Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines

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

Tanya McGill
Murdoch University, Australia
T.Mcgill@murdoch.edu.au

Michael Dixon
Murdoch University, Australia
M.Dixon@murdoch.edu.au

Abstract

Passwords have long been the preferred method of user authentication, yet poor password practices cause security issues. The study described in this paper investigates how user perceptions of passwords and security threats affect intended compliance with guidelines and explores how these perceptions might be altered in order to improve compliance. It tests a research model based on protection motivation theory [24]. Two groups of internet users were surveyed, one of which received password security information and an exercise to reinforce it. This study suggests effective ways that trainers or employers can improve compliance with password guidelines. In particular, training programs should aim to enhance IS security coping appraisal. The research model proposed in this study has also been shown to be a useful model for explaining IS security behavioral intentions.

1. Introduction

Despite their weaknesses, passwords have long been the preferred method of user authentication [1]. To an organization, password based authentication is a cost effective and easy to implement alternative [2]. Yet to a user, passwords are considered annoying and difficult to remember [3-5]. This user attitude toward passwords has ultimately led to poor password practices such as re-using passwords online [6]. Further, recent password leaks [7, 8] show the prevalence of poor password practice, with passwords such as 123456 still in use online. With such passwords, users are increasingly vulnerable to hacking giving an attacker a small number of commonly used passwords to guess from or easy access to passwords by decrypting stolen password master files [9].

The aim of this study is to investigate factors that drive users to comply with password guidelines designed to ensure users create strong passwords. Yet, several studies have found that password guidelines have no influence on password strength [3-5, 10]. Furthermore, even when an additional feedback mechanism such as a password strength meter is used, users still select insecure passwords [11]. One issue with password guidelines is that they vary greatly from site to site and presenting users with inconsistent password guidelines has a negative effect on user attitude and password practices [12]. Yet given the variety of password guidelines that exist and the motivation for advertisement-driven websites to reduce requirements to improve traffic [10], variations in password guidelines are likely to be a long term issue. Whilst approaches such as passphrases have shown some promise [13], negative attitudes among users will continue to affect compliance with password policies. It is therefore important to focus on ways to improve compliance with password guidelines and to encourage use of strong passwords.

Another issue with passwords is that users struggle to remember a series of random characters or strong passwords [3]. As the human brain can only memorize a sequence of five to nine non-arbitrary objects [14], it is not surprising that remembering passwords is considered one of the most challenging aspects of password usage [15] leading to a lack of motivation to comply with password policies [4, 10, 12]. Studies have linked this lack of motivation to how users perceive security threats [12, 16]. Users hold different perceptions about security, which affect their choices about security policy compliance [16, 17]. Additionally these perceptions can be manipulated to improve compliance with security policies [17] and to enhance actual password strength [11].

The study described in this paper is centered on concepts pertaining to security perceptions, and investigates how user perceptions of passwords and security threats affect intended compliance with guidelines and explores how these perceptions might be altered in order to improve compliance.

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.396

2. Related literature

2.1. Information security perceptions

Users' intentions to comply with recommended security measures are believed to be a function of how they perceive security risks [16, 18, 19], including perceptions of how likely a threat is to occur, how vulnerable they feel and the perceived consequences of the threat. Users' decisions to apply security measures have been shown to be driven in part by their assessment of the severity of a computer related threat [16]. However, although several attempts have been made to investigate the role of perceived vulnerability, findings have so far been mixed [16, 18, 20].

The literature also proposes that how users perceive security measures has an impact on their intentions to adopt them [17, 21]. In particular, user perceptions about the effectiveness of the security measures [16, 18, 21], and user assessments of their ability to effectively use the security measures [17], will influence their intentions. However, as several studies have shown [16, 18, 21, 22], users are less likely to apply security measures if they are perceived as a barrier or difficult to use.

Lack of computer security awareness [23] and lack of knowledge of how to apply security measures [16], have also been identified as contributing factors to poor security practices. It has been argued that if security knowledge is made more accessible, users are more likely to be motivated to practice security [16]. For example, Johnston et al. [17] used persuasive messages highlighting the dangers of spyware to influence user security perceptions and found that user intentions were influenced by using persuasive messages. Similarly, Vance et al. [11] demonstrated that interactive fear appeals can help improve password security.

2.2. Theoretical background

Protection Motivation Theory (PMT) [24] proposes that how an individual assesses risks (threat appraisal), determines whether they are likely to comply with preventative measures. PMT also suggests that the likelihood that an individual will comply with recommended precautions is dependent on how they perceive the recommended preventative measures in terms of effectiveness, their ability to perform them, and any perceived difficulties associated with the preventative measures (coping appraisal) [24, 25]. Rogers [25] developed PMT to include the concept of fear appeals, messages hypothesized to initiate threat and coping appraisal processes and ultimately change behavior.

Threat appraisal factors include (i) *perceived severity* or judgment about the severity of a threat, and (ii) *perceived vulnerability* or judgment about an individual's vulnerability to threat. These are believed to play a role in deterring individuals from destructive behaviors. Coping appraisal factors include (i) *self-efficacy* or judgment about an individual's ability to perform a preventative measures and (ii) *response efficacy* or judgment about the effectiveness of the proposed preventative measure. *Self-efficacy* and *response efficacy* are crucial in promoting use of preventative measures while *response cost* or judgment about how difficult, complex, or inconvenient a precautionary measure is, is a factor associated with an individual's decision not to undertake the recommended preventative activity.

In drawing a parallel between health related preventative behaviors and computer related preventative behaviors, a growing number of information systems (IS) security studies have adopted PMT to investigate factors that affect adoption of information security preventative measures [e.g. 16, 17, 20, 22, 26].

With the exception of Siponen et al. [27], who combined perceived severity and perceived vulnerability items to form a single threat appraisal construct, recent IS security research has examined the direct effects of individual threat appraisal and coping appraisal factors on IS security practice (e.g. perceived vulnerability and perceived severity [16, 18, 20, 21], response efficacy and self-efficacy [16-18, 20, 21], and response cost [16, 18, 20, 21, 27]). This study examines the direct effects of threat appraisal factors and coping appraisal factors on compliance with password guidelines, and explores possible relationships between the threat appraisal factors.

3. Research model

Figure 1 presents the research model for this study. The model shows the proposed relationships between threat appraisal and coping appraisal factors, and the dependent variable, user *intentions to comply* with password guidelines. Based on the PMT [24] construct *protection motivation, intentions to comply* represents the degree to which a user intends to follow a set of recommended password security guidelines. The following sections describe the key aspects of the model.

3.1. Fear appeals

As defined in PMT, fear appeals are persuasive messages aimed at motivating individuals to engage in a recommended behavior [24, 25]. This study defines *fear appeals* as persuasive messages containing information that emphasize the severity of password related threats and the likelihood of being exposed to such threats. In this study, *fear appeals* also include statements about the effectiveness of recommended password guidelines and training on how to create strong passwords that are also easy to remember. In IS security studies fear appeals have been found to have a significant influence on users' intentions to comply with recommended spyware security policies [17] and have been shown to encourage strong password usage [11, 18]. In this study, it is hypothesized that *fear appeals will* ***increase*** *user intentions to comply with password guidelines*.

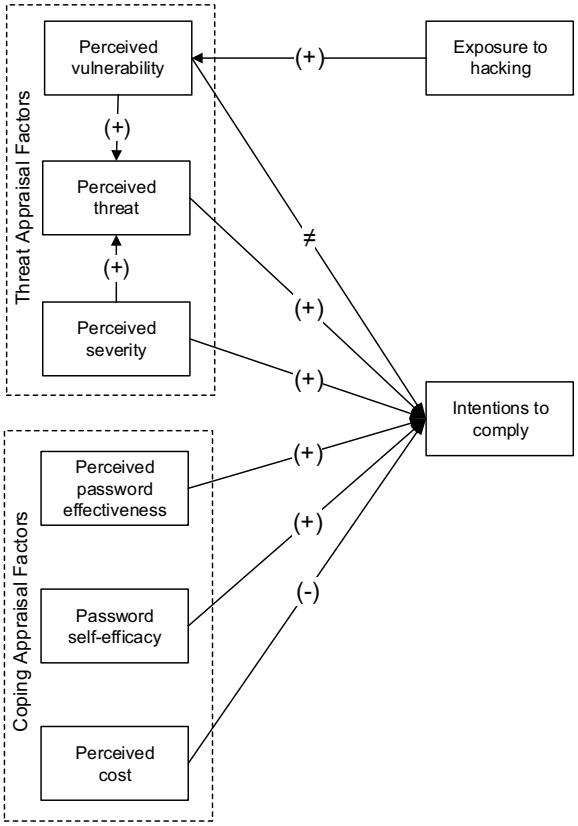

Figure 1. Research model

3.2. Threat appraisal factors

PMT suggests that threat appraisal factors have an impact on compliance with recommended precautions [24, 25]. In this study, *perceived severity* relates to the degree to which a user believes that the consequence of password related threats would be severe. Higher severity perceptions have been found to increase the likelihood of compliance with recommended precautions [24, 25]. Therefore, if a user believes that the consequences of being hacked into would be detrimental it is proposed that they are more likely to comply with password security recommendations. Woon et al. [16] found a direct effect of perceived severity on wireless security behavior and Lee et al. [21] also found a direct effect on intention to install anti-malware software. Therefore, it is hypothesized that *increasing a user's perceived severity of password related threats will* ***increase*** *intentions to comply with password guidelines.*

Perceived vulnerability relates to the degree to which a user believes that they are likely to experience password related threats. Although PMT suggests that perceived vulnerability has a direct impact on compliance with recommended measures, several IS security studies have had mixed findings [16, 18, 20, 21], failing to support a direct effect of perceived vulnerability on behavior. Further, Liang et al. [19] found that perceived vulnerability had an indirect effect on behavior and that the relationship is mediated by perceived threat, potentially explaining the mixed findings in studies that have only examined direct effects on behavioral intentions. Therefore, it is hypothesized that *perceived vulnerability to password related threats will* ***not have a direct effect*** *on intentions to comply with password guidelines.*

This study also examines the possible role of previous exposure to threat on vulnerability perceptions. Prior exposure to threats is a form of acquired knowledge that could influence an individual's perceptions about their vulnerability to threats [28]. This acquired knowledge can be from a threat incident experienced by an individual (direct) or someone they know personally (indirectly) [28, 29]. In this study, *exposure to hacking* is defined as prior exposure to a hacking incident, experienced by either a user, or someone they know personally. If a user or someone they know personally has had their online account hacked into, their *perceived vulnerability* should increase [30]. Therefore, it is hypothesized that, *exposure to hacking will* ***increase*** *users' perceived vulnerability.*

Perceived vulnerability and *perceived severity* trigger an emotional feeling towards threat. In PMT literature, this is referred to as fear arousal described using mood adjectives such as frightened or worried [24, 31]. In this study, *perceived threat* relates to the degree to which a user is worried about password related threats. PMT proposes that increased fear arousal or perceived threat increases the likelihood that an individual will comply with recommended

precautions [24]. In a password related study, Zhang et al. [18] found that users who are nervous about password hacking are more likely to implement password protection measures. It is therefore hypothesized that *increasing a user's perceived threat will **increase** intentions to comply with password guidelines.*

Herath et al. [26] examined the relationship between perceived vulnerability and perceived severity and fear arousal (level of concern). Their study found that perceptions of severity increased the level of concern about security breaches. However, they did not find a significant relationship between perceptions of vulnerability to threat and level of concern for security. Based on the concept of fear arousal, if a user believes that there is a high likelihood of being hacked into, their *perceived threat* will increase. Similarly, if a user believes that hacking can cause serious harm they are more likely to show higher levels of *perceived threat*. Therefore, it is hypothesized that *elevating a user's perceived vulnerability and perceived severity will increase their level of perceived threat.*

3.3. Coping appraisal factors

In this study, the constructs *perceived password effectiveness*, *password self-efficacy* and *perceived cost* are synonymous with PMT's [24] response efficacy, self-efficacy and response cost respectively.

Perceived password effectiveness relates to the degree to which a user believes that recommended password guidelines will prevent password threats. PMT proposes that the higher the level of perceived effectiveness the higher the probability of compliance with recommended precautions [24], and this has been confirmed in several IS security studies with home computer users [16] as well business executives [21]. In addition, perceived effectiveness was found to be the strongest predictor of behavioral intentions in a password related study [18]. This suggests that if a user believes that recommended password security measures will effectively prevent password hacking they are more likely to comply with security measures. It is therefore hypothesized that *increasing perceived password effectiveness will **increase** intentions to comply with password guidelines.*

Password self-efficacy relates to the degree to which a user is confident in their ability to create a strong password. PMT was revised by Maddux et al. [24] to include the construct self-efficacy. The revised PMT suggests that, in addition to beliefs about the effectiveness of the recommended precautionary measures, an individual's beliefs about their ability to perform the recommended measures have a positive influence on behavioral intentions [24, 32]. This sense of self-efficacy determines whether or not they would choose to undertake challenging tasks such as creating strong passwords. In IS security research, self-efficacy has been shown to have a positive effect on users' intentions to use spyware software [17], implement recommended wireless security measures [16], and install anti-malware software [21]. If a user is confident about their ability to create a strong password they should be more likely to comply with password security recommendations. It is therefore hypothesized that *increasing password self-efficacy will **increase** intentions to comply with password guidelines.*

Perceived cost relates to the degree to which a user believes that remembering passwords would be difficult if password guidelines were followed. IS security related PMT studies [e.g. 16, 18, 20, 21] have shown that users who believe that carrying out computer security measures is difficult are less likely to comply with security measures. Therefore, it is hypothesized that increasing *perceived cost will **decrease** intentions to comply* with password guidelines.

4. Research methodology

To test the research model shown in Figure 1 and examine the effectiveness of fear appeals for improving password practices, data was collected from two groups of participants forming the control and treatment groups. While the same model and hypotheses were tested for both groups, the treatment group's procedure included password security information and an exercise to reinforce it.

4.1. Respondents and procedure

The target population for this study was internet users who hold at least one online email account. To obtain this sample of internet users with a wide range of backgrounds, a third party recruiting company Authentic Response Inc. was used and participants were recruited through email invitations.

Each group completed a separate survey administered online using SurveyGizmo. The control group questionnaire, completed in approximately 15 minutes, measured background information (including self-reported knowledge of computer security) and the study variables: *exposure to hacking*; *perceived severity*; *perceived vulnerability*; *perceived threat*; *perceived password effectiveness*; *perceived cost*, *password self-efficacy*; and *intentions to comply* with password guidelines. The treatment group survey, completed in approximately 25 minutes, consisted of

the same items plus a password security information and exercise section (copies of the questionnaire items and training material can be obtained from the authors). As the intention was to influence participants' perceptions, the training session was completed after the collection of background information, but prior to collection of data relating to the model.

In order to ensure validity and reliability of the items, previously validated items were adopted where possible. With the exception of *exposure to hacking*, and *intentions to comply,* all items were treated as a 7-point Likert-type scale. *Exposure to hacking* consisted of two items measured from (0) for 'no' experience of being hacked to (7) for 'high impact'. Participants were asked to indicate if they or someone they know had ever had their online account hacked into and to indicate the degree to which the experience affected them. The items were adapted from Boss [29]. The items to measure *perceived severity* and *perceived vulnerability* were adapted from Boss [29] and Zhang and McDowell [18]. The items to measure *perceived threat* and *perceived cost* were adapted from Milne et al. [33]. *Perceived password effectiveness* was measured using items adapted from Zhang and McDowell [18] and *password self-efficacy* with items from Compeau and Higgins [34]. The items to measure *intentions to comply* were adapted from Bulgurcu et al. [35] and measured on a 7-point scale where (1) was labeled 'not at all likely' and (7) was labeled 'very likely'.

The password security information and exercise were developed using material from NIST [36], US-CERT [37] and Certified Information Systems Security Professional (CISSP) [1].

Using census balanced random sampling (a form of stratified random sampling), 3830 email invitations were distributed. 459 surveys were completed, of which, 419 (209 control and 210 treatment) were valid completions (10.9% valid response rate).

4.2. Data analysis techniques

One-way between groups ANOVA was used to determine whether levels of the threat appraisal factors, coping appraisal factors, *exposure to hacking* and *intentions to comply* with password guidelines, differed across the two groups. The hypothesized model was tested using structural equation modeling (SEM). As recommended, a two-step approach to SEM was used where the validity of the measurement model is assessed before the structural model is tested [38].

The measurement model step involves testing for construct validity and assessment of how well the observed data fits the hypothesized model. Construct validity is demonstrated when the hypothesized latent constructs are shown to be distinct from each other (discriminant validity) and when the observed variables have high factor loadings on the construct they represent (convergent validity). Construct reliability (CR) and average variance extracted (AVE) are used as a measure of convergent validity. Discriminant validity was assessed using AVE, where AVE values of two latent constructs should be greater than the square of the correlation between them.

A measurement model is said to be of good fit if the difference between the observed data and the hypothesized model is small [38]. This study reports the following fit indices and uses the associated cutoff values; absolute indices: Chi-square (χ^2), Normed chi-square ($\chi^2/df;$ 1-2), Standardized Root Mean Residual (SRMR; < 0.6-0.8) and Root Mean Squared Error of Approximation (RMSEA; <0.5-0.8); incremental indices: Comparative Fit Index (CFI; >0.95) and Tucker-Lewis Index (TLI; >0.95).

Once goodness of fit and validity of the measurement model is assessed, the structural model is then usually tested. However, in case of a multi group study, such as this one, the observed variables are first examined to ensure that they are equivalent and behave the same way across groups [39]. To test for model equivalence a previously established good fitting model and a model where all paths are constrained (assumed) equal, are compared. If the chi-square-square difference ($\Delta\chi^2$) is significant, then the two models are not equivalent. To claim model equality, a non-significant $\Delta\chi^2$ *p-value* is sought [38]. Following this, the structural models are tested. This involves model fit assessment and path analysis.

5. Results

5.1. The participants

Of the 419 participants, 42.1% were male and 57.9% female. For both groups, the majority of participants were female, 56.8% and 58.9% for control and treatment groups respectively. Ages ranged from 18 to 84 for the control group and 18 to 85 for the treatment group.

In both groups most participants, 81.6% (control) and 86% (treatment) had three or less email addresses, with 58.4% (control) and 67.1% (treatment) indicating that they had used a 7 to 10 character password voluntarily. Most participants had changed passwords voluntarily, 68.4% (control) and 71.2% (treatment) and only 15.7% and 20.1% of the control and treatment group respectively had ever shared passwords.

Both groups perceived themselves as having average or above average computer skills and

knowledge of computer security with only 8.6% of the control group and 6.2% of the treatment group rating their computer skills as below average. Slightly more indicated that they had a below average knowledge of computer security: 15.3% and 12.4%.

5.2. Assessment of measurement model

Assessment of the measurement model was conducted separately for threat appraisal factors, coping appraisal factors, and *intentions to comply*. Measurement items for the control and treatment groups were also assessed separately.

A single composite score was created for *exposure to hacking* using regression imputation in AMOS, Version 19. As this construct is not part of PMT, and therefore considered exploratory for this study, Cronbach's Alpha of 0.738 (treatment) and 0.633 (control) was considered acceptable.

Item reliability for the other constructs (for both the control group and the treatment group) was acceptable with CR ranging from 0.846 to 0.976 indicating that there were no convergent validity issues. AVE values were all greater than the CR values (0.526 to 0.889) and also greater than 0.5 indicating that there are no convergent validity issues [38]. Discriminant validity was also met given the large AVE values.

5.3. Assessment of model equivalence

The results of the equivalence test suggested that the control and treatment group threat appraisal models are equivalent. The chi-square difference ($\Delta\chi^2$) test yielded a non-significant $\Delta\chi^2$ *p-value* (0.568) suggesting that the fully constrained and unconstrained models are not significantly different and therefore the two models are equivalent. Although an initial $\Delta\chi^2$ test for the coping appraisal models suggested that the two models were significantly different ($\Delta\chi^2$ *p=0.034*), un-constraining one item yielded a non-significant $\Delta\chi^2$ *p-value* (0.136) suggesting that the two models are partially equivalent. Partial equivalence is acceptable and SEM analysis can still proceed if at least two items per latent variable are found to be equal [38]. Likewise, the $\Delta\chi^2$ test for *intention to comply* suggested partial equivalence ($\Delta\chi^2$ p = 0.063), which is adequate.

5.4. Assessment of fear appeals

The hypothesis associated with the impact of fear appeals was tested using one-way ANOVA, and the results are reported in Table 1. They show that with the exception of *perceived cost*, the treatment group showed significantly higher levels of the threat appraisal and coping appraisal factors, and their *intentions to comply* with password guidelines were significantly higher than those of the control group. Fear appeals therefore appear to influence intention to comply with password guidelines as hypothesized.

5.5. Assessment of structural model

Model fit for the nested (control and treatment) model was acceptable. The χ^2 was 1220.024 with 711 degrees of freedom (χ^2/df=1.716). The χ^2 p-value was significant (p<0.001) which is expected for a sample size greater than 200. The CFI (0.947), TLI (0.94) and RMSEA (0.042) indicated good fit for a complex model and the SRMR statistic of 0.093 was also acceptable [38]. Following the assessment of model fit, the structural model was examined.

Table 1. One-way ANOVA results

Construct	Control means	Treatment means	p-value
Exposure to hacking	1.193	1.939	0.000
Perceived vulnerability	3.645	4.358	0.000
Perceived threat	5.235	5.569	0.016
Perceived severity	4.361	4.654	0.033
Perceived password effectiveness	4.736	5.787	0.000
Password self-efficacy	5.220	5.525	0.011
Perceived cost	4.746	4.897	0.275
Intentions to comply	5.286	6.224	0.000

As can be seen from Table 2, the majority of hypothesized paths were significant. As posited *perceived threat* was shown to be a function of *perceived vulnerability* and *perceived severity,* and *exposure to hacking* was also shown to have a significant impact on *perceived vulnerability* as proposed. Also, as proposed, *perceived vulnerability* was shown not to have a significant direct effect on *intentions to comply*. However, although *perceived threat* was found to directly influence *intentions to comply*, contrary to what was proposed, *perceived severity* did not directly influence *intentions to comply* in either group. In the coping appraisal component of the model, *perceived password effectiveness* and *password self-efficacy* were shown to significantly influence *intention to comply*, for both groups. However, contrary to what was proposed, *perceived cost* was not found to influence *intention to comply* in either group.

The predictive power of the control and treatment group models was found to differ. The treatment group model had a stronger predictive power (R^2 = 0.53) than the control group model (R^2 = 0.43).

Table 2. Hypotheses results

Hypothesized Relationship			Control group			Treatment group		
			Path coefficients	p-value	Supported	Path coefficients	p-value	Supported
Exposure to hacking	→	Perceived vulnerability	0.375	0.001	Yes	0.299	0.001	Yes
Perceived vulnerability	→	Perceived threat	0.233	0.001	Yes	0.285	0.001	Yes
Perceived severity	→	Perceived threat	0.514	0.001	Yes	0.546	0.001	Yes
Perceived vulnerability	≠	Intentions to comply	0.000	0.999	Yes	0.040	0.515	Yes
Perceived threat	→	Intentions to comply	0.188	0.007	Yes	0.132	0.038	Yes
Perceived severity	→	Intentions to comply	0.026	0.373	No	-0.051	0.266	No
Perceived password effectiveness	→	Intentions to comply	0.180	0.014	Yes	0.175	0.015	Yes
Password self-efficacy	→	Intentions to comply	0.474	0.001	Yes	0.593	0.001	Yes
Perceived cost	→	Intentions to comply	-0.013	0.420	No	-0.012	0.419	No

6. Discussion

The goal of this study was to investigate how user perceptions about passwords and password security threats influence compliance with guidelines. The study also examined if these perceptions can be altered using fear appeals to improve compliance.

The proposed model has been shown to be an acceptable model for explaining user compliance with password guidelines. The study shows that *perceived threat*, *perceived password effectiveness* and *password self-efficacy* all influence *intentions to comply* with password guidelines. In addition, the study has shown that providing password information and training results in improved *intentions to comply* with password guidelines, confirming the value of fear appeals.

6.1. Effect of password security information

The results of this study suggest that the provision of information and training about password security improves *intentions to comply* with password guidelines, and the proposed model has partially explained the mechanism by which *fear appeals* can elicit change in these perceptions and behavioral intentions. These findings are consistent with studies by Johnston et al. [17], Jenkins and Durcikova [40] and Vance et al. [11], and suggest that threat appraisal and coping appraisal can be manipulated to improve compliance with password guidelines. However, in this study, the training session did not influence *perceived cost.* This finding is somewhat surprising. However, as the background statistics for this study show, many participants already used a 7 to 10 character password and changed passwords voluntarily. This suggests that the scenarios used in the measurement items for *perceived cost* may not have been an issue for the participants and therefore the training did not impact on *perceived cost.*

6.2. Effects of threat appraisal factors

In this study, *perceived severity* had no direct effect on *intentions to comply* with password guidelines. This is contrary to findings from other studies including IS security studies such as Woon et al. [16] who found that perceived severity had an influence on wireless security behavior and Lee et al. [21] who found that the more a user believed a malware attack would cause harm, the more likely they were to install anti-spyware software. Interestingly, the results in this study are consistent with research on password policy compliance [18] where no clear link between *perceived severity* and user's intentions to apply online password protection was found.

As proposed in this study, the results confirm that *exposure to hacking* is linked to *perceived vulnerability,* suggesting that the degree to which a user believes that they are likely to experience password related threats is determined by whether or not they or someone they know personally has been exposed to hacking. However, and as hypothesized in this study, *perceived vulnerability* did not directly influence participants' *intentions to comply* with password guidelines. This lack of support for a direct relationship between *perceived vulnerability* and compliance with password guidelines is consistent with several other IS security studies [e.g. 16, 18, 20, 21]. Interestingly, these studies have examined different areas of security compliance and used different populations, yet found no significant relationship between *perceived vulnerability* and *intentions to comply* with security measures. It appears likely that *perceived vulnerability* has only an indirect affect on intentions to comply as proposed by Liang et al. [19].

Perceived threat was found to have a significant effect on users' *intentions to comply* with password guidelines. Users who are concerned about password threats such as hacking are more likely to comply with password guidelines. This result is consistent with the study of Zhang et al. [18], which not only found perceived threat to be positively correlated with users intentions to apply online password protection but also, found that *perceived threat* is a better predictor of intentions to apply security measures than *perceived severity* or *perceived vulnerability*.

Consistent with previous IS security research [e.g. 19, 26], *perceived threat* is directly influenced by *perceived vulnerability* to threats and *perceived severity* of threats, this indicates that users exhibit more concern for password related threats when *perceived severity* of threat is high. Also, the more they feel vulnerable to password threats the more likely they are to show concern for password threats.

6.3. Effects of coping appraisal factors

In this study, only one threat appraisal factor *perceived threat*, was found to have a direct impact on *intentions to comply* with password guidelines. In comparison, two coping appraisal factors, *perceived password effectiveness* and *password self-efficacy,* had a positive influence. Consistent with other studies [e.g. 18, 31] this finding confirms the claim that coping appraisals are better predictors of compliance with recommended security measures.

Perceived password effectiveness had a significant influence on *intentions to comply* with password guidelines. Users comply with password guidelines with greater consistency when they believe that password guidelines will protect their online account from being hacked. This is consistent with Zhang et al. [18] who found that perceptions about effectiveness of password guidelines had a positive effect on behavioral intentions.

Password self-efficacy had a strong influence on *intentions to comply* with password guidelines. This suggests that the more confident users are in their ability to create strong passwords the more likely they are to comply with password guidelines. Of the factors considered in this study, *password self-efficacy* was the strongest predictor of compliance with password guidelines. This corroborates findings such as those of Milne et al. [31] who in their meta-analytic review of PMT studies found that of all PMT constructs, self-efficacy had the most significant impact on intention.

No relationship was found between *perceived cost* and *intentions to comply* with password guidelines. This finding is unexpected as studies have shown that users are less likely to comply if they perceive security measures as an inconvenience [20, 21], or if they find passwords difficult to remember when password guidelines are followed [18]. However, as discussed earlier, participants indicated that they had relatively good levels of compliance with common password recommendations suggesting that *perceived cost* may not be a major issue for the participants in this study.

7. Implication for practice and research

This study sought to examine ways to improve compliance with password guidelines and found that compliance with password guidelines can be improved using password security training programs that highlight the severity and likelihood of being exposed to password related threats and effectiveness of recommended password guidelines. In particular, this study shows the importance of including training on how to create strong passwords.

7.1 Implications for practice

This study found that increasing users' level of concern for password related threats (*perceived threat*) had a significant impact on their intentions to comply with password guidelines. Based on these findings, training sessions that make users aware of the likelihood of being hacked if weak passwords are used, and the possible consequences if a hacking incident is successful, should significantly increase their levels of concern for password related threats, and their awareness of the impact of non-compliance.

The findings also suggest that the degree to which users trust that following recommended password guidelines will effectively prevent hacking has a significant impact on their intentions to comply. Training sessions should therefore include information that help users understand how each recommended password guideline, such as including upper and lower case letters or avoiding dictionary words, can prevent incidents such as hacking. At the very least, password related training should include how to create strong passwords that are also easy to remember. As *password self-efficacy* had the most impact on intentions to comply in this study, improving *password self-efficacy* should be a training priority.

This study has shown that effective training does not need to be long and tedious; the improvements achieved were accomplished using a 10 minute online training session covering vulnerability to password threats, severity of password threats, effectiveness of recommended password guidelines and how to create strong-easy-to-remember passwords. With the exception of the password creating session (which

included an interactive practice session), static training materials were used in this study. As Vance et al. [11] have shown, adding interactivity results in significantly higher password strength compared to static training materials, therefore adding interactivity should lead to further potential improvements.

7.2 Implications for research

No relationship between *perceived vulnerability* and behavioral intentions was found in this study, adding to the mixed results observed in previous studies [e.g. 16, 18, 20, 21]. Weinstein [41] suggested that one of the possible reasons for a non-significant relationship is that participants may not be aware of the threats they are asked to indicate their perceived vulnerability to. Yet, *perceived vulnerability* did not influence behavioral intentions for the participants in the treatment group who were made aware of password threats through the password security information, therefore this issue requires further research.

This study did, however, advance understanding of one major aspect of *perceived vulnerability*, by clarifying the role of *exposure to hacking*, which was shown to influence *perceived vulnerability*. The relationship between *exposure to hacking* and *perceived vulnerability* should therefore be investigated further to help understand the link between *perceived vulnerability* and behavioral intentions. In future studies it might be possible to compare participants who have been impacted severely by hacking with participants who have not been impacted by hacking.

8. References

[1] Stewart, J.M., Tittel, E., and Chapple, M., Cissp: Certified Information Systems Security Professional Study Guide Sybex, San Francisco, CA 2008.

[2] Tsai, C.S., Lee, C.C., and Hwang, M.S., "Password Authentication Schemes: Current Status and Key Issues", International Journal of Network Security 2006, 3(2), pp. 101-115.

[3] Yan, J., Blackwell, A., Anderson, R., and Grant, A., "Password Memorability and Security: Empirical Results", IEEE Security & Privacy 2004, 2(5), pp. 25-31.

[4] Inglesant, P.G., and Sasse, M.A., "The True Cost of Unusable Password Policies: Password Use in the Wild", Proceedings of the 28th International Conference on Human Factors in Computing Systems, 2010 pp. 383-392.

[5] Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., and Bauer, L., "How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation", Proceedings of the 21st USENIX Conference on Security Symposium, 2012

[6] Florêncio, D., and Herley, C., "A Large-Scale Study of Web Password Habits", Proceedings of the 16th International Conference on World Wide Web, Banff, Alberta, Canada, 2007 pp. 657 - 666.

[7] Calin, B., "Statistics from 10,000 Leaked Hotmail Passwords", Retrieved 7 May 2013 from the World Wide Web, 2009.

[8] Coursey, D., "25 "Worst Passwords" of 2011 Revealed", Retrieved May 2013 from the World Wide Web, 2011.

[9] Deloitte, "P@$$1234: The End of Strong Password-Only Security ", Deloitte 2013

[10] Florêncio, D., and Herley, C., "Where Do Security Policies Come From?", Symposium on Usable Privacy and Security (SOUPS), Microsoft in Redmond, WA, 2010 pp. 83-93.

[11] Vance, A., David, E., Kirk, O., and Detmar, S., "Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment", 2013 46th Hawaii International Conference on System Sciences (HICSS), Hawaii, 2013 pp. 2988-2997.

[12] Bonneau, J., and Preibusch, S., "The Password Thicket: Technical and Market Failures in Human Authentication on the Web", Proceedings of the Ninth Workshop on the Economics of Information Security, Harvard University, USA, 2010

[13] Keith, M., Shao, B., and Steinbart, P., "A Behavioral Analysis of Passphrase Design and Effectiveness", Journal of the Association for Information Systems 2009, 10(2), pp. 63-89.

[14] Miller, G., "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information", Psychological Review 1956, 63(2), pp. 81-97.

[15] Zviran, M., and Haga, W., "Password Security: An Empirical Study", Journal of Management Information Systems 1999, 15(4), pp. 161 - 185.

[16] Woon, I., Tan, G., and Low, R., "A Protection Motivation Theory Approach to Home Wireless Security", Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, 2005 pp. 367-380.

[17] Johnston, A., and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study", MIS Quarterly 2010, 34(3), pp. 549-566.

[18] Zhang, L., and McDowell, W., "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords", Journal of Internet Commerce 2009, 8(3), pp. 180-197.

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

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

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

[22] Workman, M., Bommer, W.H., and Straub, D., "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test", Computers in Human Behavior 2008, 24(6), pp. 2799-2816.

[23] Adams, A., Sasse, M., and Lunt, P., "Making Passwords Secure and Usable", People and Computers 1997, pp. 1-20.

[24] Maddux, J., and Rogers, R., "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change", Journal of Experimental Social Psychology 1983, 19(5), pp. 469-479.

[25] Rogers, R., "A Protection Motivation Theory of Fear Appeals and Attitude Change", Journal of Psychology 1975, 91(1), pp. 93-114.

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

[27] Siponen, M., Pahnila, S., and Mahmood, M.A., "Compliance with Information Security Policies: An Empirical Investigation", Computer 2010, 43(2), pp. 64-71.

[28] Skogan, W., and Maxfield, M., Coping with Crime: Individual and Neighborhood Reactions Sage Publications, Beverly Hills, CA 1981.

[29] Boss, S.: 'Control, Perceived Risk and Information Security Precautions: External and Internal Motivations for Security Behavior'. PhD Thesis, University of Pittsburgh, 2007.

[30] Creese, S., Hodges, D., Jamison-Powell, S., and Whitty, M. (2013). Relationships between Password Choices, Perceptions of Risk and Security Expertise *Human Aspects of Information Security, Privacy, and Trust* (pp. 80-89): Springer.

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

[32] Rippetoe, P., and Rogers, R., "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat", Journal of Personality and Social Psychology 1987, 52(3), pp. 596-604.

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

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

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

[36] Scarfone, K., and Souppaya, M. (2009). Guide to Enterprise Password Management (Draft) *Recommendations of the National Institute of Standards and Technology (Nist)*. Gaithersburg, MD: NIST Special Publication 800-118.

[37] McDowell, M., Rafail, J., and Hernan, S., "Choosing and Protecting Passwords", Retrieved October 2010 from the World Wide Web, 2009.

[38] Hair, J., Black, W., Babin, B., Anderson, R., and Tatham, R., Multivariate Data Analysis Prentice Hall, Upper Saddle River, NJ 2010.

[39] Byrne, B.M., "Testing for Multigroup Equivalence of a Measuring Instrument: A Walk through the Process", Psicothema 2008, 20(4), pp. 872-882.

[40] Jenkins, J.L., Durcikova, A., and Burns, M.B., "Forget the Fluff: Examining How Media Richness Influences the Impact of Information Security Training on Secure Behavior", System Science (HICSS), 2012 45th Hawaii International Conference on, 2012 pp. 3288-3296.

[41] Weinstein, N., "Perceived Probability, Perceived Severity, and Health-Protective Behavior", Health Psychology 2000, 19(1), pp. 65-74.