang and Xue 2010). While some studies excluded response cost as a variable of interest, as it is suggested security behaviours are not costly (Zhang and McDowell 2009), the studies that considered it found support for its inclusion (Hanus and Wu 2016; Liang and Xue 2010; Thompson et al. 2017). Self-efficacy has also had consistent support within the literature (Anderson and Agarwal 2010; Crossler and Bélanger 2014; Hanus and Wu 2016). Perceived reward was excluded as a potential variable in all the aforementioned studies.

1.3.3 PMT and smartphone security behaviours

PMT has also been used to study smartphone security behaviours, evaluating aspects such as theft or loss (Tu et al. 2014), app permissions (Kusyanti and Catherina 2018), general smartphone security (Verkijika 2018), and comparisons between smartphone and Personal Computing (PC) behaviours (McGill and Thompson 2017; Thompson et al. 2017). Perceived severity and perceived vulnerability have support within the literature (Thompson et al. 2017; Verkijika 2018), suggesting that smartphone users employ protective behaviours if they feel vulnerable to threats, and if they perceive the threat to have severe consequences. In line with other information security research, self-efficacy has the most support within the PMT smartphone literature (Kusyanti and Catherina 2018; Thompson et al. 2017; Verkijika 2018). These findings suggest that users may lack awareness in how to appropriately and effectively protect their smartphones (McGill and Thompson 2017).

1.4 Study aims

Referring to the evidence outlined throughout the previous sections, there is a substantial research gap regarding understanding smartphone user security behaviour. Most notably, there is a lack of understanding of smartphone specific security behaviours and the extent to which behaviours performed within organisations transfer to home settings. Consequently, it is important to examine and compare the behaviours of smartphone users within organisational and personal settings. For example, it is not clear whether organisational policies and procedures within the workplace transfer to personal smartphones. Therefore, the aim of this study is to understand how people behave on smartphones across contexts, and whether context influences behaviour. Specific research questions explored as part of this study were as follows: 1) to what extent do people employ the same security behaviours on smartphones regardless of context? and, 2) can PMT be used to explain this comparison?

2 Method

2.1 Participants

A total of ten (8 females, 2 males) working Australians (ranging from 34 to 56 years of age, M = 45, SD = 7.81) participated in the interviews. Participants were all employed by an Australian insurance company. All were employed full-time 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, have a smartphone supplied by the organisation to assist in their work duties, and also have a personal phone owned by the individual for use outside of work. Participants were given pseudonyms, and any identifying information was removed.

2.2 Procedure

Participants were recruited internally through the organisation (i.e., advertisements and emails). Interviews were semi-structured, with open-ended questions to avoid biased answers (Potter and Hepburn 2005). Loosely based on survey questions from Dang-Pham and Pittayachawan (2015), Thompson et al. (2017) and Verkijika (2018), the interview questions focussed to how dual smartphone owners used both devices in daily activities, the differences and similarities in use, and in regard to protective behaviours. All interviews were audio recorded and transcribed verbatim, using the orthographic method advised by Braun and Clarke (2013).

Interviews lasted between 16 and 34 minutes (M = 25.8, SD = 5.82), and data saturation, as outlined by Guest et al. (2006), was reached between the eighth and ninth interviews. A summary of the preliminary themes was emailed to the participants for review as recommended by Tracy (2010).

2.3 Analysis

Thematic analysis was used to analyse the data, combining both inductive and deductive approaches. This mixed approach enabled a robust and rigorous analysis (Fereday and Muir-Cochrane 2006), following Braun and Clarke's (2013) six-step guide. The first phase, familiarisation involved transcribing the interviews while noting preliminary themes. The next few phases involved generating initial codes, searching for and reviewing themes. This part of the analysis 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 which did not align with PMT constructs. At this stage, cross-checking of the themes with other researchers was employed, as encouraged by Pope and Mays (2005) to minimise researcher bias. Deductive analysis lead to the themes within PMT and inductive analysis identified the additional theme 'social influence', which was then named. The final stage of analysis involved 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 and Clarke 2013).

3 Results

A key overarching theme identified from the data was that people behave more safely on their work smartphones compared to on their personal smartphones. PMT was used to further explore this finding. The participants did not ultimately know why they performed protective behaviours on their work smartphones, or how the behaviours benefitted their 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. In regards to the PMT, it was found that perceived vulnerability, perceived reward, response cost and 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. using unsafe surveys without reading privacy agreements). This also included storing sensitive information on the smartphone without the correct precautions in place. 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 perceived similar severity for their work and personal devices. Perception of severity was generally based on purpose of use, and the information accessed or stored on the smartphone. For example, Cathy indicated that her personal smartphone would have more severe consequences than her work smartphone due to the personal 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.*

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 perceive the threat. 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:

> *… 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 feeling was shared by most participants who described IT support as extremely skilled, capable and able to 'shutdown' (Cathy, Dorothy, Scott, Di) or 'wipe' – otherwise known as clear – devices (Amanda, Cathy, Dorothy, Di) and 'know exactly what to do' (Dorothy, Daniella, Sam). As described by Pauline above, participants indicated that this perception of company security practices reduced the need for individuals to protect themselves.

3.3 Self-efficacy

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

> *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.*

This suggests that participants do not have skills to protect their work smartphones, but rather, there is support and stricter controls on use of smartphones. Participants did not often engage in risky behaviour on their work smartphones. This included not connecting to unsecure Wi-Fi due to supplied data plans, not engaging on social media, or downloading additional apps. The majority of the participants acknowledged they purposefully and consciously decided to behave safely on their work smartphone, as identified by Lisa:

> *… 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 from a user. Protective behaviours such as using a passcode and refraining from downloading unregistered apps were often mandatory. However, some behaviours such as backing up the device or downloading and updating anti-viral software were managed by IT, and were not the responsibility of the user, 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 security 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 … 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.*

It should be acknowledged, then, that participants commonly expressed being aware of when 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.*

Participants seemed to be aware of maladaptive behaviours and restricted these on their work devices. However, that was not the case for their personal smartphones. For example, Daniella admitted to downloading numerous apps on her personal device without reading 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 the cost associated with those good security behaviours. For example, the time required to read the terms and conditions.

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 security 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 in previous research as additional variables to supplement the explanatory power of a PMT model (Johnston and Warkentin 2010; Lee and 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 use of their work smartphones, participants used phrases such as 'being caught', '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 behaving 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 has explored aspects relating to PMT and information security behaviour. However, despite the rapid adoption of smartphones, to date, no studies had compared user security behaviour on work vs personal smartphones. Therefore, the aim of this study was to explore and compare user smartphone security behaviour in 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 was that people employed more secure behaviours on their work compared to their personal smartphones. To further explain this finding, we employed PMT and identified several important themes. The strongest themes were perceived vulnerability, need for self-efficacy, perceived reward and response cost. Also, there were no consistent significant differences regarding perceived severity and response efficacy, and finally, inductive analysis identified the role of social influence on both personal and work smartphones.

Participants generally felt that their personal devices were far more vulnerable to security threats. This finding is not surprising, with limited support for perceived vulnerability within organisational settings (Herath and Rao 2009; Ifinedo 2012; Vance et al. 2012). Participants felt less vulnerable on their work smartphones for several reasons. Firstly, participants used their work smartphones for a limited set of specific work-related functions, such as phone calls and email communication. They did not engage in risky behaviours on their smartphones due to lack of need and policy. This was also underpinned by the idea that engaging in risky behaviours was linked to punishment, rather than good protective behaviours being linked to benefits for the individual. Finally, the IT staff were responsible for the majority of the security behaviours, leaving the participant feeling safe in the hands of IT. However, participants did not have this safety-net on their personal smartphones, and frequently admitted to engaging in risky behaviour such as not reading privacy statements, and connecting to unsecure Wi-Fi.

The concept of a safety-net also influenced self-efficacy on personal smartphones. This is contrary to previous literature which identified a high need for self-efficacy within organisational settings (Herath and Rao 2009; Lee and Larsen 2009; Siponen et al. 2014; Vance et al. 2012). In this study, participants often considered themselves 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 (Butavicius et al., 2020). This meant that they did not have to practice all protective behaviours on their work smartphones, and this may have transferred to their use of their personal smartphones. It did not seem as though participants knew exactly how the organisation protected the smartphones; therefore, this limited their ability and autonomy to perform these behaviours themselves. From a practical perspective, if participants understood how the work smartphone was protected and why, this knowledge and understanding might more readily transfer to other contexts, such as how they use and engage with their personal device.

Participants often discussed perceived reward and response cost in the same manner. Despite being defined as separate components and within separate appraisal processes, these have often been operationalised as a single construct (Sommestad et al. 2015b; Thompson et al. 2017; Verkijika 2018). 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 smartphones, such as backing up data or reading privacy statements, which were considered too time consuming and inconvenient. In sum, 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, and 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 behaviours (Liang and Xue 2009). Social influence can encourage compliance due to the need for getting approval, acceptance or the fear of punishment (Liang and 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 and Larsen 2009; Liang and Xue 2009). This therefore suggests that variables such as perceived severity may have been affected by social influence.

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 it is important to note that the ultimate consequence of performing risky or maladaptive behaviours on their work smartphones would have resulted in dismissal from the workplace. The organisation had policies in place regarding 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 (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.

It must also be acknowledged that the participants within this study had participated in several technology and cyber-security training courses within their workplace. The results of this study could suggest that as a result of this training, participants behaved safely on their work smartphones, complying with policy. However, it is interesting to note that this knowledge did not transfer to their personal devices. Although employees behaved safely on their work smartphones, the lack of good behaviour performed in the personal context suggests that the training was not fully effective. 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.

4.2 Limitations and future directions

While this study has provided a useful insight into the relationship between organisational and personal smartphone security behaviours, it is not without its limitations. Firstly, the sample was limited to a single workplace, which may be subject to bias. Future research should attempt to triangulate current results, by for example considering workplaces and organisational settings, and those who specialise in smartphone security and training (Tracy 2010). It should also be noted that the interviews were based on self-report and in aid of convenience, were conducted within the workplace. It is possible then, despite being made aware of confidentiality, that participants may have 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, and discouraging participation from those who behaved poorly. It is also important to note that this organisation had effective IT support, which may not be true of all organisations.

Considering the results of this study, it is suggested that future research could focus on 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 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. Future research could focus on improving current training and education so that protective behaviours are transferred

across contexts, as users understand the benefit to their organisation as well as personal security. 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 too much information on cyber-security (Reeves et al. 2021). This should be essential in the development of successful education programs.

4.3 Conclusion

This study compared smartphone security behaviours of users on personal smartphones and work supplied smartphones. Results indicated that participants behaved safer on their work compared to their personal smartphones. 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 provided useful insight explaining the current findings, additional variables would certainly 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., and Flowerday, E. 2014. "Smartphone Information Security Awareness: A Victim of Operational Pressures," *Computers & Security* (42), pp. 56-65.

Alsaleh, M., Alomar, N., and Alarifi, A. 2017. "Smartphone Users: Understanding How Security Mechanisms Are Perceived and New Persuasive Methods," *PloS one* (12:3), p. e0173284.

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

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

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

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

Dang-Pham, D., and Pittayachawan, S. 2015. "Comparing Intention to Avoid Malware across Contexts in a Byod-Enabled Australian University: A Protection Motivation Theory Approach," *Computers & Security* (48), pp. 281-297.

Fereday, J., and 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* (5:1), pp. 80-92.

Guest, G., Bunce, A., and Johnson, L. 2006. "How Many Interviews Are Enough? An Experiment with Data Saturation and Variability," *Field Methods* (18:1), pp. 59-82.

Hanus, B., and Wu, Y. A. 2016. "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Information Systems Management* (33:1), pp. 2-16.

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

Hovav, A., and 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), pp. 35-49.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS quarterly* (34:3), pp. 549-566.

Kusyanti, A., and Catherina, H. P. A. 2018. "An Empirical Study of App Permissions: A User Protection Motivation Behaviour," *International Journal of Advanced Computer Science and Applications* (9:11), pp. 106-111.

Lee, Y., and Larsen, K. R. 2009. "Threat or Coping Appraisal: Determinants of Smb Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18:2), pp. 177-187.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS quarterly* (33:1), pp. 71-90.

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

Martens, M., De Wolf, R., and 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), pp. 139-150.

McGill, T., and Thompson, N. 2017. "Old Risks, New Challenges: Exploring Differences in Security between Home Computer and Mobile Device Use," *Behaviour & Information Technology* (36:11), pp. 1111-1124.

Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of Applied Social Psychology* (30:1), pp. 106-143.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and 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), pp. 126-139.

O'Dea, S. 2022. "Smartphone Subscriptions Worldwide 2016-2027," Statista.

Ophoff, J., and Robinson, M. 2014. "Exploring End-User Smartphone Security Awareness within a South African Context," (978:1), pp. 1-7.

Pope, C., and Mays, N. 2005. "Qualitative Methods in Health Research," in: *Qualitative Research in Health Care,* I. Holloway (ed.). Carlton, Victoria: Blackwell Publishing Ltd.

Potter, J., and Hepburn, A. 2005. "Qualitative Interviews in Psychology: Problems and Possibilities," *Qualitative Research in Psychology* (2:4), pp. 281-307.

Reeves, A., Delfabbro, P., and Calic, D. 2021. "Encouraging Employee Engagement with Cybersecurity: How to Tackle Cyber Fatigue," *SAGE Open* (11:1).

Reeves, A., Parsons, K., and Calic, D. 2017. "Securing Mobile Devices: Evaluating the Relationship between Risk Perception, Organisational Commitment and Information Security Awareness," *International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, Adelaide, Australia, pp. 145-155.

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

Rogers, R. W. 1983. "Cognitive and Psychological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in: *Social Psychophysiology: A sourcebook,* J.T. Cacioppo and R.E. Petty (eds.). New York, NY: Guilford Press, pp. 153-176.

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp. 217-224.

Sommestad, T., Karlzén, H., and 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), pp. 26-46.

Sommestad, T., Karlzén, H., and Hallberg, J. 2015b. "The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance," *Information & Computer Security* (23:2), pp. 200-217.

Thompson, N., McGill, T. J., and Wang, X. 2017. "“Security Begins at Home”: Determinants of Home Computer and Mobile Device Security Behavior," *Computers & Security* (70), pp. 376-391.

Torre, I., Sanchez, O. R., Koceva, F., and Adorni, G. 2018. "Supporting Users to Take Informed Decisions on Privacy Settings of Personal Devices," *Personal and Ubiquitous Computing* (22:2), pp. 345-364.

Tracy, S. J. 2010. "Qualitative Quality: Eight “Big-Tent” Criteria for Excellent Qualitative Research," *Qualitative Inquiry* (16:10), pp. 837-851.

Tu, Z., Yuan, Y., and Archer, N. 2014. "Understanding User Behaviour in Coping with Security Threats of Mobile Device Loss and Theft," *International Journal of Mobile Communications* (12:6), pp. 603-623.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3-4), pp. 190-198.

Verkijika, S. F. 2018. "Understanding Smartphone Security Behaviors: An Extension of the Protection Motivation Theory with Anticipated Regret," *Computers & Security* (77), pp. 860-870.

Wang, Y., Chen, Y., Ye, F., Liu, H., and Yang, J. 2019. "Implications of Smartphone User Privacy Leakage from the Advertiser's Perspective," *Pervasive and Mobile Computing* (53), pp. 13-32.

Zhang, L., and 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), pp. 180-197.