What motivates teenagers to comply with security guidelines?

Full paper

Florence Mwagwabi
Discipline of Information Technology,
Mathematics & Statistics
Murdoch University
Singapore, 169662
Email: f.mwagwabi@murdoch.edu.au

Jhee Hee Jiow
Health and Social Sciences Cluster
Singapore Institute of Technology
Singapore 138683
Email: jhee.jiow@singaporetech.edu.sg

Abstract

We examined factors that inspire teenagers to comply with cyber security guidelines. We used protection motivation theory (PMT), and extended the model to include personal norms and normative beliefs. For teenage computer users, believing they are susceptible to hacking or that the consequences of being hacked would be severe, had no bearing on their password choices. This is an interesting finding highlighting a potential difference between adults and teenagers. We found personal norms is a better predictor of teenagers' security behaviour than PMT's threat perceptions. This is an important finding which opens new avenues for future research, particularly in explaining teenagers' security behaviour. This study contributes to finding ways to improve security practices at an early age. To the best of our knowledge this is the first password security study that applies PMT to examine security behaviours in teenagers.

Keywords: protection motivation theory, teenagers cyber security behaviour, compliance behaviours in teenagers, password compliance intention, social media password practices, normative beliefs, personal norms, anticipated guilt.

1 INTRODUCTION

Most children have been exposed to at least one cyber risk (DQ-Institute 2018). Children in the teenage age-group (13 to 18), have access to all the Internet has to offer (DQ-Institute 2018; Tsirtsis 2016). This raises the question: to what extent are children exposed to cyber risks? DQ-Institute (2018), conducted a global study of more than 80,000 children in an attempt to answer this question. Exacerbated by a constant cell-phone and social media usage, exposure to cyber risks in children is growing exponentially, the study found. Globally, almost 60% of children as young as eight are exposed to some form of cyber threats including cyberbullying, game addiction and online sexual behaviour. Interestingly, even a major survey such as DQ-Institute (2018), does not mention children's exposure to computer security risks such as malware, phishing or password threats.

Surveys on cyber risks in teenagers focus on risks such as, interacting with strangers (e.g., DQ-Institute 2018; Soh et al. 2018), problematic internet use (e.g., Anderson 2017; Soh et al. 2018), adult content (Cybersafe.org 2016), cyber-bullying and online harassment (e.g., DQ-Institute 2018; Lwin et al. 2012). Yet, few studies explicitly cite cyber security threats (Tsirtsis 2016).

We identify three gaps in the literature related to cyber risks in teenagers. First, research on how to inspire better cyber security practices in teenagers is lacking. To address this gap, we examine factors that inspire teenagers to comply password guidelines on social media. Secondly, theory grounded studies in this area is also lacking. We address this gap by applying PMT to investigate teenagers' compliance with password security guidelines. Given that parents and peers also play a role in teenagers' risky behaviours (ACMA 2011; Soh et al. 2018), we extend PMT to investigate the role of parents and peers in teenagers' compliance with security guidelines.

Lastly, theory grounded research on cyber security behaviour focuses on adults. To address this gap, we use PMT (Rogers 1983), to understand teenagers' protection motivation on social media. We have chosen teenagers as our target population and Facebook as the proxy for social media. This is because teenagers are more active on social media and while Instagram, YouTube and Snapchat usage is increasing, Facebook is still widely used by teenagers globally (ACMA 2016; DQ-Institute 2018; Ofcom 2018). Further, teenagers are more likely to share a lot more personal information on Facebook (ACMA 2011), hence more likelihood of exposure to cyber security threats on the Facebook platform.

Investigating teenager cyber behaviour internationally is challenging because of different study methodologies and varying teenage age-group categorization. For example, in the surveys described in ACMA (2016), on teen internet use, the data in Australia was collected from 14-17 olds, US from 12-17 and UK from 12-15 year olds. In this paper, we describe a teenager as a person who falls within the ages of 13-18 years.

While we seek to examine security behaviours in teenagers, it is important to address some key characteristics unique to teenagers. These may determine how teenagers perceive security and motivate them to comply with security guidelines. Understanding cybersecurity behaviours in teenagers is complicated by the fact that, the teenage phase is when parents and peers have a strong influence on risky behaviour (Soh et al. 2018). Siblings play a significant role in teenagers' social media use (ACMA 2011). While parents play a role, peer influence is typically stronger (ACMA 2011; Soh et al. 2018). We therefore examine how social influence plays a part in teenagers' cyber security behaviour.

PMT (Rogers 1983), is used InfoSec to investigate users' underlying security perceptions, and what inspires better security practices (e.g., Johnston et al. 2015; Posey et al. 2015). While PMT, originally used in health-related context, is used to investigate protection behaviours in all age groups (Lwin et al. 2012), applications of PMT in IS security studies have focused on the adult population. That is, the studies have implicitly assumed that the participants displayed some level of maturity needed to process IS security related sanctions and threats. As teenagers and adults are in different cognitive developmental stages (Lwin et al. 2012) and as PMT requires some level of cognitive processing of threats (Rogers 1983), we expect adults and teenagers to differ in their threat appraisal. This study therefore raises the question of whether PMT can explain security compliance behaviours in teenagers and whether teenagers' threat and copping appraisal display the same level of maturity as adults.

As young people are exposed to the internet from a very young age, understanding security threat perceptions among teenagers is important (Tayouri 2015). Teenagers are aware of the importance of cyber safety education (ACMA 2011) and acknowledge that they do receive cyber safety training at school and home (Cybersafe.org 2016). Yet, teenagers exhibit poor security practices, as ACMA (2013) reveals, most teenagers share their social media passwords with parents, siblings and friends. Understanding the underlying factors that lead to poor password practices is important because online usernames and

passwords are more valuable compared to stolen credit card information (Ablon et al. 2014). Furthermore, poor security practices have serious implications beyond an individual's personal online accounts (Jenkins et al. 2014). Thus, our proposed study should contribute to finding ways to improve security practices at an early age.

2 LITERATURE REVIEW

PMT predicts protection motivation on an individual level (e.g., Mwagwabi et al. 2018; Thompson et al. 2017) and in organizations (e.g., Crossler et al. 2014; Posey et al. 2015).We address the question of whether PMT (Rogers 1983) can be used to predict security behaviour in teenagers. We first examine how security perceptions and perceptions about security recommendations influence behaviours and if PMT can predict protective behaviour in teenagers.

2.1 PMT theoretical background

PMT was developed to explain health behaviour. Rogers (1983), identified three variables: perceived severity and perceived susceptibility to threat, and response efficacy as predictors of protection motivation, operationalized as behavioural intentions. Bandura's (1982) work on self-efficacy inspired the extension of PMT (Rogers 1983), to include self-efficacy as a predictor of protection motivation.

PMT suggests perceived severity, the assessment of severity of threat and perceived vulnerability, assessment of susceptibility to threat, influence security behaviours. The role of perceived severity and perceived vulnerability on protection motivation is mediated by an intervening variable, fear. The variable fear, added in the revised PMT (Rogers 1983), is described as an emotional feeling toward threat. Many applications of PMT in IS security research exclude fear, however the emotional feeling towards threat is an important predictor of security behaviour (e.g., Boss et al. 2015; Mwagwabi et al. 2018). We therefore include fear of threat as a direct predictor of behaviour and a function of perceived severity and perceived vulnerability.

Response efficacy, perception about the effectiveness of the recommended protection measures, and self-efficacy, an individual's confidence in their ability to perform recommended protection measures, promote protection motivation. When the recommended measure is perceived as difficult or inconvenient, response cost, the individual is unlikely to carry out the recommended response. Previous applications of PMT in IS security research support the link between response efficacy, response cost and self-efficacy, and security behaviour (e.g., Boss et al. 2015; Menard et al. 2018; Posey et al. 2015). We examine the role of these three factors in predicting protection motivation in teenagers.

2.2 The influence of risk perceptions and coping appraisal in teenagers' cyber security behaviour

As few studies have explicitly examined the relationship between teenagers' perceived risks and online behaviours (e.g., Ho et al. 2017; Lwin et al. 2012; Youn 2009), more studies are needed to better understand the role of risk perceptions in teenagers' cyber security behaviours. Using PMT, Youn (2009) found perceived vulnerability influences privacy concerns, which in turn drives privacy protection motivation. Lwin et al. (2012) found perceived severity of online harassment, response efficacy and self-efficacy play a significant role in teenagers' intention to protect against online harassment.

Adults and teenagers appear to differ. Young computer users are unique not because their decision-making and risk behaviours are influenced by friends and parents (ACMA 2011; Soh et al. 2018), but also because their risk coping mechanisms differ from adults (Turow and Nir 2000). As a risk copping strategy, when handling personal information on the internet, teenagers seek help from their parents (Turow and Nir 2000). This means parents and peers play a significant role in teenagers' risky behaviours and coping mechanism, thus it is important to also examine the role social influence in teenagers' security behaviours.

2.3 The role of normative beliefs and personal norms in teenagers cyber security behaviour

Fear, an emotional feeling toward threat (Rogers 1983), is an important predictor of security behaviour (Boss et al. 2015). In teenagers however, as Burnett et al. (2009) found, fear has a less social role in guiding behaviours compared to emotions such as embarrassment and guilt. Teenagers demonstrate a heightened self-consciousness when they know someone is observing them (Somerville et al. 2013). In a simulated social experiment conducted using functional brain imaging (fMRI), Somerville et al. (2013) examined teenagers response to peer evaluation. Being observed by a peer is enough to elicit self-

conscious emotion of embarrassment which in turn drives the teenagers to behave in certain manner. At this age, teenagers exhibit a heightened motivation to be accepted by their peers, thus how teenagers perceive experiences of being evaluated is important to examine. This sensitivity to social evaluation leads to anticipated emotions formed, based on personal norms (Schwartz 1977). Because teenagers appear to be sensitive to peer evaluation, the anticipated emotion of guilt or embarrassment associated with personal norms (Onwezen et al. 2013), is of interest in this study.

In teenagers, personal norms, associated with social expectations (Schwartz 1977), have a strong influence on behaviour. Personal norms include both internalized assessment of values and social expectations for behaviours (Elek et al. 2016). These internalized norms can be manifested as a reaction to an individual's self-expectation for behaviour (Schwartz 1977). Schwartz (1977) notes that there is an overlap between social norm and personal norms, given that personal norms are learned through social interactions. However, with personal norms, conformity or violation can lead to either the feeling pride or guilt, respectively. The anticipated guilt, which stems from the assessment of what their peers will think, leads to concerns about experiencing these feelings in the future.

Further, peer and parent relationship take an important role during teenage years (Albert et al. 2013; Soh et al. 2018; Somerville et al. 2013). In investigating peer influence on teenage risk-taking decision making, Albert et al. (2013) compared how adolescents and adults make decisions in a variety of risk situations. In one experiment, the participants completed tasks in the their peers' presence. Using a first-person driving game, Albert et al. (2013), assessed teenage participants' susceptibility to peer influence. Participants who completed the tasks in their peers' presence took significantly more risks, suggesting that risky behavior is heightened by peer influence. While parental influence on teenagers decreases as they grow older compared to peer influence the literature supports the influence of both parents and peers on teenagers' behaviors and decsion-making (Soh et al. 2018). This paper contributes to this debate by considering both parents and friends' influence as decribed in (Baker et al. 2003).

3 RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

To achieve the objectives described in this study, we propose a research model based on PMT (Rogers 1983). We extend PMT to explore the role of normative beliefs and personal norms in teenagers' motivation to protect their social media accounts.

3.1 Hypotheses developed from the PMT framework

The nine hypotheses described next, relate to the six variables described in PMT. The novelty of this study lies not in testing the PMT model nor in the extended model. It lies in the adaptation of PMT in the context of teenage cyber security behaviour. To the best of our knowledge, this is the first application of PMT in this context. Our study provide new insight into whether PMT can also predict security behaviours in young citizens.

IS applications of PMT suggest perceived severity of a threat and perceived vulnerability to threats inspire better security behaviours. In turn, perceived severity and perceived vulnerability, triggers an emotional response, fear, which in turn increases the likelihood of protection motivation (e.g., Boss et al. 2015; Mwagwabi et al. 2018; Posey et al. 2015). In the context of online harassment, perceived severity influences teenagers' intentions to protect against online harassment (Lwin et al. 2012). We therefore hypothesize:

H1: Perceived vulnerability will have a positive effect on intentions to comply with social media password guidelines.

H2: Perceived severity will have a positive effect on intentions to comply with social media password guidelines.

H3: Fear of threats will have a positive effect on intentions to comply with social media password guidelines.

H3: Fear of threats will have a positive effect on intentions to comply with social media password guidelines.

H4: Perceived vulnerability will have a positive effect on fear of threats.

H5: Perceived severity will have a positive effect on fear of threats.

Response efficacy, response cost and self-efficacy, refereed in this study as perceived password effectiveness, perceived cost, and password self-efficacy respectively, also drives security behaviour (e.g.,

Boss et al. 2015; Menard et al. 2018; Posey et al. 2015). While response efficacy and self-efficacy have a positive influence, response cost has a negative influence on protection motivation. In teenagers, response efficacy and self-efficacy play a significant role in teenagers' intention to protect against online harassment (Lwin 2012). We therefore hypothesize:

H6: Perceived password effectiveness will have a positive effect on intentions to comply with social media password guidelines.

H7: Password self-efficacy will have a positive effect on intentions to comply with social media password guidelines.

H8: Perceived cost will have a negative effect on intentions to comply with social media password guidelines.

3.2 Extending the PMT framework

As our target population is teenagers, we also explore the role of personal norm, which drives behaviour in teenagers (Elek et al. 2016). In this study we examine the anticipated emotions that are formed based on personal norms (Schwartz 1977). These internalized norms can be manifested as feeling of embarrassment or guilt if their social media account was hacked.

We define normative beliefs as a teenagers' belief that their parents and friends would ridicule, gossip about them if their social media account was hacked. Normative beliefs result from all the information communicated from other people such as friends, peers and colleagues. Individuals' expectations of such social networks (Ajzen 1991), or beliefs about what other's think, have a significant influence on individuals' decision to take action. Peer and parent relationship take an important role in teenagers (Albert et al. 2013; Soh et al. 2018;). In the context of social media, Ho et al. (2017) found subjective norm, that is, perceived expectations of significant others, had a strong influence on teenagers' willingness to protect their online privacy. Therefore, normative beliefs and personal norms would influence teenagers' compliance with IS security policies. We therefore hypothesize:

H9: Normative beliefs will have a positive effect on intentions to comply with social media password guidelines.

H10: Personal norms will have a positive effect on intentions to comply with social media password guidelines.

We also examine the relationship between intentions and actual compliance. Intentions are assumed to predict behaviour (Ajzen 1991), however the effects sizes are marginal (Floyd et al. 2000). Therefore we examine the extent to which intentions predict actual compliance with social media password guidelines. Therefore we hypothesize:

H11: Intentions to comply will have a positive effect on actual compliance with social media password guidelines.

4 METHODOLOGY

In this section, we provide a description of our participants, study design and measurement items. The participants were recruited by TOUCH CyberWellness (TCW) Singapore through the cyber wellness courses they conduct participating secondary schools across Singapore. A sample of 255 students between 13- 16 years were randomly selected to participate in the study within the period of November 2017 to May 2018. We chose the cut-off age of 13 because Facebook's starting age is 13 (DQ-Institute 2018). To ensure confidentiality and anonymity, we generated a random 6-digit Index Number which we assigned to each participant prior to completing the survey.

4.1 Measurement development

To ensure validity and reliability of the measurement items, we selected previously validated items and reworded them in the context of password related threats. We measured the items on a 7-point Likert scale from (1) 'strongly disagree' to (7) 'strongly agree'. Perceived vulnerability (e.g. "There is a chance that someone could hack into my Social Media accounts.") and perceived severity (e.g. "I believe that if someone successfully hacked into my Social Media account the consequences would be severe") were adapted from Zhang and McDowell (2009). Fear of threat (e.g. "The thought of someone hacking into any of my Social Media accounts frightens me.") was adapted from Milne et al. 2002. Perceived password effectiveness (e.g. "Making sure that my passwords do not contain any dictionary words will make them more difficult to guess."), password self-efficacy (e.g. "I am confident that I can protect my

Social Media account from hackers.") and perceived cost (e.g. "Strong passwords take too much effort to create."), were adapted from Zhang and McDowell (2009), Compeau and Higgins (1995) and Milne et al. (2002) respectively. From Schwartz (1977), we adapted items to reflect the anticipated emotions based on personal norms (e.g. "I would feel guilty if my account was hacked."), and normative beliefs (e.g. "My parents would scold me if my Social Media account was hacked.") were adapted from Ajzen (1991).

5 DATA ANALYSIS AND RESULTS

In this section, we present the analysis, assessment of the measurement model and path analysis. We present the results of each hypothesis here, and discuss the implications in Section 6. We analysed the data using partial least squares, using SmartPLS 3 software (Ghozali and Latan 2015). We elected PLS-SEM instead of covariance-based SEM due to the large number of latent constructs (Lowry and Gaskin 2014) in our study. A total of 246 students aged 13 to 16 completed the study on Qualtrics.com. Due to the participants' age, and following our ethics requirements, data on gender was not collected.

We evaluated the measurement model using the recommended PLS-SEM measurement metrics (Hair et al. 2017), as follows. To confirm convergent validity we used average variance extracted (AVEs) and we used composite reliability (CR) to assess the individual item's internal consistency. The AVE and CR values were above 0.70, thus confirming convergent validity and internal consistency. To assess discriminant validity, we used the heterotrait-monotrait ratio (HTMT). This measures the average of all items' correlations, across constructs (Hair et al. 2017). Our HTMT values were below 0.9 suggesting no discriminant validity issues. Once the path model was tested, we assessed the model's predictive power. The paths between the PMT constructs, normative and personal norms produced an R^2 of 0.567 for intentions to comply, and the path between intentions to comply and actual compliance was significant (0.844, p=0.000) and produced an R^2 of 0.712. This means that our model accounted for 56.7% and 71.2% of the variance of intentions to comply and actual password compliance. In the remaining section, we present the results of our hypotheses, followed by a discussion of our results in Section 6.

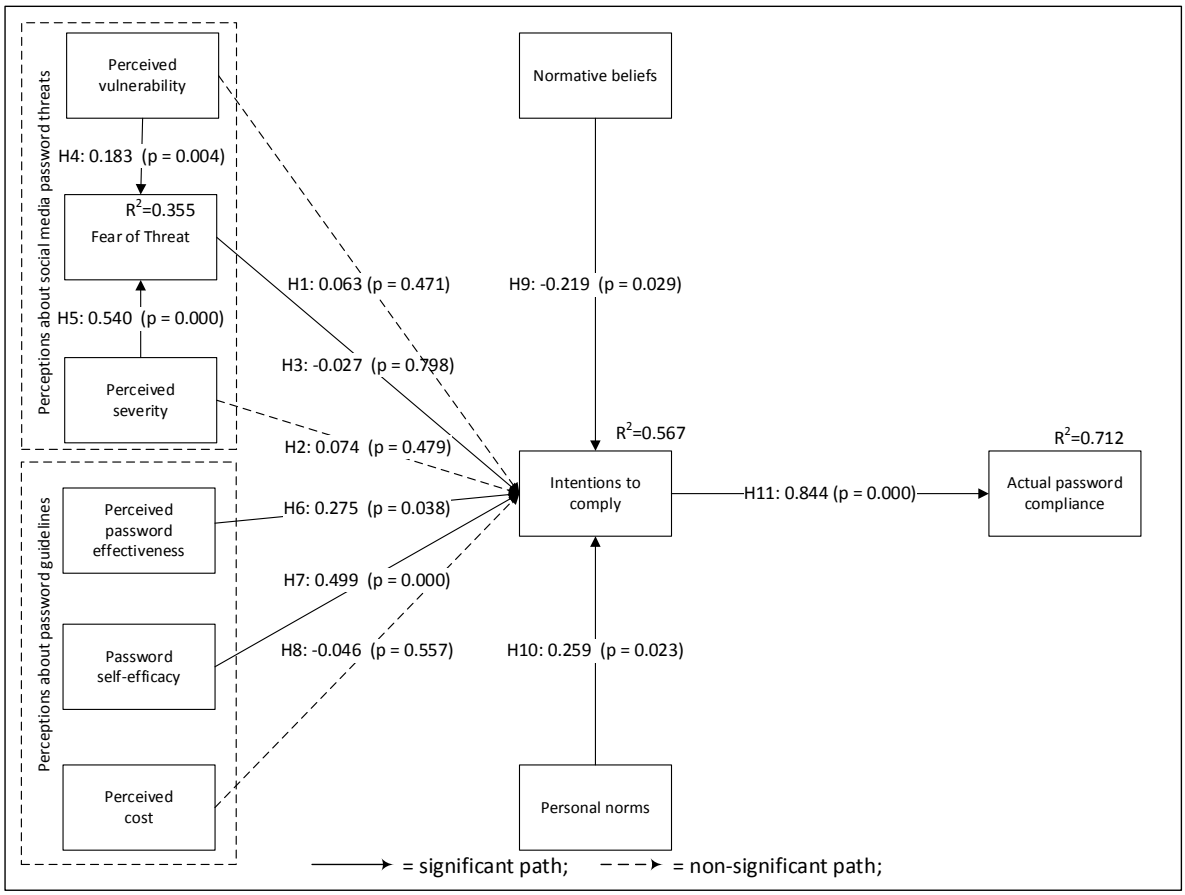

Figure 1. Proposed Research Model Results

As figure 1 shows, the threat component had no influence on intentions to comply, rejecting H1, H2 and H3. Therefore, perceived vulnerability, perceived severity and fear of threats, had no influence on the teenagers' intentions to comply with social media password guidelines. As hypothesized in H4 and H5, fear of threats was influenced by perceived vulnerability and perceived severity, implying the participants' fear of password threats, stems from their perceived vulnerability and perceived severity of threats.

Perceived password effectiveness and password self-efficacy influenced compliance intentions. This supports H6 and H7, suggesting teenagers' motivation to comply with social media password guidelines, depend on perceived effectiveness of password guidelines and confidence in their ability to create strong passwords. Perceived cost did not affect compliance intentions, rejecting H8. Thus, the teenagers, were not negatively influenced by the difficulty associated with maintaining strong passwords.

Interestingly, normative beliefs had a significant, but negative influence on compliance intentions. While this result rejects our hypothesis, H9, the relationship was significant implying that the teenagers' were negatively influenced by their friends and parents' expectations, and what they thought if their social media account was hacked. H10, the link between personal norms and compliance intentions, was supported, therefore personal norms affects teenagers' intention to comply with social media password guidelines.

We summarize our hypothesized relationships in Table 1, indicating which ones were supported.

Construct	Support
H1: Perceived vulnerability → intentions to comply	Not supported
H2: Perceived severity → intentions to comply	Not supported
H3: Fear of threats → intentions to comply	Not supported
H4: Fear of threats → perceived vulnerability	Supported
H5: Fear of threats → perceived severity	Supported
H6: Perceived password effectiveness → intentions to comply	Supported
H7: Password self-efficacy → intentions to comply	Supported
H8: Perceived cost → intentions to comply	Not supported
H9: Normative beliefs → intentions to comply	Not supported
H10: Personal norms → intentions to comply	Supported

Table 1. Summary of hypotheses

6 DISCUSSION AND CONCLUSION

We identified three gaps in the literature, including little focus on cyber security behaviour and how to inspire better cyber security practices in teenagers. Theory grounded cyber security research focusing on teenagers is also lacking. To address this gap, we applied PMT to investigate factors that inspire teenagers to comply with cyber security guideless on social media. Given the role parents and peers play in teenagers' protective behaviour (ACMA 2011; Soh et al. 2018), we extended PMT and included personal norms and normative beliefs. We investigated the role of security perceptions, perceptions about the security recommendations, normative beliefs and personal norms in teenagers' compliance intentions.

We found perceived vulnerability, perceived severity and fear of threat, have no influence on teenagers' compliance intentions. For teenage computer users, believing they are susceptible to hacking or that the consequences of being hacked would be severe, had no bearing on their password choices. This is an interesting finding highlighting a potential difference between adults and teenagers. IS security studies (Boss et al. 2015; Mwagwabi et al. 2018; Posey et al. 2015) have found a link between threat appraisal and security behaviours in adults. Our finding is potentially because teenagers tend to under estimate their vulnerabilities online (Lwin et al. 2012), a phenomena Weinstein (1984) described as optimistic bias where individuals tend to believe negative events are less likely to happen to them. This tendency to discount their susceptibility online appears to contribute minimally to their motivation to undertake the recommended security guidelines. It is also possible that an emotional feeling toward threat (Rogers 1983), play a lesser role in guiding teenage behaviour and that in teenagers emotions such as embarrassment and guilt play a more significant role (Burnett et al. 2009). Consistent with our findings, the anticipated feeling of embarrassment or guilt associated with personal norms, better predicts security compliance in teenagers. This means, it is possible that the cognitive threat appraisal (Rogers 1983), may be different in teenagers.

Consistent with IS security research (e.g., Boss et al. 2015; Posey et al. 2015), we found teenagers' self-efficacy and perceptions that strong passwords will protect their social media accounts, has a positive impact on their willingness to comply with social media password guidelines. In our study, copping appraisal appears to better predict teenagers' compliance behaviour, as suggested in PMT (Rogers 1983). This may also be a result of teenagers wide use of social media (Anderson and Jiang 2018), leading to enhanced confidence (self-efficacy) and knowledge of how to protect themselves (perceived effectiveness), using the available protective measures.

This study yielded some interesting findings that future studies should explore further. Whether teenagers perceive strong passwords as difficult to manage has no significant impact on their protection motivations. Further, personal norms engenders compliance in social media password guidelines. Teenage social media users are more likely to follow security guidelines when they are concerned about feeling guilty. This concern is born out of their assessment of what their peers will think.

Interestingly, our results show a negative relation between normative beliefs and teenagers security compliance behaviour. This is contrary to the literature on peers and parents' influence on teenagers' behaviour (Ajzen 1991; Soh et al. 2018). However, the findings on the role of peer and parents are mixed. For example, Baker et al. (2003) also found no link between parents and friends' influence on teenagers' intentions to engage in healthy behaviours. A potential reason for the lack of support in our study, albeit a significant relationship is, as the study by Soh et al. (2018) reveals, parents and peers may have a significant but opposite relationship, and while peers increase teenagers' online risk taking propensity, parents decrease the likelihood of risky online activities in teenagers.

Contrary to findings in PMT studies (e.g., Crossler et al. 2014; Mwagwabi et al. 2018; Posey et al. 2015; Thompson et al. 2017) which support the link between threat appraisal and coping appraisal and security behaviours, in our study it appears that, for teenagers, threat appraisal does not have an impact on their protection motivations. We found that teenagers' self-expectations associated with personal norms, whether they feel embarrassed if their social media account was hacked, is a better predictor than their threat perception.

7 IMPLICATIONS FOR RESEARCH AND PRACTICE

Our study reveals two important research implications. Firstly, we found that personal norms is a stronger predictor of teenagers' security behaviours. Teenagers are driven by the emotional feeling of guilt or embarrassment if their social media account was hacked than by the emotional feeling of fear of being hacked. Secondly, our study reveals an important finding suggesting there may be significant differences between adults and teenagers in security compliance behaviour. More importantly, the influence from peers has a dominant influence towards risky behaviours in teenagers. For example, Albert et al. (2013), who used brain imaging to study teenagers' susceptibility to peer pressure, reveal that teenagers have a higher propensity to online risky behaviour when observed by their peers.

Our findings suggest that teenage group potentially differ from the adult group in terms of compliance behaviour and highlight important implications for future research. Future research on IS security behaviour should investigate the differences in adults and teenagers. These potential differences can draw interesting implications. This is an important finding, which opens new avenues for future research seeking to investigate teenagers' security behaviour.

For practitioners, this study provides insight into significant factors that lead to security compliance in teenagers. The findings reveal that when using persuasive communication teenagers and adults are possibly different in the way they respond to threat stimuli. Consistent with Burnett et al. (2009), we found that in the context of cyber security threats, fear has a less social role in guiding teenagers' behaviours. Teenagers make their decisions based on their personal feelings, their personal norms are relevant to their decision to protect their social media than their fear of cyber security threats. Thus, in practice, our findings suggest the value of targeting emotions based on personal norms rather than fear of threats.

In terms of coping mechanisms, as teenagers' perceptions of the recommended security measures become more favourable, and their confidence in protecting their social media account increase, they become more willing to follow security guidelines. Cyber security campaigns should therefore aim at enhancing awareness of the efficacy of the recommended security measures.

8 LIMITATIONS

The project faced some significant data collection issues including difficulty in finding schools to participate in a cyber security study. Feedback gathered from the participants showed the students found the surveys lengthy and tedious to complete. This is unsurprising as the participants were 13 to 16 years of age. While we conducted a pilot test, future projects should pilot test their surveys focusing on gauging the time it would take to complete the surveys and to target a completion time of between 10 to 15 minutes.

Another notable limitation is we collected data in Singapore. Cultural differences play a role in individuals' security behaviours (Menard 2018), therefore future studies should consider examining security behaviours of teenagers across countries. Another potential limitation is data was collected from people between the ages of 13-16. While we chose a cut-off age of 13 following Facebook's minimum age requirement, future studies should consider a wider age range of for example 13-18 years.

Lastly, another potential limitation is the use of Facebook as a proxy for social media use. While Facebook is still widely used by teenagers, the use of YouTube, Instagram or Snapchat is increasing (DQ-Institute 2018; Ofcom 2018), therefore future studies should also consider teenagers' cyber security behaviours on Instagram, YouTube and Snapchat.

9 REFERENCES

Ablon, L., Libicki, M. C., and Golay, A. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Rand Corporation.

ACMA. 2011. "Young Australians' Experience of Social Media: Qualitative Research Report." Australian Communications and Media Authority.

ACMA. 2013. "Young Australians' Experience of Social Media: Quantitative Research Report." Australian Communications and Media Authority.

ACMA. 2016. "Aussie Teens and Kids Online." Australian Communications and Media Authority.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Albert, D., Chein, J., and Steinberg, L. 2013. "The Teenage Brain: Peer Influences on Adolescent Decision Making," *Current directions in psychological science* (22:2), pp. 114-120.

Anderson, E. L. 2017. "Internet Use and Problematic Internet Use: A Systematic Review of Longitudinal Research Trends in Adolescence and Emergent Adulthood," *International journal of adolescence and youth* (22:4), pp. 430-454.

Anderson, M., and Jiang, J. 2018. "Teens, Social Media & Technology." Pew Research Center.

Baker, C. W., Little, T. D., and Brownell, K. D. 2003. "Predicting Adolescent Eating and Activity Behaviors: The Role of Social Norms and Personal Agency," *Health Psychology* (22:2), p. 189.

Bandura, A. 1982. "Self-Efficacy Mechanism in Human Agency," *American Psychologist* (37:2), pp. 122-147.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., and 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 (MISQ)* (39:4), pp. 837-864.

Boush, D. M., Friestad, M., and Rose, G. M. 1994. "Adolescent Skepticism toward Tv Advertising and Knowledge of Advertiser Tactics," *Journal of consumer research* (21:1), pp. 165-175.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Burnett, S., Bird, G., Moll, J., Frith, C., and Blakemore, S.-J. 2009. "Development During Adolescence of the Neural Processing of Social Emotion," *Journal of cognitive neuroscience* (21:9), pp. 1736-1750.

Burr, W. E., Dodson, D. F., Newton, E. M., Pelner, R. A., and Polk, W. T. 2013. "Electronic Authentication Guideline: Nist Special Publication 800-63-2." NIST Special Report 800-63-3.

Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), pp. 189-211.

Crossler, R. E., Long, J. H., Loraas, T. M., and Trinkle, B. S. 2014. "Understanding Compliance with Byod (Bring Your Own Device) Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap," *Journal of Information Systems*).

CSA-Singapore. 2019. Retrieved 25 July 2019, from https://www.csa.gov.sg/gosafeonline

Cybersafe.org. 2016. "Children's Internet Usage Study," in: *Center for Cyber Safely and Education*.

Dang, D., Pittayachawan, S., and Nkhoma, M. 2015. "Demystifying Online Personas of Vietnamese Young Adults on Facebook: A Q-Methodology Approach," *Australasian Journal of Information Systems* (19), pp. 1-22.

DQ-Institute. 2018. "Outsmart the Cyber-Pandemic: Empower Every Child with Digital Intelligence by 2020."

Elek, E., Miller-Day, M., and Hecht, M. L. 2006. "Influences of Personal, Injunctive, and Descriptive Norms on Early Adolescent Substance Use," *Journal of Drug Issues* (36:1), pp. 147-172.

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

Ghozali, I., and Latan, H. 2015. "Partial Least Squares, Konsep, Teknik Dan Aplikasi Menggunakan Program Smartpls 3.0 Untuk Penelitian Empiris," *Semarang: Badan Penerbit UNDIP*).

Gunnar, M. R., Wewerka, S., Frenn, K., Long, J. D., and Griggs, C. 2009. "Developmental Changes in Hypothalamus–Pituitary–Adrenal Activity over the Transition to Adolescence: Normative Changes and Associations with Puberty," *Development and psychopathology* (21:1), pp. 69-85.

Hair J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2017. *A Primer on Partial Least Squares Structural Equation Modeling (Pls-Sem)*. 2nd Ed. Sage Publications.

Ho, S. S., Lwin, M. O., Yee, A. Z., and Lee, E. W. 2017. "Understanding Factors Associated with Singaporean Adolescents' Intention to Adopt Privacy Protection Behavior Using an Extended Theory of Planned Behavior," *Cyberpsychology, Behavior, and Social Networking* (20:9), pp. 572-579.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., and Lowry, P. B. 2014. "Improving Password Cybersecurity through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals," *Information Technology for Development* (20:2), pp. 196-213.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS quarterly* (39:1).

Lowry, P. B., and Gaskin, J. 2014. "Partial Least Squares (Pls) Structural Equation Modeling (Sem) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It," *IEEE transactions on professional communication* (57:2), pp. 123-146.

Lwin, M. O., Li, B., and Ang, R. P. 2012. "Stop Bugging Me: An Examination of Adolescents' Protection Behavior against Online Harassment," *Journal of Adolescence* (35:1), pp. 31-41.

Maddux, J. E., and 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), pp. 469-479.

Marett, K., McNab, A. L., and Harris, R. B. 2011. "Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory," *AIS Transactions on Human-Computer Interaction* (3:3), pp. 170-188.

Menard, P. 2018. "The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination," *Computers & security* (75), pp. 147-166.

Milne, S., Orbell, S., and Sheeran, P. 2002. "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British Journal of Health Psychology* (7:2), pp. 163-184.

Mwagwabi, F., McGill, T. J., and Dixon, M. 2018. "Short-Term and Long-Term Effects of Fear Appeals in Improving Compliance with Password Guidelines," *CAIS* (42), p. 7.

Ofcom. 2018. "Children and Parents: Media Use and Attitudes."

Onwezen, M. C., Antonides, G., and Bartels, J. 2013. "The Norm Activation Model: An Exploration of the Functions of Anticipated Pride and Guilt in Pro-Environmental Behaviour," *Journal of Economic Psychology* (39), pp. 141-153.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study," *PACIS 2007 Proceedings*), p. 73.

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

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

Soh, P. C.-H., Chew, K. W., Koay, K. Y., and Ang, P. H. 2018. "Parents vs Peers' Influence on Teenagers' Internet Addiction and Risky Online Activities," *Telematics and Informatics* (35:1), pp. 225-236.

Somerville, L. H., Jones, R. M., Ruberry, E. J., and Dyke, J. P. 2013. "The Medial Prefrontal Cortex and the Emergence of Self-Conscious Emotion in Adolescence," *Psychological science* (24:8), pp. 1554-1562.

Tayouri, D. 2015. "The Human Factor in the Social Media Security–Combining Education and Technology to Reduce Social Engineering Risks and Damages," *Procedia Manufacturing* (3), pp. 1096-1100.

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.

Tsirtsis, A. 2016. "Cyber Security Risks for Minors: A Taxonomy and a Software Architecture." IEEE, pp. 93-99.

Turow, J., and Nir, L. 2000. "The Internet and the Family: The View from Parents, the View from Kids,".

Weinstein, N. 1984. "Why It Won't Happen to Me: Perceptions of Risk Factors and Susceptibility," *Health psychology* (3:5), pp. 431 - 457.

Youn, S. 2009. "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents," *Journal of Consumer affairs* (43:3), pp. 389-418.

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), pp. 180-197.