https://doi.org/10.48009/2_iis_2020_279-288

Issues in Information Systems
Volume 21, Issue 2, pp. 279-288, 2020

THE INFLUENCE OF COGNITIVE FACTORS AND PERSONALITY TRAITS ON MOBILE DEVICE USER'S INFORMATION SECURITY BEHAVIOR

Nils Lau, Nova Southeastern University, nils@nova.edu
Ling Wang, Nova Southeastern University, lingwang@nova.edu
Inkyoung Hur, Florida Atlantic University, ihur@fau.edu
Marlon Clarke, Nova Southeastern University, mrclarke@nova.edu

ABSTRACT

As individuals have become more dependent on mobile devices to communicate, to seek information, and to run business, their susceptibility to various threats to information security has increased. Although research has investigated user's information security intention in recent years, not enough is currently known about how cognitive factors and personality traits impact the adoption and use of mobile device security technologies. The purpose of this research was to empirically investigate the influence of cognitive factors and personality traits on mobile device user's intention to use mobile device security technologies. A research model was developed by combining constructs from both the Protection Motivation Theory (PMT) and the Big Five Factor Personality Traits. Partial Least Square Structural Equation Modeling (PLS-SEM) was used to analyze web-based survey data gathered from a total of 356 mobile device users. The findings of this study show that perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, and mobile self-efficacy have a significant positive effect on user's intention to use mobile device security technologies. Except for the trait conscientiousness, the personality traits were not found to significantly influence user's intention to use mobile security technologies.

Keywords: Protection Motivation Theory (PMT), Personality Traits, Information Security (IS), Mobile Devices, and Data Breach.

INTRODUCTION

The pervasiveness of mobile devices and their growing importance for personal and business use have created unique challenges for information security research. Although mobile device usage has numerous benefits, its connectivity to the internet brings many security threats to mobile device users (Xu et al., 2016). As highlighted by Tu et al. (2015), mobile devices are more susceptible to data breaches than traditional computing systems as their mobility means data is carried everywhere and connected to different insecure networks. To protect against these security threats, it is important that mobile device users have the intent to adopt secure technologies and actually use them. Mobile device users are still considered to be the weakest link in the defense against existing information security threats as their actual security behavior often differs from intended behaviors (Shropshire et al., 2015; Uffen et al., 2013). While previous research has found user's intention to be a significant antecedent of information security technology adoption, the user's intention still covers only a small amount of variance in the actual security behavior (Matt & Peckelsen, 2016; Giwah et al., 2019). As a substantial part of the variance remains unexplained, other factors do notably influence the user's intention to use information security technologies. In the context of mobile device security behavior, such as data backup, biometric protection, and password protection, it is evident that a great percentage of mobile device users have the intent to use mobile technologies in safe ways, but only some of these mobile device users may act on this intent.

Theoretical Background

Previous studies have made contributions to predictions of user's security intentions; however, most studies lack an explicit inclusion of actual security usage as a dependent construct in their models. In exploring the actual adoption of mobile device security technologies as a dependent construct to explain mobile device user security behaviors, this study adds to the body of knowledge on mobile device use and information security behaviors. According to Burns et al. (2017), protection motivation theory (PMT) uses behavioral intention as a proxy for actual security behavior. They point out many studies are derived from the theory of planned behavior (Ajzen, 1985), which has behavioral intention as the primary driver of observed actual behavior. But while behavioral intentions are generally well correlated with

security behaviors, as revealed by Boss et al. (2015), relatively few studies have investigated the actual user's security behavior.

PMT (Rogers, 1975; Rogers, 1983), as a framework, postulates that the motivation to protect oneself from danger is related to the subject's cognitive belief in the following aspects: the severity of the threat, the susceptibility of the threat, the effectiveness of coping response in preventing the threat, the cost of response, and the ability to execute the coping response. The rationale for leveraging the PMT was its potential to provide a theoretical explanation on the cognitive processes individuals undergo when faced with security threats. However, the use of mobile device security technologies is not only cognitively governed. Therefore, this study sought to place a stronger emphasis on the personality factors to explain mobile user's intention to adopt mobile device security technologies.

One emerging area of interest in applying behavioral science theories to understand user security behaviors has to do with personality traits. Personality traits refer to a stable set of characteristics that determine the differences in individuals' thoughts, feeling, and actions (Goldberg, 1992). Due to its importance for human cognition and behavior, researchers have integrated personality traits to assess personality differences within the information security domain. There is considerable agreement in the literature that personality can be represented by five constructs (Matt & Peckelsen, 2016), all of which have been integrated into the Big Five-Factor Model (BFFM). The BFFM clusters all personality traits into five constructs: conscientiousness, extraversion, neuroticism, intellect, and agreeableness. The rationale for leveraging these personality traits is in the potential to explain differences between human beings, and to show how certain measurable traits exhibited by those human beings can be used to understand and guide mobile device security behavior. Building on PMT, this study integrated a comprehensive concept that accounts for user's perceived threats of mobile device data breaches and their belief in the measures that could be taken to alleviate these threats. In addition, the personality traits provided a picture of the individual differences that are germane in the usage decision.

Hypothesis Development

Figure 1 shows a research model of cognitive factors and personality traits that may affect intention to use mobile device security technologies. This research model consists of twelve constructs; perceived threat severity (TSE), perceived threat susceptibility (TSU), perceived response costs (RC), response efficiency (RE), mobile self-efficacy (MSE), mobile device user intention (MDUI), extraversion (EXTRA), agreeableness (AGREE), conscientiousness (CONS), neuroticism (NEURO), intellect (INTEL), and mobile device security usage (MDSU). We used the five cognitive factors defined in Posey et al. (2015). TSE was defined as the perceived seriousness of the consequences of falling victim to a mobile device security threat. TSU refers to the perception of the likelihood of becoming a victim of a mobile device security threat. RC refers to any costs perceived to be incurred by the adoption of protective behaviors against a mobile device security threat. RE was defined as the belief that recommended behaviors will be effective in mitigating a mobile device security threat. MSE refers to an individual's belief in their own ability to perform the recommended behaviors to protect against a mobile device security threat. McCrae and Costa (1997) defined the five human personality traits as follows: EXTRA: do not mind being the center of attention. AGREE: sympathize with others' feelings. CONS: pay attention to details. NEURO: get stressed out easily. INTEL: quick to understand things. Lastly, MDUI was defined as an individual's willingness to adopt mobile device security technologies, while MDSU represent the actual usage of these technologies.

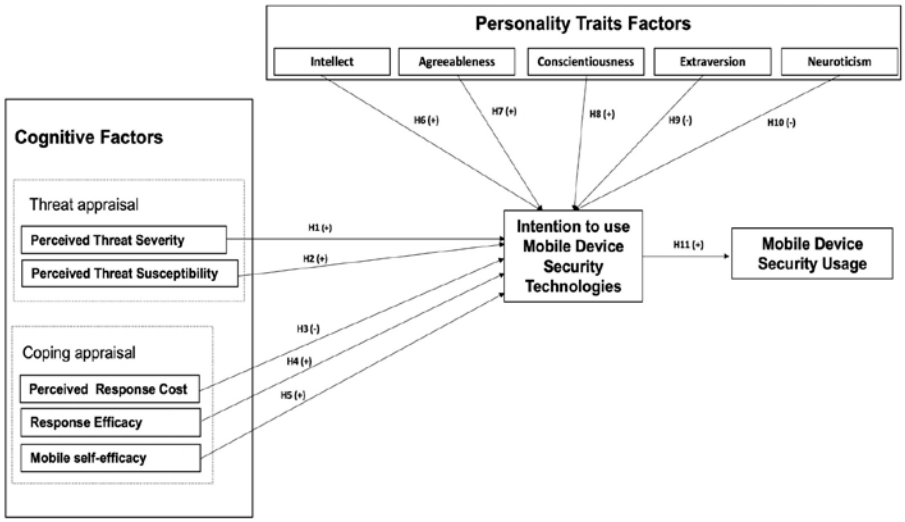

Figure 1. Research Model for Mobile Device Security Usage

Threat Appraisal Factors

The positive effect of perceived threat severity and susceptibility on behavioral intention has been widely supported in the literature (Alsaleh, Alomar, & Alarifi, 2017; Woon et al., 2005). For instance, Woon et al. (2005) explored the cognitive psychological factors that influence the decision of home wireless network users to implement security features on their wireless networks, and they found that perceived threat severity was a significant factor in determining if a user running a home wireless network will enable security measures. Furthermore, Gutteling et al. (2017) suggested that when users perceive high threat susceptibility, they are motivated to undertake adaptive responses that will protect them from the threat. While most previous studies have concluded that threat severity and susceptibility were an important predictor of security-related protection, some other studies, such as the study by Mwagwabi et al. (2018), have found that threat appraisal factors were not significant predictors of behavioral intention. This highlights the need for more research around this domain to understand how the threat appraisal factors may influence intentions and the usage of mobile device security technologies. Thus, we hypothesized:

H1. Perceived severity positively influences the intention to use mobile device security technologies.
H2. Perceived susceptibility positively influences the intention to use mobile device security technologies.

Coping Appraisal Factors

Previous studies have confirmed the negative relationship between response costs and the intentions to perform protective behaviors against security threats. For instance, Chenoweth et al. (2009) found a negative relationship between response costs and the intention to use anti-spyware software. According to Crossler and Belanger (2014), response cost drives users toward maladaptive responses. It reduces the desire of users to adopt protective behaviors (Posey et al., 2015). In addition, Rogers (1975) posited that if the response cost of performing a behavior is high, then it hinders the performance of adaptive responses. Hence, we hypothesized:

H3. Response cost negatively influences the intention to use mobile device security technologies.

PMT proposes that response efficacy and self-efficacy positively influence the intention to perform protective behaviors (Doane et al., 2016; Tsai et al., 2016). For instance, Boss et al. (2015) found moderate to high levels of response efficacy were positively associated with the intention to use anti-malware software. Giwah et al. (2019) also found a positive relationship between response efficacy and protection motivation in the context of data breaches. The findings of the research studies suggest that an increase in a user's response efficacy for the recommended protective behaviors against mobile device security threats would result in an increase in their intention to use mobile device security technologies. Prior studies have also found self-efficacy (Thompson et al., 2017) as well as mobile self-

efficacy (Giwah et al., 2019; Keith et al., 2015) to be the strongest predictor of information security behavioral intentions. Therefore, as an individual's response and self-efficacy increases, so should their intention to perform protective behaviors. We therefore proposed the hypotheses:

H4. Response efficacy positively influences the intention to use mobile device security technologies.
H5. Mobile self-efficacy positively influences the intention to use mobile device security technologies.

Personality Traits Factors

According to Xu et al. (2016), users high on the intellect trait are more likely to become innovators and early adopters of new technologies and services than other personality traits. Given that mobile device security technologies are still niche products (Matt & Peckelsen, 2016), intellectually inclined individuals have a higher interest in adopting mobile device security technologies. A study conducted by Farhadi et al. (2012) on the relationship between personality traits and deviant work behavior found that agreeable individuals were less likely to be involved in deviant work behavior. Mount, Ilies, and Johnson (2006) and Salgado (2002) also found there is a negative relationship between agreeableness and deviant behavior. According to Matt and Peckelsen (2016), an agreeable individual is more likely to follow the rules even if their behavior is not monitored. Thus, an agreeable individual is considered more likely to follow information security policies and be aware of the impact that a compromised system will have on the organizations' resources.

Conscientious individuals are likely to take control of and protect their personal information, since they tend to be aware of the dangers associated with security breaches (Korzaan & Boswell, 2008). For instance, Pattinson et al. (2015) examined the relationship between non-malicious computer-based behavior and personality traits, and concluded that conscientious individuals were less prone to risky computer-based behaviors. Shropshire et al. (2015) found a significant positive association between the conscientious personality trait and security intentions, and suggested that conscientious individuals tend to stick to established procedures and experience discomfort when deviating from familiar paths. Consequently, mobile device users who possess the conscientiousness trait would be highly open to use mobile device security technologies in order to protect themselves against potential threats. Based on these arguments and the noted positive association between intellect, agreeableness, conscientiousness, and intention to use mobile security technologies, the below hypotheses were developed:

H6. Intellect positively influences the intention to use mobile device security technologies.
H7. Agreeableness positively influences the intention to use mobile device security technologies.
H8. Conscientiousness positively influences the intention to use mobile device security technologies.

Since extroverted individuals tend to be more involved in opportunities to provide and obtain information in specific situations, they see information security polices as a barrier that prevents the exchange of information. Extroverted individuals also tend to live an action-oriented life that includes taking high risks (Uebelacker & Quiel, 2014). This suggests that extroverted individuals who score high on extraversion will be less likely to initiate the usage of mobile device security technologies. Furthermore, individuals who reveal neuroticism traits tend to score lower on the attitude toward cyber security behavior. The distrust inherent in neurotic individuals makes them more likely to regard security measures with skepticism, hence forming negative attitudes because of the belief that a potential action cannot make a significant difference in protecting their mobile device (Uffen et al., 2013). Thus, we hypothesized:

H9. Extraversion negatively influences the intention to use mobile device security technologies.
H10. Neuroticism negatively influences the intention to use mobile device security technologies.

Intention

While PMT has been applied to user's information security behavior (Boss et al., 2015; Crossler & Belanger, 2014; Giwah et al., 2019), only a small number of studies have used actual behavior as the dependent variable (Giwah et al., 2019; Matt & Peckelsen, 2016; Thompson et al., 2017). Measuring intention rather than actual behaviors can be troublesome as intention does not always lead to actual behavior (Giwah et al., 2019). There is ample evidence in the literature that supports the significant positive association between security intentions and actual security behavior (Tu et al., 2015; Verkijika, 2018; Xu et al., 2016). Therefore, this study hypothesized that:

H11. Mobile device security intentions positively influence the actual usage of mobile device security technologies.

RESEARCH METHODOLOGY

Research Design

This study utilized a quantitative approach to assess how cognitive factors and personality traits influence the usage of mobile device security technologies. Prior to conducting the survey for the main data collection, a Delphi study was conducted with 11 subject matter experts familiar with mobile device security technologies. The Delphi method ensures both reliability and validity as it exposes the study to a panel of differing, and often contradictory, opinions while seeking consensus through subject matter experts' feedback. The survey was also pilot tested with 20 participants in order to examine its usability and identify potential problems with the study.

Development of Instrument

The survey instrument for this study was developed from previously validated, established, and well-accepted instruments. This study used a web-based survey instrument to collect quantitative data on the independent variables (TSE, TSU, RC, RE, MSE, EXTRA, AGREE, CONS, NEURO, INTEL, MDUI) and the dependent variable (MDSU) based on prior measures validated information security research. This study utilized the measures proposed by Claar and Johnson (2012), Boss et al., (2015), and Woon et al. (2005) to assess the PMT constructs and actual usage of mobile device technologies. The validated measures of the International Personality Item Pool (IPIP) 50-item questionnaire instrument of Goldberg (1992) was used to assess the personality traits. The IPIP scales was scored by assigning a value of 1 to 5 to the item's responses. Once numbers were assigned for all the items in the scale, all the values were added to obtain a total scale score. Finally, Uffen et al. (2013) and Shropshire et al. (2015)'s validated, and reliable measures of behavior intention was revised and used in this study to measure the mobile device user intention and behavior.

Data Collection

To test the research model and the associated hypotheses, we collected survey data from mobile device users. The participants were representative of the target demographic population, that is, mobile device users within the United States, 18 years or older, who have been using their mobile devices to access the internet for at least one year. Emails soliciting participation were directly sent to neighbors, work colleagues, and friends. Following the Mahalanobis distance multivariate analysis, two cases were removed for demonstration of outliers. Therefore, a total of 356 responses were kept for the data analysis.

RESULTS

Testing the Measurement Model

Cronbach's alpha and average variance extracted (AVE) in SmartPLS 3.0 were used as measures of internal reliability and convergent validity, respectively. The Cronbach alpha's and composite reliability coefficients of 0.7 or higher was used to suggest internal reliability and AVE values of at least 0.5 as acceptable validity (Hair et al., 2014). Results show that both the Cronbach's alpha and composite reliability values exceed the 0.7. Therefore, high levels of internal consistency reliability have been confirmed among all the latent variables. According to Hair et al. (2014), indicators with outer loadings between 0.4 and 0.7 should be considered for removal only when deleting the indicators leads to an increase in AVE. After eliminating the outer loading below than or equal to 0.4, the AVE revealed that ten out of the twelve latent variables were found to be equal to or greater than the minimum acceptable value of 0.5. Another aspect of validity that needs assessment is discriminant validity, defined as the extent to which a construct is truly distinct from other constructs (Hair et al., 2014). This study used the Fornell and Larcker (1981) criterion for assessing the discriminant validity. This approach shows that the squared root of each construct AVE was higher than the correlation with other variables. Given these results, adequate reliability, convergent, and discriminant validity of the instrument can be assumed.

Testing the Structural Model

Three hundred fifty-six sets of survey data were analyzed using Partial Least Square (PLS) with SmartPLS 3.0. As a sub-type method of structural equation model, PLS is widely used in information systems research (Hair et al., 2014). Results of the standardized PLS path coefficient model for the proposed theoretical model are presented in Figure 2. The numbers that are noted above the arrows represent the path coefficients (β), while the R^2 values are noted within the given constructs where R^2 is applicable. Path coefficients are used to estimate the strengths of the relationship between the constructs in the model, while R^2 is a measure of the predictive accuracy of the model (Hair et al., 2014). Path coefficients have range values between -1 and +1, with values that are closer to +1 indicating strong positive relationships, values closer to -1 depicting strong negative relationships, and values that are closer to zero indicating weak relationships (Hair et al. 2014). R^2 values of 0.75, 0.50, and 0.25 have been classified as substantial, moderate, and weak, respectively, and indicate that the amount of variance in the dependent variables can be explained by the independent variables (Hair et al., 2014).

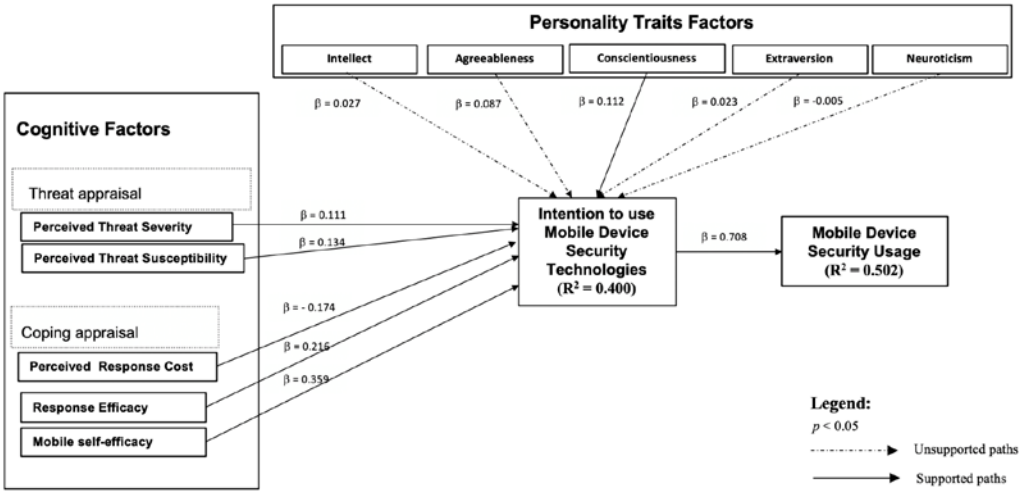

Figure 2. Results of the PLS analysis

As shown in Figure 2, the coefficient of determination, R^2, is 0.400 for MDUI and 0.502 for MDSU latent variables. This means that personality factors (EXTRA, AGREE, CONS, INTEL, and NEURO) as well as cognitive factors (TSE, TSU, RC, RE, and MSE) moderately explain 40% of the variance in MDUI, while MDUI moderately explains 50.2% of the variance in MDSU. The path coefficient values suggested that MDUI has the strongest effect on MDSU (β = 0.708). Additionally, MSE has the strongest effect on MDUI (β = 0.359), followed by RE (β = 0.216) and RC (β = -0.174). Many of the paths had very low path coefficients such as EXTRA (β = 0.023), AGREE (β = 0.087), INTEL (β = 0.027), and NEURO (β = - 0.005). These low values indicate weak positive relationships for the paths with positive values and weak negative relationships for the paths with negative values.

The SmartPLS 3.0 tool also generates t-statistics for significance testing of both the inner and outer model, using a procedure called bootstrapping. Figure 2 shows the results of the bootstrapping analysis with 500 re-sampling used to test the significance of the hypothesized relationships in this study. Based on the path analysis and bootstrapping results, TSE (β = 0.111, p = 0.027) and TSU (β = 0.134, p = 0.049) have significant positive associations with MDUI. Thus, **H1** and **H2** were fully supported. RC (β = -0.174, $p < 0.001$) is negatively related to MDUI, hence, the data analysis results full support for **H3**. In contrast, RE (β = 0.216, $p < 0.001$) as well as MSE (β = 0.359, $p < 0.001$) are positively related to MDUI. Thus, **H4** and **H5** were fully supported. The analysis results also showed that personality factor INTEL (β = 0.027, $p > 0.05$) surprisingly had no significant effect on MDUI. Similarly, AGREE (β = 0.087, $p > 0.05$) did not show to have a significant effect on MDUI. Nevertheless, the personality factor CONS (β = 0.112, *p=0.02*) had a significant positive contribution on MDUI. Thus, **H6** and **H7** were not supported, while **H8** was supported. The effect of EXTRA (β = 0.023, $p > 0.05$) on MDUI was non-significant. Hence, **H9** was not supported.

Interestingly, NEURO (β = -0.005, $p > 0.05$) also had no significant effect on MDUI. This implies that the path relationship between NEURO and MDUI, **H10,** was not supported. The model further suggested that MDUI (β = 0.708, $p < 0.001$) had a significant and direct positive effect on MDSU. Thus, **H11** was supported.

DISCUSSIONS AND CONCLUSIONS

Discussions of the Findings

The first research question incorporated the PMT predictors of behavior in the form of threat severity, threat susceptibility, response costs, response efficiency, and mobile self-efficacy, and their influence on the mobile device user's intention to use mobile device security technologies. Based on the data analysis, mobile device user intention was positively influenced by perceived threat severity. As perceived severity increases, mobile device users are more likely to adopt mobile device security technologies. This finding is consistent with Alsaleh et al. (2017) and Woon et al. (2005). The findings of this study suggest that perceived threat susceptibility is a necessary factor for mobile device users to adopt mobile device security measures. Furthermore, the results of this study show that response cost has a significant negative contribution on mobile device user intention. This finding is consistent with previous literature that suggests that perceived response costs in terms of effort, time, and money influence the intention of adopting protective behaviors against information security threats (Boss et al., 2015; Burns et al., 2017; Posey et al., 2015). Thus, it can be inferred from this study's findings that an increase in response costs results in a decrease in the intention to perform recommended protective behaviors.

This study shows that response efficacy has a significant positive contribution on intention to use mobile device security technologies. Interestingly, mobile self-efficacy not only had a significant positive contribution on mobile device user intention, but also was the strongest predictor of intention. Prior research has also found mobile self-efficacy to be the most significant factor in explaining security behavior in the context of mobile devices (Giwah et al., 2019; Keith et al., 2015; Posey et al., 2015). Similarly, Thompson et al. (2017) as well as Verkijika (2018) suggest that self-efficacy is the strongest predictor of information security intentions of both home computer and mobile devices. The finding of this study is consistent with such studies and indicates that an increase in an individual's self-efficacy in using the recommended mobile device security technologies against security threats should result in an increase in their intention to use these protective technologies.

The second research question incorporated the five personality traits constructs and their influence on the mobile device user's intention to use mobile device security technologies. Our data analysis results showed that there were no significant effects of any personality traits on mobile device user's intention except for conscientiousness. As proposed, conscientiousness had a significant positive contribution on intention. This implies that within the context of mobile device security usage, individuals that score high in terms of the degree of their conscientiousness would be more likely to adopt mobile protective technologies.

The third and final research question examined the role of intention as a predictor of actual mobile device security usage. The results of the study suggested that actual mobile device security usage is significantly influenced by the user's intention to adopt mobile device security technologies. The existing literature supports this finding. According to Posey et al., (2015), the impact of intention on behavior is not only significant, but positively so. Giwah et al. (2019), citing Rogers (1983), asserts that when threat and coping appraisals are at moderate to high levels, an individual's intention is equally increased, thereby significantly influencing actual behavior.

Implications for Research/Practice

Theoretically, this study adds to the body of knowledge on the factors that influence the adoption of mobile device security technologies. The findings of this study brought clarity on the cognitive factors and personality trait differences that lead to the actual usage of mobile device security technologies by mobile device users. Furthermore, this study is one of the few that combines the PMT factors and personality traits into a single research model within the context of mobile device security usage.

The findings of this study also offer practical implications. First, our results identified that coping appraisal factors were the best determinant of intentions, and subsequently the usage of mobile device security technologies. This implies that any efforts to increase a user's belief in the effectiveness of a protective behavior against mobile device threats (Response Efficacy), and their confidence in performing these behaviors (Mobile Self-Efficacy), as well as reducing the perceived costs to perform these behaviors (Response Costs), would increase a user's intention to perform these behaviors. This would encourage the actual usage of mobile device security technologies. One recommendation is for training materials and resources relating to mobile device security threats to include recommended behaviors that are perceived to be effective, and that a user feels confident enough to perform themselves. This would work towards increasing the user's response efficacy and mobile self-efficacy, respectively. In addition, information presented to users should also emphasize the small costs required to use the recommended protective behaviors against mobile device threats, particularly in comparison to the potentially large costs of becoming a mobile device data breach victim.

Despite prior literature (Gratian et al., 2018; Matt & Peckelsen, 2016; Uffen et al., 2013; Xu et al., 2016), this study found that the personality traits agreeableness, extraversion, intellect, and neuroticism have no significant influence on mobile device security usage. Since the model did not find these traits significant on the mobile device users' intentions to use security technologies, a possible practical recommendation of this study is for an organization to take the position that employees of all age groups, regardless of personality traits, may be susceptible to risky behavior in the context of data breaches. This reinforces the need for organization-wide security training of all employees and for information security policies and procedures.

Limitations

There is a limitation to this study. It relates to the fact that this study measured self-reported data. Self-reported data entail certain risks to validity, including self-selection biases, problems with accuracy, and the individual participant's desire to be viewed in a positive way (Rosenbaum et al., 2006). A further limitation of self-reported data is the inability of the researcher to verify the honesty of the participant. Finally, due to the survey being close to a hundred questions, it is possible that random clicking, fatigue, or failures to carefully read questions affected the accuracy of the responses. As such, caution should be exercised when generalizing the results from this study.

Conclusions

This study provides further evidence that PMT cognitive factors have a significant positive effect on user's intention to use information security technologies. In particular, mobile self-efficacy has the strongest effect on the intention to use mobile device security technologies. Most of the personality traits factors were not found to be significant, except for conscientiousness. The user's intention to use mobile device security technologies was found to have a significant effect on the actual usage of mobile device security technologies. Hence, the results support the suitability of the use of PMT and personality factors in the mobile device security technologies context. This study has contributed to information security literature by providing empirical results on factors that influence the use of mobile device security technologies.

REFERENCES

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. Springer, Berlin, Heidelberg.

Alsaleh, M., Alomar, N., Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS One*, 12(3), 1-35.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864.

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68*, 190-209.

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii International Conference on Systems Science*, Big Island, HI, 1-11.

Crossler, R. E., & Belanger, F. (2014). An extended perspective on individual security behaviors: Protection Motivation Theory and a Unified Security Practices (USP) instrument. *The Database for Advances in Information Systems, 45*(4), 51-71.

Doane, A., Boothe, L., Pearson, M., & Kelley, M. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computer in Human Behavior, 60*, 508-513.

Farhadi, H., Fatimah, O., Nasir, R., & Shahrazad, W. S. (2012). Agreeableness and conscientiousness as antecedents of deviant behavior in workplace. *Asian Social Science*, *8*(9), 1-6.

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.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 18*(1), 39-50.

Giwah, A.D., Wang, L., Levy, Y., & Hur, I. (2019). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital*, 1469-1930.

Goldberg, L. R. (1992). The development of markers for the Big-Five factor structure. *Psychological Assessment, 4*(1), 26–42.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security, 73*, 345-358.

Gutteling, J. M., Terpstra, T., & Kerstholt, J. H. (2017). Citizens' adaptive or avoiding behavioral response to an emergency message on their mobile phone. *Journal of risk research*, 1466-4461.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publications.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile- computing self-efficacy in consumer information disclosure. *Information Systems Journal, 25*(6), 637-667.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems, 48*(4), 15-24.

Matt, C., & Peckelsen, P. (2016). Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior. *Proceedings of the 49th International Conference on System Sciences (HICSS)*, Hawaii, USA, 4832-4841.

McCrae, R., & Costa, P. (1997). Personality trait structure as a human universal. *American Psychologist, 52*(5), 509-516.

Mount, M., Ilies, R., & Johnson, E. (2006). Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction. *Personnel Psychology, 59*(3): 591-622.

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems, 42*, 147-182.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security Behavior: An Australian Web-based study. *In Proceedings of the third human international conference on human aspects of information security, privacy, and trust*. Springer International Publishing, New York, NY, USA.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114.

Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York: Guilford Press.

Rosenbaum, A., Rabenhorst, M. M., Reddy, M. K., Fleming, M. T., & Howells, N. L. (2006). A comparison of methods for collecting self-report data on sensitive topics. *Journal of Violence and Victims, 21*(4), 461-71.

Salgado, J. F. (2002). The Big Five personality dimensions and counterproductive behaviors. *International Journal of Selection and Assessment, 10*, 117-125.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Explaining initial adoption of information security behavior. *Computers & Security, 49*(0), 177-191.

Thompson, McGill, & Wang. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. *Computer & Security, 70*, 376-391.

Tsai, H., Jiang, M., Alhabash, S., LaRose, R., Rifon, N., & Cotton, S. (2016). Understanding online safety behaviors: a protection motivation theory perspective. *Computer & Security, 59*, 138-150.

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), 506-517.

Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. *IEEE Workshop on Socio-Technical Aspects in Security and Trust*, 24-30.

Uffen, J., Kaemmerer, N., & Breitner, M. H. (2013). Personality traits and cognitive determinants-An empirical investigation of the use of smartphone security measures. *Journal of Information Security, 4*(4), 203-212.

Verkijika, S.P. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computer & Security, 77*, 860-870.

Woon, I., Tan, G., & Low, R. (2005). A protection Motivation Theory Approach to Home Wireless Security. *Proceedings of International Conference of Information Systems*, 31, 367-380.

Xu, R., Frey, R. M., Fleisch, E., & Ilic, A. (2016). Understanding the impact of personality traits on mobile app adoption Insights from a large-scale field study. *Computers in Human Behavior, 62*, 244-256.