Compliance with security guidelines in teenagers: the conflicting role of peer influence and personal norms

Florence Mwagwabi
Murdoch University,
Singapore
F.Mwagwabi@murdoch.edu.au

Jhee Hee Jiow
Singapore Institute of Technology
Singapore

Abstract

What drives teenagers to comply with computer password guidelines? Using an extended form of protection motivation theory (PMT) (Rogers, 1983), we found that even if teenage computer users believe they are susceptible to being hacked, or that being hacked would be detrimental, it has no bearing on their password choices. Other motives outside of PMT also drive teenage security behaviour. Personal norms fully mediate the relationship between the perceived severity of threat and compliance intentions such that perceived severity is not sufficient to encourage compliance. Teenagers must actually feel obligated to comply. While personal norms may encourage compliance, concerns about feeling embarrassed or ashamed if their social media accounts are hacked into actually encourages compliance. On the other hand, peer influence, such as the fear of being teased about someone hacking into their account, discourages compliance. Our study contributes to understanding early security practices and highlights potential differences between adult and teenage behaviours to consider in future studies. For example, our findings suggest that password security guidelines alone will not suffice to ensure teenage compliance; they may need enforced password rules at the authentication level to eliminate any opportunity to violate password rules. Our study will benefit children and parents as well as organizations that have changed work practices to enable employees to work from home, but which places children in danger of clicking on malicious links on their parents' computers. To our knowledge, this is the first password security study that applies PMT to examine computer-based security behaviours in teenagers.

Keywords protection motivation theory, PMT, teenage cyber security behaviour, compliance behaviours in teenagers, password compliance intention, social media password practices, peer influence, personal norms, anticipated guilt, anticipated embarrassment

1 Introduction

While teenagers (13–16 years in this study) have access to all that the Internet has to offer (DQ-Institute, 2018; Tsirtsis, Tsapatsoulis, Stamatelatos, Papadamou, & Sirivianos, 2016), most children have been exposed to some form of cyber threat (DQ-Institute, 2018). In 2018, the DQ-Institute surveyed more than 80,000 children exploring the extent of their exposure to cyber risk. Exacerbated by the always-on cell phone and social media usage, the DQ-Institute also found that children's exposure to cyber threat is growing exponentially. Almost 60% of children as young as eight are exposed to cyber risk, including cyber bullying, game addiction, and online sexual behaviour. The problem we find with major surveys such as this DQ-

Institute study is that they overlook other potential computer security risks, such as malware, phishing, and password attacks.

With millions of children studying from home due to COVID-19, exposure to cyber security threats such as clicking on infected links and downloading malware is a major problem (Braue, 2020). Cyber attacks targeting children are widely reported in the media (e.g., BBC, 2012; Braue, 2020; Corron, 2018), but research specifically related to teenage cyber risk is lacking. Our study will benefit children and parents as well as organizations who have updated their work practices to enable employees to work from home but which places teenagers in danger of clicking on malicious links on their parents' computers (Braue, 2020).

Studies on cyber risk in teenage computer use have focused on threats such as problematic internet use (e.g., Buckingham, Banaji, Carr, Cranmer, & Willett, 2005; DQ-Institute, 2018; Soh, Chew, Koay, & Ang, 2018), access to adult content (Cybersafe.org 2016), cyber bullying and online harassment (e.g., DQ-Institute, 2018; Lwin, Li, & Ang, 2012), but few cite cyber security threat (Tsirtsis et al., 2016).

In literature related to teenage cyber risk we identified three specific gaps. Firstly, there is a lack of research on how to inspire better cyber security practices in teenagers. To address this, our research examines factors that motivate teenagers to comply with password guidelines on social media. We focus on online social media because applications such as Facebook are a significant avenue through which teenagers are exposed to cyber security threat (Tsirtsis et al., 2016). Secondly, there is a lack of theory-based studies in teenage cyber security behaviour. Our research addresses this by applying protection motivation theory (PMT) to investigate teenage compliance with password security guidelines.

Thirdly, as theory-based research on cyber security behaviour focuses on adults, this research uses PMT (Rogers, 1983) to try and understand the protection motivation of teenagers using social media. Teenagers were chosen as our target population, and Facebook as the proxy for social media, because teenagers are more active on social media than adults. While Instagram, YouTube, and Snapchat usage has increased, Facebook is still widely used by teenagers (ACMA, 2016; Ofcom, 2018). Further, teenagers are likely to share personal information on Facebook (ACMA, 2011) which increases their exposure to cyber security threat on this platform.

Understanding teenage cyber security behaviour is complicated because peer influence in this age group plays a strong role in teenage risk-taking behaviour (Gardner & Steinberg, 2005; Soh et al., 2018; Somerville, Jones, Ruberry, & Dyke, 2013). Since peers play such an essential role (ACMA, 2011; Soh et al., 2018), this research extends PMT to examine just how peer influence can impact teenage security behaviour.

Investigating teenage cyber behaviour is challenging because age-group categorizations differ across different studies. For example, in the internet-use surveys described in ACMA (2016), data was collected from teenagers aged 14–17 years (Australia), 12–17 years (USA), and 12–15 years (UK). For this research, undertaken in Singapore, a teenager is defined as a person who falls within 13–18.

In the InfoSec (IS) domain, PMT (Rogers, 1983) is used to investigate users' underlying security perceptions and security practices (e.g., Johnston, Warkentin, & Siponen, 2015; Posey, Roberts, & Lowry, 2015). Used initially in a health-related context, PMT has been used to investigate protection behaviours in all age groups (Lwin et al., 2012). Yet PMT applications in IS security

research have focused only on adult populations. Teenagers and adults have different stages of cognitive-development (Lwin et al., 2012; Steinberg, 2008). Since PMT requires the cognitive processing of cyber threat (Rogers, 1983), threat appraisal in teenagers is expected to differ from that of adults. This study questions whether PMT can explain security compliance behaviour in teenagers, and whether the threat and coping appraisal abilities of teenagers display the same level of maturity as adults.

A key ingredient in protection motivation is the perception of cyber threat and recommended safeguards (Rogers, 1983). With early exposure to the Internet, understanding teenage security perception is critical (Tayouri, 2015). Teenagers are aware that cyber safety education is important (ACMA, 2011, 2013), and are familiar with internet safety rules (Livingstone, Mascheroni, & Staksrud, 2017). While they acknowledge receiving cyber safety training (Cybersafe.org, 2016), and despite exhibiting some security awareness, teenagers possess poor security practices such as sharing passwords (ACMA, 2013). Problems with poor security and password practices range from how valuable passwords are on the dark market, even when compared with credit card information (Ablon, Libicki, & Golay, 2014), to how easily hackers can crack passwords from other known or leaked passwords (Maor, 2020). This means poor security practices can have severe implications beyond accessing teenagers' online accounts (Braue, 2020; Jenkins, Grimes, Proudfoot, & Lowry, 2014). By providing insights into security practices at an early age, our study will benefit a wide range of stakeholders.

2 Literature Review

Prior research using PMT has looked at individual adult cyber security behaviours (e.g., Mwagwabi, McGill, & Dixon, 2018; Thompson, McGill, & Wang, 2017) and security behaviour within organizations (e.g., Menard, Bott, & Crossler, 2017; Posey et al., 2015). Lacking in the security literature, this study explores whether PMT (Rogers, 1983) can be used to predict teenage cyber security behaviour. This is achieved by first examining how perceptions about security and security behaviour recommendations influence teenage behaviours, and whether PMT can predict protective behaviour in teenagers.

2.1 PMT theoretical background

Rogers (1983) developed PMT to explain health-related behaviour and identified perceived severity, perceived susceptibility, and response efficacy as key predictors of health protection motivation. Bandura's (1982) work on self-efficacy inspired Rogers (1983) to include self-efficacy in the PMT framework.

PMT proposes that threat severity and threat susceptibility appraisal are what drive protective behaviour. An intervening variable, fear, mediates perceived severity and perceived vulnerability. The revised PMT (Rogers, 1983) model describes fear as being an emotional response to cyber security threat. Many PMT applications in IS security research exclude fear, yet it is an essential predictor of security behaviour (e.g., Boss, Galletta, Lowry, Moody, & Polak, 2015; Mwagwabi et al., 2018). This study consequently includes the fear of cyber threat as a direct predictor of protection behaviour and a function of perceived severity and perceived vulnerability.

The perceived effectiveness of protection measures—i.e., response efficacy and confidence in implementing protection measures—i.e., self-efficacy, affect protective behaviour. On the other hand, response cost—i.e., the perceived inconvenience of protection measures—has a

negative influence on protection motivation. These three variables—response efficacy, self-efficacy and response cost constitute PMT's coping appraisal. Applications of PMT in IS security research (e.g., Boss et al., 2015; Menard et al., 2017; Posey et al., 2015) support the link between coping appraisal and security behaviour. We examine how these three variables help to predict protection motivation in teenagers.

2.2 Risk perceptions, coping appraisal, and cyber security behaviour in teenagers

While some studies have examined the relationship between teenagers' perceived cyber risk and online behaviour (Lwin et al., 2012; Youn, 2009), more studies are needed to better understand exactly how risk perceptions drive teenage security behaviour. Using PMT, Youn (2009) found that perceived cyber vulnerability influences privacy concerns and drives protection motivation. Perceived severity, response efficacy, and self-efficacy drive teenagers' intentions to prevent online harassment (Lwin et al., 2012). These studies support using the PMT model to predict teenage security behaviour.

As mentioned, when it comes to risk-taking behaviours on the Internet, adults and teenagers may differ (Gardner & Steinberg, 2005). There is consequently a need to understand how well PMT predicts teenage security behaviour.

2.3 Peer influence, personal norms, and cyber security behaviour in teenagers

Fear is an emotional response to threat (Rogers, 1983) and influences security behaviour in adults (Boss et al., 2015; Mwagwabi et al., 2018). Yet in teenagers, as found by Burnett, Bird, Moll, Frith, and Blakemore (2009), the fear of threat has a less social role in guiding their behaviour than the fear of embarrassment and guilt (Grasmick & Bursik Jr, 1990). Teenage fear is manifested as guilt or shame when they violate personal norms (Grasmick & Bursik Jr, 1990) that are associated with social expectations as well as expectations they have of themselves (Schwartz, 1977). As a result, before teenagers engage in any behaviour, they first assess the cost of feeling embarrassed or guilty.

Schwartz (1977) notes that there is an overlap between social norms and personal norms, given that people acquire personal norms through social interaction. The conformity or violation of personal norms can lead to feelings of pride or guilt, respectively. On the other hand, the anticipated guilt from perceived peer evaluation can lead to concerns about experiencing it in the future, so their ensuing behaviour is motivated by avoiding feelings of guilt.

Personal norms appear to mediate the relationship between cyber risk perceptions and behaviour (De Groot, 2010; De Groot & Steg, 2009; Schwartz, 1977). Personal norms can therefore explain how threat awareness translates into behavioural intentions (De Groot, 2010). This study explores the potential mediating role of personal norms and intentions to comply with security guidelines. Our findings should provide better insight into how the relationship between perceived severity and compliance evolves (Hair, Hult, Ringle, & Sarstedt, 2016).

Following De Groot (2010), De Groot and Steg (2009), and Schwartz (1977), in this study feelings of guilt or embarrassment both reflect and motivate teenage individuals to behave according to their personal norms (Onwezen, Antonides, & Bartels, 2013; Schwartz, 1977).

Teenagers also demonstrate a heightened self-consciousness when they know their peers are observing them (Gardner & Steinberg, 2005; Somerville et al., 2013). In an experiment aimed at understanding teenage risk-taking behaviour, Gardner and Steinberg (2005) observed and compared the decisions teenagers make when alone against when their peers are present. This involved using a computer game requiring participants to make decisions in risky situations—such as running a red traffic light when driving—and found that despite awareness of the adverse consequences of e.g., running a red light, the teenagers took double the risk in the presence of peers than they took in their absence. Steinberg (2008) attributes this risk-seeking propensity to how the teenage brain cognitive control system works, especially in their peers' company.

Teenage risk-taking behaviour and sensitivity to peer evaluation heightens between the ages of 13–16, and declines towards adulthood (Steinberg, 2008). Like Gardner and Steinberg (2005), Somerville et al. (2013) found that sensitivity to peer evaluation peaks at around 17 years. Using functional magnetic resonance imaging (fMRI), Somerville et al. (2013) found that peer evaluation can trigger a self-conscious emotion of embarrassment, which determines a teenager's subsequent behaviour. This paper explores the role peer influence plays in teenage compliance to security guidelines.

3 Research Model and Hypotheses Development

To achieve the objectives described in this study, a research model based on PMT (Rogers, 1983) has been proposed. This extends PMT to explore how peer influence and personal norms affect teenage motivations for protecting their social media accounts.

3.1 Hypotheses developed from the PMT framework

The nine hypotheses explored in this study relate to the six variables that are defined in PMT (Rogers, 1983). Our contribution to protection motivation research lies not in testing the PMT model nor in the extended model. Rather, 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 provides new insights into whether PMT can also predict security behaviours in young citizens.

Given that PMT research on cyber security behaviour has primarily focused on adults, the literature reviewed in this section relates to adult security behaviour. PMT applications in IS suggest that perceived severity and perceived vulnerability to cyber threat inspires better security behaviours. Studies have shown that if adults believe they are susceptible to cyber threat, they are likely to follow security guidelines. For example, Li et al. (2019) found that employees are willing to comply with security guidelines if they believe their organization could be vulnerable to cyber attack. Adult users are also more likely to follow security guidelines if they believe the consequences would be severe. This finding is consistent with that of Lee and Larsen (2009), who found that business executives are more likely to apply security measures if they believe an attack on their organization would have severe consequences.

Perceived severity and perceived vulnerability to threat triggers the emotional response of fear, which in turn increases the likelihood of compliance behaviour (e.g., Boss et al., 2015; Mwagwabi et al., 2018; Posey et al., 2015). This relationship has been shown in organizational settings where Posey et al. (2015) found that when employees assess high degrees of cyber

threat vulnerability and severity, their fear increased. This in turn increased their willingness to protect their company's information assets. In the context of password use on the Internet, Mwagwabi et al. (2018) found that when users perceive an increased vulnerability to password attack and believe the consequences would be severe, their fear increased. This resulted in improving the quality of passwords. While research on teenage security behaviour is limited, Lwin et al. (2012) found that in the context of online harassment, perceived severity influences teenagers' intentions to protect against it. From these findings we hypothesize:

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

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

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

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

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

Response efficacy, response cost, and self-efficacy, which are referred to in this study as perceived password effectiveness, perceived cost, and password self-efficacy, also drive cyber security behaviour (e.g., Boss et al., 2015; Menard et al., 2017). While response efficacy and self-efficacy have a positive influence, response cost negatively influences protection motivation. The above three factors have also been shown to affect organizational and individual cyber security behaviour. In their study of how organizations can motivate employees to protect their information assets, Posey et al. (2015) found that when employee response efficacy increases, their motivation to protect their organization's information assets also increases. In addition, employees must believe that they have the necessary skills to protect their organization's information assets from cyber threat.

In the context of individual security behaviour, Crossler, Andoh-Baidoo, and Menard (2019) showed that when users perceive security measures as being easy to use or requiring minimal effort to implement, their likelihood to take action increases. Accordingly, Crossler et al. (2019) found that regardless of the culture, when individual computer users find security measures challenging to implement, they are less willing to take action. In teenagers, response efficacy and self-efficacy play a significant role in their intention to protect against online harassment (Lwin et al., 2012). From these findings we hypothesize:

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

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

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

3.2 Extending the PMT framework

This study also explores the role of personal norms and peer influence in driving teenage security behaviour (Elek, Miller-Day, & Hecht, 2006; Gardner & Steinberg, 2005; Somerville et al., 2013). Following De Groot (2010), De Groot and Steg (2009), and Schwartz (1977), we found

that encompassed in the construct of personal norms are the anticipated feelings of guilt or embarrassment which in turn motivate teenagers to behave in line with their norms (Schwartz, 1977). This study proposes that the anticipated feelings of embarrassment or guilt result from a teenagers' social media account being hacked will motivate them to comply with security guidelines.

However, De Groot and Steg (2009) argue that personal norms are only experienced through these feelings when the individual is aware of the consequences of non-compliance, so only then can personal norms trigger security behaviour. Personal norms therefore act as a mediating variable that enables cyber risk awareness to translate into behavioural compliance.

In a separate study by De Groot (2010), personal norms were also measured as feelings of guilt or embarrassment that mediate the link between risk awareness and behavioural intentions, explaining how threat awareness translates into behavioural intentions. De Groot's study also found that perceived norms mediate the relationship between risk perceptions and a willingness to take action. Thus, the awareness of risk consequences influences the willingness to take action only through the emotional feeling of guilt or embarrassment (De Groot, 2010).

Exploring the potential mediating role of teenage personal norms will bring better insight into how the relationship between perceived threat severity and compliance evolves (Hair et al., 2016). By introducing personal norms as a mediating variable, this study can explore and reveal whether there is a relationship between perceived threat severity and teenage compliance. We hypothesize that an awareness of the consequences of password threats (perceived severity) influences personal norms. Furthermore, we hypothesize that personal norms mediate the relationship between perceived severity and compliance intentions.

H9: Perceived severity will have a positive effect on teenage personal norms.

H10: Personal norms mediate the relationship between perceived severity and teenage intentions to comply with social media password guidelines.

H11: Personal norms will have a positive effect on teenage intentions to comply with social media password guidelines.

As mentioned, peer influence plays an essential role in teenagers' decision-making processes (Albert, Chein, & Steinberg, 2013; Soh et al., 2018). Though there are different kinds of peer influence (Brown, 2004), susceptibility to negative peer influence heightens during the teenage years (Gardner & Steinberg, 2005). Peer pressure occurs when peers prescribe or model a particular behaviour. Our study explores an intentional peer influence through teasing, gossiping, or conversation that reinforces the normative expectations of a specific groups (Brown, 2004). Since peer influence involves behaviour such as teasing someone if their online account is hacked, it is appropriate to include it in the model we use in this study.

It follows that this study defines peer influence as a teenagers' belief that their friends would ridicule or gossip about them if someone hacked into their social media account. Given that the propensity to negative peer influence heightens in teenage years (Gardner & Steinberg, 2005), particularly through teasing (Brown, 2004), we argue that peer pressure incites teenagers to expose themselves to risk which could lead to violation of security guidelines. We argue that for teenagers between ages 13–16 in our study, being teased about being hacked incites risky behaviour (Gardner & Steinberg, 2005) and discourages them from complying. These findings give rise to the following hypotheses:

H12: Peer influence will have a negative effect on teenage intentions to comply with social media password guidelines.

The PMT Framework is generally used to predict behavioural intentions, operationalized as protection motivation (Maddux & Rogers, 1983; Rogers, 1975, 1983). This assumes that by measuring behavioural intentions we can predict actual behaviour (Prentice-Dunn & Rogers, 1986). A meta-analysis of PMT research suggests that PMT's influence on the results was significant, regardless of whether a study measures behavioural intention or actual behaviour as the dependent variable (Floyd, Prentice-Dunn, & Rogers, 2000; Milne & Milne, 2000). While behavioural intentions are assumed to predict behaviour (Ajzen, 1991; Fishbein & Ajzen, 2010), their actual effects are marginal (Floyd et al., 2000). As such, PMT studies began to examine behavioural intentions as well as actual behaviour (Boss et al., 2015; Milne & Milne, 2000). In this study, we examine the degree to which teenagers report their willingness to comply with social media security guidelines. We also examine the extent to which their intentions predict how they currently comply with social media password guidelines. To do this, we operationalized protection motivation as the intention to comply (e.g., I intend to follow….") and actual behaviour as the teenagers' current compliance with social media password guidelines (e.g., "I always follow the password guidelines…"). Please see the Appendix for the full list of measurement items. From these findings we hypothesize:

H13: Intentions to comply will have a positive effect on actual teenage compliance with social media password guidelines.

4 Methodology

In this section, we describe this study's participants, its design, and its measurement items. Our participants were recruited by TOUCH CyberWellness (TCW), Singapore, through cyber wellness courses they provide to participating secondary schools across Singapore. We randomly selected 246 students aged 13–16 years to participate in the study between November 2017 and May 2018. To ensure confidentiality and anonymity a randomly generated 6-digit Index Number was assigned to each participant before they completed our survey.

We chose the cut-off ages of 13 and 16 for two reasons. Firstly, because Facebook's starting age is 13 (DQ-Institute, 2018). Secondly, the peer influence on risky teenage behaviour peaks between 13 and 16 years (Gardner & Steinberg, 2005) and then declines with age (Steinberg, 2008).

4.1 Measurement development

To ensure the validity and reliability of this study's measurement items, we selected previously validated items and reworded them to reflect password threats. These items were measured on a 7-point Likert scale from (1) 'strongly disagree' to (7) 'strongly agree.' For example, we adapted the variables of perceived vulnerability (e.g., "There is a chance that someone could hack into my Social Media account") and perceived severity (e.g., "I believe that if someone successfully hacked into my Social Media account the consequences would be severe") from Zhang and McDowell (2009). The fear of threat (e.g., "The thought of someone hacking into any of my Social Media account frightens me") was adapted from Milne, Orbell, and Sheeran (2002). Perceived password effectiveness (e.g., "Making sure that my passwords are strong will protect my Social Media from hackers"), 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 anticipated feelings of embarrassment or guilt associated with personal norms (e.g., "I would feel guilty if my account was hacked"). Peer influence in this study relates to casual conversations between peers that involve teasing or gossiping (Brown, 2004), (e.g., "My friends would ridicule me if my Social Media account was hacked."). Please see Appendix for the full list of measurement items and item loadings.

5 Data Analysis and Results

This section entails an assessment of this study's measurement items and its structural model. Section 6 then discusses the results of our hypotheses and the implications of this study. The data was analysed using partial least squares, using SmartPLS 3.2.8 software (Ringle, Wende, & Becker, 2015) as PLS is appropriate for analysing complex models like ours with its many parameters and relationships (Lowry & Gaskin, 2014). That PLS predicts future behaviour rather than checking model fit (CB-SEM) also made it more appropriate to use for our study.

In total, 246 students aged 13–16 completed this study's survey on Qualtrics. Due to our participants' ages, and following our ethics requirements, we did not collect gender statistics. Only 9% of the participants reported that their social media account had ever been hacked. When asked if they knew anyone else whose account had been hacked, 40% said yes. A small proportion (25%) indicated that they do not use social media every day.

To assess the measurement items' significance and relevance, we used the PLS bootstrapping procedure for 5,000 subsamples (Hair et al., 2016). The measurement model was evaluated by using the recommended PLS-SEM measurement metrics (Hair et al., 2016) and is discussed in the following.

To confirm convergent validity, we used the average variance extracted (AVE) value—i.e., the average squared value across explained variance of the measurement items—and to assess each individual item's internal consistency we used composite reliability (CR) statistics. To establish convergent validity, AVE should be > or equal to 0.50, implying that each latent variable accounts for at least 50% of the indicators' variance. This study's AVE values were above 0.50, thus confirming convergent validity. The CR statistics and Cronbach's alpha (a measure of internal consistency) were at least 0.70, which confirms its internal consistency.

To assess discriminant validity, we used heterotrait-monotrait ratio (HTMT) statistics. Discriminant validity tests whether a latent variable does not correlate too highly with other latent variables, and whether any empirical distinction between latent variables exists (Hair et al., 2016; Henseler, Ringle, & Sarstedt, 2015). As recommended by Henseler et al. (2015), this study's HTMT values were below 0.850, and neither of the confidence intervals values included 1, suggesting that our model has no discriminant validity issues.

PLS has no established goodness-of-fit statistics (Hair et al., 2016). But as this study is not testing or comparing competing models, assessing goodness-of-fit is not necessary (Hair et al., 2016). Nonetheless, we elected to report the following recommended goodness-of-fit statistics for PLS (Hair, Risher, Sarstedt, & Ringle, 2019; Henseler & Sarstedt, 2013) The SRMR, which measures the gap between the estimated and the observed model, should be ≤ 0.08 (0.10); and

the NFI should be > 0.95 (0.90). Though this study's SRMR and NFI values were within what Henseler and Sarstedt recommend (2013), we report them cautiously (Hair et al., 2019).

We also assessed the structural model for collinearity issues, path significance and direction, and explanatory power. For collinearity issues, we evaluated each latent variable separately and ensured the VIF (variance inflation factor) values were ≤ 5 so no collinearity issues occurred in the structural model. The highest outer VIF was 3.778 (fear of threat item), and the lowest outer VIF value was 1.421 (intentions to comply item).

Common method bias checks whether surveys elicit any potential social desirability to answer questions in a certain way, or whether a surveys' instructions influence participants' answers. To check for common method bias, we examined the inner VIF values to ensure they were all <3 (Kock, 2015) and found no evidence of method bias. The highest inner VIF was 1.669 (perceived password effectiveness), and the lowest inner VIF value was 1.000 (intentions to comply). Based on the inner VIF values reported here, we found no evidence of measurement method bias. Then using the PLS bootstrapping method we assessed our model's significance of path coefficients and whether its relationship directions are relevant. All p-values ($p < 0.05$) for the indicators are significant, confirming the relevance of the indicators. A full list of these results is available upon request.

Hypothesized relationship		R^2	t-Statistic	Explanatory power	f^2	Strength
H4	Perceived vulnerability → Fear of threat	0.355	1.386	Moderate	0.051	Weak effect
H5	Perceived severity → Fear of threat	0.355	2.259	Moderate	0.442	Strong effect
H1	Perceived vulnerability → Intentions to comply	0.567	0.204	Moderate	0.007	Weak effect
H3	Fear of threat → Intentions to comply	0.567	0.043	Moderate	0.001	Weak effect
H2	Perceived severity → Intentions to comply	0.567	0.266	Moderate	0.008	Weak effect
H9	Perceived severity → Personal norms	0.103	1.864	Weak	0.114	Weak effect
H6	Perceived password effectiveness → Intentions to comply	0.567	0.910	Moderate	0.075	Weak effect
H7	Password self-efficacy → Intentions to comply	0.567	1.278	Moderate	0.259	Moderate effect
H8	Perceived cost → Intentions to comply	0.567	0.164	Moderate	0.003	Weak effect
H11	Personal norms → Intentions to comply	0.567	0.944	Moderate	0.071	Weak effect
H12	Peer influence → Intentions to comply	0.567	0.887	Moderate	0.054	Weak effect
H13	Intentions to comply → Actual compliance	0.712	0.694	Moderate	2.473	Strong effect

Table 1. Explanatory power and effect size of the proposed model

Finally, we assessed the model's predictive relevance (Hair et al., 2019) by using R^2 and effect size f^2. R^2 measures the model's predictive accuracy and reflects variance in the endogenous latent variables, as explained by all exogenous latent variables. Effect size f^2 determines how much certain independent variables in the model explain the dependent variables, thereby

contributing to the R^2 level, where $f^2 \leq 0.02 < 0.15$ is a weak effect; 0.15 to < 0.35 is a moderate effect; ≥ 0.35 is a strong effect.

As indicated by the R^2 values in Table 1, the explanatory power of this study's model is weak to moderate, while the f^2 effect sizes range between weak and strong. The paths between the PMT constructs, peer influence, and personal norms produced an R^2 of 0.567 for intentions to comply. The path between intentions to comply and actual compliance was significant (0.844, p=0.000) and yielded an R^2 of 0.712. This means our model accounted for 56.7% and 71.2% of the variance for intentions to comply and actual password compliance, respectively. This is consistent with Boss et al. (2015), who also found a high correlation between computer users' backup intentions and their actual backup behaviour.

We also examine the effect size f^2 to determine how much the independent variables of this study's model explain the primary dependent variable of a participants' intention to comply with password guidelines. Password self-efficacy had the most effect size f^2 of 0.259, indicating a moderate effect on our target dependent variable (intention to comply). While most hypothesized paths are significant, the effect sizes are small, which further indicates a mediator relationship (Hair et al., 2016).

Table 2 shows that this study's H10 hypothesis—that personal norms mediate the relationship between perceived severity and intentions to comply with social media password guidelines—was supported. To assess this hypothesized mediator role, we examined its direct and indirect effects. The direct effect of perceived severity on compliance intention is not significant. The paths between perceived severity to personal norms to compliance intentions are significant, and the indirect effects are also significant (p=0.048; t=1.98). This indicates a full mediation (Carrión, Nitzl, & Roldán, 2017; Zhao, Lynch Jr, & Chen, 2010), and only the indirect effect through the hypothesized mediator variable of personal norms exists. This suggests that the impact of perceived threat severity on compliance intentions is fully transmitted with the help of personal norms.

Mediated path	Path coefficient	t-Statistic	Std. Dev	Effect
Perceived severity → Intentions to comply	-0.046 NS	0.699	0.105	Full mediation
Perceived severity → Personal norms	0.275***	4.390	0.073	
Personal norms → Intentions to comply	0.183*	2.328	0.111	

*p<0.05; **p < 0.01; ***p<0.001

Table 2. Results of the hypothesized mediated relationship

While the following section presents the results of our hypotheses, a discussion of these results is outlined in Section 6. Table 3 also presents the results of our path analysis.

Table 3 shows that H4 and H5 are supported as both perceived vulnerability and perceived severity have a significant impact (p=0.004, $ß$=0.183; p=0.000, $ß$=0.540) on the fear of threat. It shows that H3 is not supported, however, the fear of threat has no significant effect (p=0.795, $ß$=-0.027) on intentions to comply.

As the threat component, that is perceived vulnerability and perceived severity have no significant influence (p=0.463, ß=0.063; p=0.485, ß=0.074) on intentions to comply, H1 and H2 are also not supported. As for the coping appraisal component, only perceived cost has no significant negative influence (p=0.554, ß=-0.046) on intentions to comply, meaning H8 is not supported either. Perceived password effectiveness has a significant effect (p=0.039, ß=0.275)

on intentions to comply, which supports H6. Password self-efficacy has a significant effect (p=0.000, ß=0.499) on intentions to comply, supporting H7. Intentions to comply has a strong and significant impact (p=0.000, ß=0.844) on actual compliance with password guidelines, supporting H13. Among all antecedent constructs, password self-efficacy has the strongest total effect (0.421) on actual compliance.

Hypothesized paths	Path Coefficient	Std. Dev	t-Statistic	*p-value*	Support
Perceived vulnerability → Fear of threat	0.183	0.062	2.925	0.004	Supported
Perceived severity → Fear of threat	0.540	0.077	6.986	0.000	Supported
Perceived vulnerability → Intentions to comply	*0.063*	0.086	0.736	*0.462*	Not supported
Fear of threat → Intentions to comply	*-0.027*	0.103	0.260	*0.795*	Not supported
Perceived severity → Intentions to comply	*0.074*	0.105	0.699	*0.485*	Not supported
Perceived severity → Personal norms	0.320	0.073	4.390	0.000	Supported
Perceived password effectiveness → Intentions to comply	0.275	0.133	2.066	0.039	Supported
Password self-efficacy → Intentions to comply	0.499	0.132	3.790	0.000	Supported
Perceived cost → Intentions to comply	*-0.046*	0.077	0.592	*0.554*	Not supported
Personal norms → Intentions to comply	0.259	0.111	2.328	0.020	Supported
Peer influence → Intentions to comply	-0.219	0.099	2.203	0.028	Supported
Intentions to comply → Actual compliance	0.844	0.059	14.337	0.000	Supported

Table 3. Path coefficients

The paths for our proposed PMT model extension are all significant. Peer influence has a significant negative impact (p=0.028, ß=-0.219) on intentions to comply, supporting H12. And personal norms have a significant positive influence (p=0.020, ß=0.259) on intentions to comply with password guideline, which supports H11.

The results for the structural model of this research are shown in Figure 1. However it shows that the threat component of our adapted PMT (Rogers, 1983) model had no direct influence on intentions to comply, rejecting H1, H2, and H3. Perceived vulnerability, perceived severity, and fear of threat had no impact on the teenagers' intentions to comply with social media password guidelines. As hypothesized in H4 and H5, fear of threat stems from perceptions of vulnerability and threat severity.

The coping appraisal of the research model we derived from PMT (Rogers, 1983) better predicts compliance intentions. Perceived password effectiveness and password self-efficacy had a significant influence on compliance intentions, which supports H6 and H7. This suggests that teenagers' motivation to comply with social media password guidelines depends on their belief in whether the recommended password security measure is effective, and they are confident in protecting their social media accounts from hackers. Perceived cost did not affect compliance intentions, which rejects H8.

As hypothesized, peer influence has a significant but negative impact on teenagers' compliance intentions, supporting H12. Contrary to peer influence, we found that personal norms have a positive impact on teenagers' compliance intentions, which supports H11.

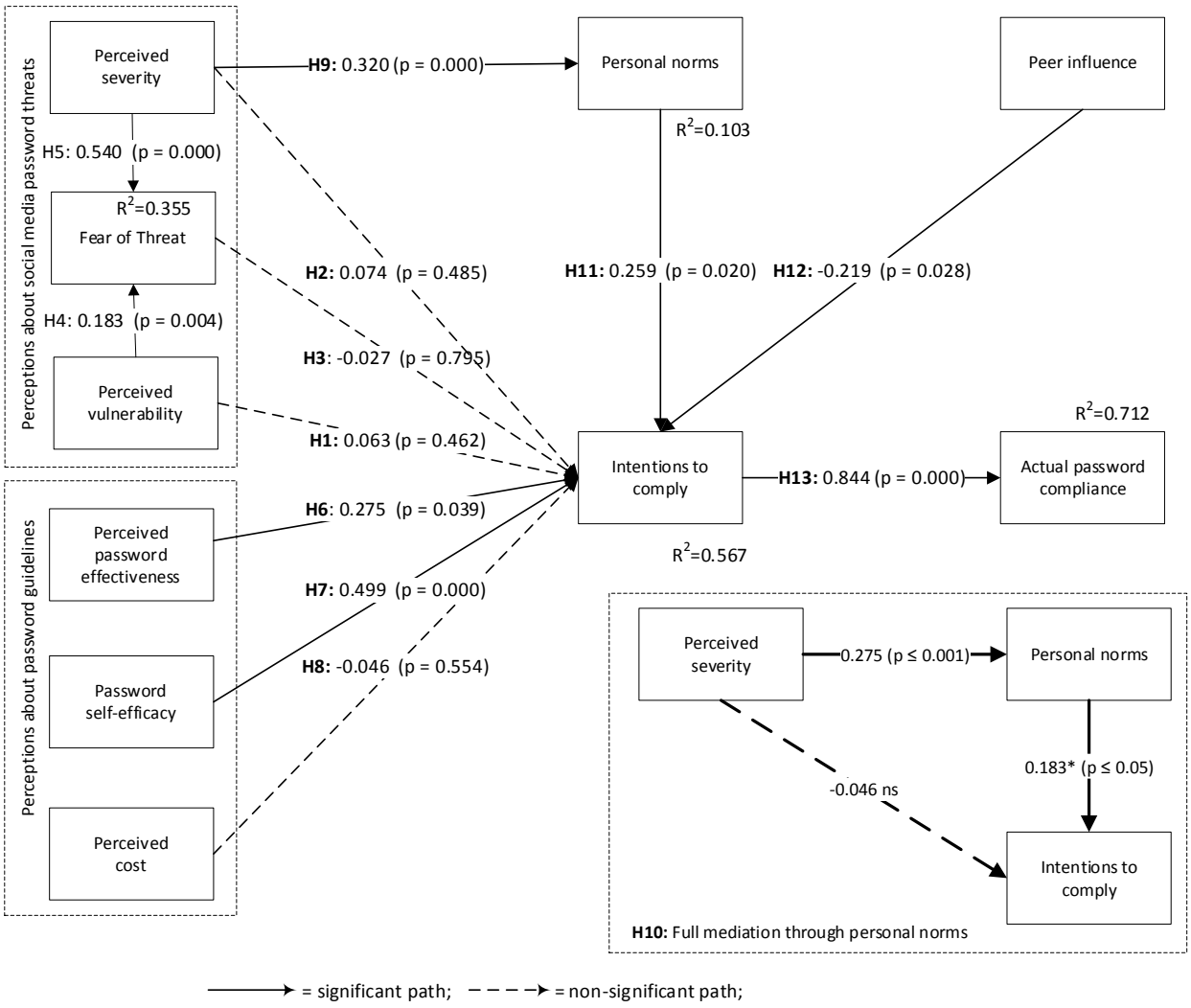

Figure 1. Proposed Research Model Results

This study also explored the extent to which teenager's compliance intentions can predict their actual compliance. Behavioural intentions are assumed to predict behaviour (Ajzen, 1991; Fishbein & Ajzen, 2010). However, since the effects of the relationship are marginal (Floyd et al., 2000), PMT studies examine behavioural intentions as well as actual behaviour (Boss et al., 2015; Milne & Milne, 2000). Consistent with Boss et al. (2015), we found a strong relationship between intentions and compliance, which supports H13.

6 Discussion and Conclusion

We identified three gaps in literature on cyber security behaviour, including that there is little research focusing on teenage security behaviour and also a lack of theory-based research focusing on teenage security behaviour. To address this, and as discussed, we proposed a research model derived from PMT (Rogers, 1983) to investigate what drives teenagers to comply with security guideless on social media. Given the role peers play in teenagers' protective and risky security behaviours (ACMA, 2011; Gardner & Steinberg, 2005; Soh et al., 2018; Somerville et al., 2013), our model extended the PMT model to explore the roles that personal norms and peer influence might play. In all, our model investigated the role of

security perceptions, perceptions about security recommendations, peer influence, and personal norms on teenage compliance intentions.

We found that perceived vulnerability, perceived severity, and fear of cyber threat do not influence teenagers' compliance intentions. Also, if teenagers believe there is a chance someone might hack into their social media account, it will not affect their compliance with security guidelines. And they are surprisingly unlikely to follow password measures recommended by their social media service, even if they believe being hacked would be detrimental or that the consequences of having personal information stolen would be severe. Contrary to PMT (Rogers, 1983) and findings in other IS-related PMT studies (e.g., Boss et al., 2015; Mwagwabi et al., 2018; Posey et al., 2015), we found that the fear of threat did not influence compliance intentions. This is an interesting revelation; even the thought of someone hacking their account or successfully cracking their passwords does not evoke enough emotional response to make teenagers want to protect their social media account.

This finding highlights a potential difference between adults and teenagers in threat appraisal and decisions about whether to comply with or ignore recommended security measures. A likely reason for this finding is that teenagers tend to underestimate their online vulnerability (Lwin et al., 2012). In fact, of the 246 teenagers who participated in our study, only 9% reported their social media account had been hacked. Yet 40% indicated they knew someone else whose social media account had been hacked. This tendency to underestimate their susceptibility to cyber threat is a phenomenon Weinstein (1984) described as 'optimistic bias'; individuals—like the teenagers in our study—tend to believe that adverse events are less likely to happen to them. This tendency to discount their online susceptibility appears to affect their motivation to carry out recommended security guidelines. Another possible reason for this is that the emotional response to threat proposed in PMT (Rogers, 1983) may play a lesser role in guiding teenage behaviour. Our findings show that teenage emotions such as embarrassment and guilt play a more significant role (Burnett et al., 2009).

Consistent with our findings, the anticipated embarrassment or guilt associated with personal norms better predict teenagers' security compliance. While fear of threat did not influence our participants, feeling embarrassed or ashamed about an account being hacked appears to be a better driver of teenagers' compliance. It is possible to derive from this that the teenage cognitive threat appraisal process proposed in PMT (Rogers, 1983) differs from adults, likely because they are at different stages of cognitive development (Lwin et al., 2012; Steinberg, 2008); the brain's cognitive control system changes during the teenage years such that, and as Steinberg (2008) explains, the adolescent stage is when the brain is sensitive to peer evaluation and seeks risky behaviour. This explains why teenagers' concern for feeling embarrassed or ashamed is a better predictor of their compliance intentions. A key revelation that stems from this is that teenagers' concern about feeling embarrassed or ashamed if their account was hacked into is highly likely to drive security behaviour, while the fear of someone actually hacking into their social media account does not motivate them take security measures.

Consistent with prior IS security research (e.g., Boss et al., 2015; Posey et al., 2015), we found that self-efficacy and perceptions that strong passwords will protect social media accounts have a positive impact on the teenagers' willingness to comply with social media password guidelines i.e., coping appraisal is a good predictor of teenage compliance behaviour . This may be because social media use is prevalent among teenagers (DQ-Institute, 2018). Our results show that participants regularly use social media, which could explain their enhanced

confidence (self-efficacy) and their awareness of the value of available protective measures (perceived effectiveness).

One coping appraisal variable which is not supported in our study is perceived cost. Whether teenagers perceive that strong passwords are challenging to manage or that following the recommended security measures would require too much effort did not affect their willingness to follow strict password guidelines. One potential reason is linked to the teenagers' confidence level in their social media use (DQ-Institute, 2018).

Our findings reveal an interesting relationship between perceived threat severity and compliance intentions through personal norms: personal norms actually mediate the effect of perceived threat severity. This means that awareness of the adverse consequences of password security threat alone does not lead to compliance i.e., it is not sufficient to influence security behaviour in teenagers. However, they feel morally obligated or guilty about not complying, which means their awareness of the adverse consequences of security threats plays a vital role in forming their personal norms. So it is only when these two conditions are met that personal norms translate into compliance.

Since risk-taking behaviour increases from childhood and heightens between 13–16 years of age (e.g., Gardner & Steinberg, 2005; Somerville et al., 2013; Steinberg, 2008), we explored the role peer influence plays in security behaviour. Our findings suggest peer influence plays a significant role in teenagers' risky security behaviours by negatively influencing their willingness to protect their social media accounts. Peer influence, which in this study relates to being teased about their accounts being hacked, appears to discourage teenagers from following recommended security measures. Interestingly, our findings are consistent with prior research (e.g., Gardner & Steinberg, 2005; Somerville et al., 2013; Steinberg, 2008), meaning we all agree that risky behaviour linked to peer influence peaks at 13–16 years of age. Even when teenagers at this age are aware of the adverse consequences of cyber risk (Gardner & Steinberg, 2005), risk-taking, particularly in their peers' presence, increases. This explains why our study found that peer pressure, such as when teenagers are teased about their social media accounts being hacked, discourages compliance. This is an interesting finding that opens new avenues for future research about IS security behaviours and whether the negative peer influence observed in our 13–16 year-old participants would decline with age.

7 Implications for Research and Practice

This research explored whether PMT (Rogers, 1983) can be used to predict security behaviour in teenagers. We found that while coping appraisal predicts compliance in teenagers, there are other motives outside of PMT that drive their security behaviour. Our study reveals two important research implications. Firstly, personal norms are a strong predictor of teenage security behaviours as they are driven more by feelings of guilt or embarrassment about their social media account being hacked than by their fear of being hacked.

Secondly, following the risky behaviour that occurs between ages 13–16 (Gardner & Steinberg, 2005), and because the teenagers in our study are in this age group, we argued that being teased about being hacked discourages teenagers from complying with recommended security guidelines and found this hypothesis to be true. This important finding suggests potential differences between adults and teenagers in security compliance behaviour. Peer influence has a dominant effect on risky behaviour in teenagers. For example, Albert et al. (2013) used brain

imaging to study teenagers' susceptibility to peer pressure and found they have a higher propensity for risky online behaviour when observed by peers.

Our study's findings suggest a difference between teenage and adult motives that drive their compliance behaviour. This highlights important implications for future research on IS security behaviour, which would benefit from investigating differences in adult and teenage behaviours. These potential differences draw interesting questions about whether the phenomena observed in our 13 –16 year-old participants would hold in adults, and how this could be important in tailoring cyber security training for teenagers.

Our study used PMT (Rogers, 1983), a protection motivation framework, to explain the underlying security motivation of teenagers. While our data largely supports our hypotheses, it is important to note that our model yielded weak to moderate explanatory power and weak to strong effect sizes. Though our hypothesized relationships were supported, the relationship strength ranged from weak to strong (Benitez, Henseler, Castillo, & Schuberth, 2020; Hair et al., 2019). While it is unlikely for all variables to have high effects sizes (Benitez et al., 2020), our study found that password self-efficacy had the most yet moderate effect size on the teenagers' willingness to comply with password guidelines. Consequently, while personal norms, peer influence, and perceived effectiveness of password measures influence teenage compliance intentions, the magnitude of impact these constructs had was small. From the motivational theory standpoint of our research model's case, the effectiveness of our tested variables to motivate teenagers to comply with security guidelines is medium to small. This raises questions about whether some motives are stronger than others, and if so, which ones they are. While our study found that PMT's coping appraisal is a good predictor of teenagers' security compliance, future studies could explore if motives beyond the PMT model may drive their security behaviour.

Self-determination theory (SDT) is one example of a motivational framework that could be used in future research of security behaviour. SDT provides a differentiated taxonomy of extrinsic motivation that explains why different motives produce different attitudes and outcomes (Ryan & Deci, 2000; Sheldon, Osin, Gordeeva, Suchkov, & Sychev, 2017). For example, following SDT's proposed extrinsic motivation continuum, peer influence—the least effective of the motivation types in our study—aligns with external motivation as teenagers are motivated by what others think. This motivation type was also found to have the smallest effect size of all the significant relationships in our research. With personal norms, on the other hand, teenagers are motivated to act because of internal pressure, such as feeling ashamed by not acting. According to SDT (Sheldon et al., 2017), this makes personal norms a more stable motive than peer influence. This is consistent with our results which found personal norms yielding a slightly larger effect size than peer influence.

Our studies also found that perceived password effectiveness yielded a slightly larger effect size than personal norms. Echoing the SDT taxonomy of extrinsic motivation (Sheldon et al., 2017), this indicates that perceived password effectiveness is a more stable motive than peer influence and personal norms. If teenagers see the value of such recommended measures, they are more motivated to comply with password guidelines.

In the context of our study, while protecting one's social media or online accounts is necessary, nothing about creating strong passwords is inheritably enjoyable. People do not do it out of intrinsic motivation (Ryan & Deci, 2000). This also indicates that teenagers must act on extrinsic motivation. As our study shows, motivation to comply with security guidelines

varied in its effect, which means that future research could explore what forms of motivation are effective and which are sustainable.

For practitioners of cybersecurity training for teenagers, this study provides insight into security compliance behaviours in teenagers. When using persuasive communication, the findings reveal that teenagers and adults are possibly different in the way they respond to cyber security threat stimuli. Consistent with Burnett et al. (2009), we found that fear has a less social role in guiding teenage behaviour concerning these threats. Instead we found that teenagers make decisions based on emotional feelings, so personal norms are more relevant to their decisions about protecting their social media than their fear of security threat. This suggests that there is value in targeting emotions based on personal norms rather than the fear of threat in practice.

In terms of coping mechanisms, as teenagers' perceived that recommended security measures are favourable, and their confidence in protecting their social media account increases, security guidelines are followed more frequently. Our study suggests that confidence in protecting their social media has the most influence in teenagers' willingness to follow recommended security measures. Cyber security campaigns for teenagers should therefore focus on enhancing teenagers' ability to create and maintain strong passwords. Further, cyber security training for teenagers should understand that teenagers will comply with security guidelines if they believe the recommended security measure is valuable.

Lastly, we found that teenagers' security practices are influenced by their peers. Since peer influence on risky behaviour is heightened between 13–16 years of age, as suggested by Gardner and Steinberg (2005), it may be necessary to remove any opportunity for risky security behaviour. In the context of password security for teenagers in this age group, instead of relying on security guidelines, password rules should be enforced at the authentication level to eliminate any opportunity to violate password rules.

8 Limitations

The project faced some significant data collection issues, including

(i) difficulty finding schools willing to participate in a cyber security study.

(ii) participant feedback showed they found the surveys lengthy and tedious. This is unsurprising as the participants were 13–16 years of age. Though we conducted a pilot test, future projects should focus on gauging a survey's completion time and target 10–15-minutes.

(iii) the data we collected was only from Singapore. This is because cultural differences can play a role in individual security behaviours (Menard, 2018). Future studies could consider examining security behaviours in teenagers across different countries.

(iv) the data we collected was from people between 13–16 years of age. Though we chose a cut-off age of 13 following Facebook's minimum age requirement, future studies could consider a wider age range, such as 13–18 years of age.

(v) we used Facebook as a proxy for wider social media use. While Facebook use is prevalent among teenagers, YouTube, Instagram, or Snapchat are also widely used (DQ-Institute, 2018; Ofcom, 2018). Future studies could consider teenagers' cyber security behaviours on platforms such as Instagram, YouTube, and Snapchat.

References

Ablon, L., Libicki, M. C., & 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.* Retrieved from https://www.acma.gov.au/-/media/mediacomms/Report/pdf/Like-post-share-Young-Australians-experiences-of-social-media-Qualitative-research-report.pdf?la=en

ACMA. (2013). *Young Australians' experience of social media: Quantitative research report.* Retrieved from https://www.acma.gov.au/-/media/mediacomms/Report/pdf/Like-post-share-Young-Australians-experience-of-social-media-Quantitative-research-report.pdf?la=en

ACMA. (2016). *Aussie teens and kids online.* Retrieved from https://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Research-snapshots/Aussie-teens-and-kids-online

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Albert, D., Chein, J., & Steinberg, L. (2013). The teenage brain: Peer influences on adolescent decision making. *Current directions in psychological science, 22*(2) 114–120. BBC. (2012). Hackers spread malware via children's gaming websites. *BBC Technology News*. Retrieved from https://www.bbc.com/news/technology-16576542

Benitez, J., Henseler, J., Castillo, A., & Schuberth, F. (2020). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. *Information & Management*, 57(2), 103–168.

Boss, S., Galletta, D., 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 (MISQ), 39*(4), 837–864).

Braue, D. (2020). Cyber attackers target children at home. *Australian Computer Society, ICT News*. Retrieved from https://ia.acs.org.au/article/2020/cyber-attackers-target-children-at-home.html

Brown, B. B. (2004). Adolescents' relationships with peers. *Handbook of adolescent psychology, 2.* 363–394.

Buckingham, D., Banaji, S., Carr, D., Cranmer, S., & Willett, R. (2005). *The media literacy of children and young people: A review of the research literature.* pp. 1–76. London: London Knowledge Lab.

Burnett, S., Bird, G., Moll, J., Frith, C., & Blakemore, S.-J. (2009). Development during adolescence of the neural processing of social emotion. *Journal of cognitive neuroscience, 21*(9), 1736–1750.

Carrión, G. C., Nitzl, C., & Roldán, J. L. (2017). Mediation analyses in partial least squares structural equation modeling: Guidelines and empirical examples. In *Partial least squares path modeling*. (pp. 173–195). Springer, Cham.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189–211.

Corron, L. (2018). *Social Cyber Threats Facing Children and Teens in 2018*. Retrieved from https://staysafeonline.org/blog/social-cyber-threats-facing-children-teens-2018/

Crossler, R. E., Andoh-Baidoo, F. K., & Menard, P. (2019). Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of US and Ghana. *Information & Management, 56*(5), 754–766.

Cybersafe.org. (2016). *Children's Internet Usage Study.* Center for Cyber Safety and Education. Retrieved from https://www.iamcybersafe.org/s/parent-research

De Groot, J. I. M. (2010). Morality and Nuclear Energy: Perceptions of Risks and Benefits, Personal Norms, and Willingness to Take Action Related to Nuclear Energy Morality and Nuclear Energy. *Risk analysis, 30*(9), 1363–1373. doi:10.1111/j.1539-6924.2010.01419.x

De Groot, J. I. M., & Steg, L. (2009). Morality and prosocial behavior: The role of awareness, responsibility, and norms in the norm activation model. *The Journal of social psychology, 149*(4), 425–449.

DQ-Institute. (2018). *Outsmart the Cyber-Pandemic: Empower Every Child with Digital Intelligence by 2020*. Retrieved from https://www.dqinstitute.org/wp-content/uploads/2018/08/2018-DQ-Impact-Report.pdf

Elek, E., Miller-Day, M., & Hecht, M. L. (2006). Influences of personal, injunctive, and descriptive norms on early adolescent substance use. *Journal of Drug Issues, 36*(1), 147–172.

Fishbein, M., & Ajzen, I. (2010). *Prediction and change of behavior: The reasoned action approach*. New York: Psychology Press.

Floyd, D., Prentice-Dunn, S., & Rogers, R. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology, 30*(2), 407–429.

Gardner, M., & Steinberg, L. (2005). Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study. *Developmental psychology, 41*(4), 625.

Grasmick, H. G., & Bursik Jr, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law and society review*, 837–861.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM).* Sage Publications.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. doi:10.1108/EBR-11-2018-0203

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science, 43*(1), 115–135.

Henseler, J., & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics, 28*(2), 565–580.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cyber security 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), 196–213.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS quarterly, 39*(1), 113-134.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration (IJEC), 11*(4), 1–10.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cyber security policy awareness on employees' cyber security behavior. *International Journal of Information Management, 45*, 13–24. doi:https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Livingstone, S., Mascheroni, G., & Staksrud, E. (2017). European research on children's internet use: Assessing the past and anticipating the future. *New media & society, 20*(3), 1103–1122. doi:10.1177/1461444816685930

Lowry, P. B., & 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), 123–146.

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of Adolescence, 35*(1), 31–41. doi:https://doi.org/10.1016/j.adolescence.2011.06.007

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

Maor, E. (2020). *Recycling Credentials in Four Easy Steps*. Retrieved from https://intsights.com/blog/recycling-credentials-in-four-easy-steps

Menard, P. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security, 75*, 147–166. doi:10.1016/j.cose.2018.01.020

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems, 34*(4), 1203–1230.

Milne, S., Orbell, S., & Sheeran, P. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of applied social psychology, 30*(1), 106–143.

Milne, S., Orbell, S., & 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), 163–184.

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

Ofcom. (2018). Children and parents: Media use and attitudes. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf

Onwezen, M. C., Antonides, G., & 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*, 141–153.

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.

Prentice-Dunn, S., & Rogers, R. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research, 1*(3), 153–161.

Ringle, C., Wende, S., & Becker, J.-M. (2015). SmartPLS 3. SmartPLS GmbH, Boenningstedt. *Journal of Service Science and Management, 10*(3).

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

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology* (pp. 153–176). New York: Guilford Press.

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary educational psychology, 25*(1), 54–67.

Schwartz, S. H. (1977). Normative influences on altruism. In *Advances in experimental social psychology* (Vol. 10, pp. 221–279). Academic Press.

Sheldon, K. M., Osin, E. N., Gordeeva, T. O., Suchkov, D. D., & Sychev, O. A. (2017). Evaluating the dimensionality of self-determination theory's relative autonomy continuum. *Personality and Social Psychology Bulletin, 43*(9), 1215–1238.

Soh, P. C. H., Chew, K. W., Koay, K. Y., & Ang, P. H. (2018). Parents vs peers' influence on teenagers' Internet addiction and risky online activities. *Telematics and Informatics, 35*(1), 225–236.

Somerville, L. H., Jones, R. M., Ruberry, E. J., & Dyke, J. P. (2013). The Medial Prefrontal Cortex and the Emergence of Self-Conscious Emotion in Adolescence. *Psychological science, 24*(8), 1554–1562. doi:10.1177/0956797613475633

Steinberg, L. (2008). A Social Neuroscience Perspective on Adolescent Risk-Taking. *Developmental review: DR, 28*(1), 78–106. doi:10.1016/j.dr.2007.08.002

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*(1), 1096–1100.

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

Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., & Sirivianos, M. (2016). *Cyber security risks for minors: a taxonomy and a software architecture.* Paper presented at the 2016

11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP).

Weinstein, N. (1984). Why it won't happen to me: Perceptions of risk factors and susceptibility. *Health Psychology, 3*(5), 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), 389–418.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3), 180–197.

Zhao, X., Lynch Jr, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of consumer research, 37*(2), 197–206.

Appendix

Constructs	Survey items and scale	Item Loadings
Actual compliance with password guidelines (Ajzen, 1991; Fishbein & Ajzen, 2010)	**Strongly disagree 1 | Strongly disagree 7**	
	I always follow the password guidelines suggested by my Social Media service.	0.721
	I always choose a password with a combination of numbers, letters and symbols.	0.794
	I always take measures to protect my Social Media account.	0.766
	For my social media accounts, I always choose strong passwords.	0.834
Intentions to comply with password guidelines (Floyd, Prentice-Dunn, & Rogers, 2000; Milne & Milne, 2000; Mwagwabi et al. 2018)	**Extremely unlikely 1 | Extremely likely 7**	
	I intend to choose a password with a combination of numbers, letters, and symbols as suggested by my Social Media service.	0.716
	I intend to follow the security measures recommended by my Social Media service.	0.747
	I intend to protect my Social Media account from hackers.	0.751
Perceived severity (Zhang and McDowell, 2009)	**Not at all severe 1 | extremely severe 7**	
	I believe that if someone successfully guessed my Social Media passwords the consequences would be….	0.774
	Having my Social Media account accessed by someone without my knowledge would be….	0.769
	If my personal information was stolen from my Social Media account, the consequences would be…	0.773
Perceived vulnerability (Zhang and McDowell, 2009)	**Strongly disagree 1 | Strongly disagree 7**	
	It is likely that someone could successfully guess my Social Media passwords.	0.776
	There is a chance that someone could successfully crack at least one of my Social Media passwords.	0.676
	There is a chance that someone could hack into my Social Media accounts.	0.864
	It is likely that someone would try to hack into my Social Media accounts.	0.693
	It is extremely likely that my Social Media account will be attacked in the future.	0.647
Fear of threat Milne, Orbell, and Sheeran (2002)	**Strongly disagree 1 | Strongly disagree 7**	
	The thought of someone hacking into any of my Social Media accounts frightens me.	0.868
	The thought of someone using my personal information from any of my Social Media accounts makes me worried.	0.827
	The thought of someone successfully cracking my Social Media passwords frightens me.	0.915

Constructs	Survey items and scale	Item Loadings
Perceived password effectiveness (Zhang and McDowell, 2009)	**Strongly disagree 1 | Strongly disagree 7**	
	Making sure that my passwords contain a combination of numbers, letters and special characters, will protect my Social Media account from hackers.	0.739
	Making sure that my passwords are strong will protect my Social Media account from hackers.	0.774
	I can protect my Social Media accounts better if I use strong passwords.	0.743
	The security measures recommended by my Social Media service are effective.	0.706
Password self-efficacy (Compeau and Higgins, 1995)	**Strongly disagree 1 | Strongly disagree 7**	
	I have the necessary skills to protect my Social Media account from hackers.	0.686
	I would be able to use strong passwords if I had a lot of time.	0.566
	I would be able to remember strong passwords if I had instructions on how to create memorable passwords.	0.739
	I am confident that I can protect my Social Media account from hackers.	0.786
Perceived cost (Milne et al. 2002)	**Strongly disagree 1 | Strongly disagree 7**	
	Strong passwords are difficult to remember.	0.743
	Strong passwords take too much effort to create.	0.878
	Strong passwords take too much time to type.	0.807
	If I change my passwords regularly, it would be difficult for me to remember them.	0.661
	Following the security measures recommended by my Social Media services is too much trouble.	0.678
Peer Influence (Brown, 2004)	**Strongly disagree 1 | Strongly disagree 7**	
	My friends would ridicule me if my account was hacked.	0.777
	My friends would think that I am "weak" if my account was hacked.	0.805
	My friends would gossip about me if my account was hacked.	0.885
Personal norms (De Groot, 2010; Schwartz, 1977)	**Strongly disagree 1 | Strongly disagree 7**	
	I would feel ashamed if my account was hacked.	0.844
	I would feel guilty if my account was hacked.	0.889
	I would feel embarrassed if my account was hacked.	0.851

Full list of survey measurement items and item loadings

doi: https://doi.org/10.3127/ajis.v25i0.2953