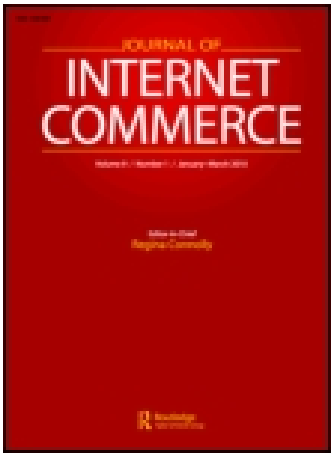

Journal of Internet Commerce
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/wico20

Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords

Lixuan Zhang [a] & William C. McDowell [b]

[a] Hull College of Business , Augusta State University , Augusta, Georgia, USA

[b] Department of Management, College of Business , East Carolina University , Greenville, North Carolina, USA

Published online: 19 Dec 2009.

To cite this article: Lixuan Zhang & William C. McDowell (2009) Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords, Journal of Internet Commerce, 8:3-4, 180-197, DOI: 10.1080/15332860903467508

To link to this article: http://dx.doi.org/10.1080/15332860903467508

Journal of Internet Commerce, 8:180–197, 2009

ISSN: 1533-2861 print/1553-287X online
DOI: 10.1080/15332860903467508

Routledge
Taylor & Francis Group

Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords

LIXUAN ZHANG
Hull College of Business, Augusta State University, Augusta, Georgia, USA

WILLIAM C. McDOWELL
Department of Management, College of Business, East Carolina University, Greenville, North Carolina, USA

By using the protection motivation theory, this article tests a model of password protection intentions for online users. Hypotheses are proposed concerning the intention to engage in good password practices. Data were collected from 182 college students of 3 universities in the southern United States. The results suggest that fear, response cost, and response efficacy are significantly related to online password protection intentions. However, perceived severity and vulnerability are not significant predictors. The study suggests that reducing cognitive costs for passwords is imperative.

KEYWORDS password protection, privacy, protection motivation theory, security

INTRODUCTION

The growth of e-commerce has increased the quantity of passwords each online user must acquire and use. Passwords are one of the most common mechanisms that users employ to protect their online privacy and security and are used for a variety of accounts. A large-scale study of Web passwords involving half a million users shows that each user has about 25 accounts that require passwords, and a user, on average, types 8 passwords per day (Florêncio and Herley 2007). By authenticating a person's identity, passwords serve as the first line of defense against malicious hackers. Passwords are employed to protect users' online information, including financial information and any personal identifiable information. Passwords, however, are very

Address correspondence to Dr. Lixuan Zhang, Hull College of Business, Augusta State University, Augusta, GA 30904, USA. E-mail: gzhang@aug.edu

vulnerable to hackers' attacks and are regarded as one of the most likely human error risk factors to impact information systems (Carstens, McCauley-Bell, and DeMara 2004). For example, in a study examining the vulnerability of online passwords, researchers found that more than half of the passwords on an e-commerce Web site were crackable in less than four hours and almost a third of these passwords were crackable in less than one minute (Cazier and Medlin 2006).

Given the popular usage of passwords as well as their vulnerability, companies and Web site vendors often offer user guidance on strong password creation. For example, many large companies offer tips for creating a secure password. Google provides a password strength meter, which assesses passwords as weak, fair, good, or strong, based on criteria such as password length and character composition. Weak passwords (such as the word "password") are forbidden to be used. Similarly, Microsoft allows a system administrator to set a stringent password policy enforcing password aging, minimum length, or a mix of letters, numbers, and symbols. However, a recent study found that the enforced password composition rules may not necessarily discourage users from using meaningful information, such as names or birthdates, in their passwords (Campell, Kleeman, and Ma 2007).

Why users are careless in their password choices and are reluctant to use strong passwords is a question that remains to be answered. Previous research has examined users' password management strategies (Gaw and Felten 2006), users' behavior associated with password security (Bryant and Campbell 2006), and the core characteristics of user-generated passwords (Zviran and Haga 1999). Although these studies provide rich insights on users' password behaviors, most of them are descriptive studies that lack sound theoretical background. By using the protection motivation theory (PMT), this article intends to investigate the protection motivations of online users associated with their password behavior.

The rest of this article is organized as follows. The study presents related literature about password usage followed by a description of the PMT. Following the review of the relevant literature, hypotheses about the protection motivation for using passwords are formulated. Data are then analyzed, and results are discussed. Finally, theoretical implications of this research are presented along with implications for practice.

LITERATURE REVIEW

Passwords are widely used as a method of authentication. Compared to their alternatives, including hardware authentication and biometric identifications, passwords are simpler to use and involve less financial cost. Online users, however, often regard password usage as a nuisance rather than as protection (Adams and Sasse 1999). Passwords are often considered as an overhead

cost for online users, since using passwords does not enhance productivity (Weirich and Sass 2001). Therefore, online users often choose weak passwords. The following section presents previous research regarding users' password practices. Specifically, password length, password composition, the information contained in the passwords, frequency of password updates, and password reuse are discussed.

Password Length

Passwords should have a minimum of six characters. Longer passwords are generally stronger passwords. In 1999, a study examined 997 computer users and found that 47 percent of the respondents did not have a password with a minimum of six characters (Zviran and Hag 1999). Since this eye-opening study, more recent studies have shown considerable improvement in the password length of computer users. A study examining the passwords of an e-commerce Web site found that the mean length of a password was 7.4 characters (Cazier and Medlin 2006). Another study indicated that 82 percent of 884 undergraduate students have passwords with 6 characters or more for their university Web mail accounts (Bryant and Campbell 2006).

Password Composition

Good passwords should mix letters, numbers, and special characters because such passwords are very difficult to crack. Despite the security that such passwords offer, users still prefer alphabetic characters for their passwords. Past research revealed that more than 80 percent of respondents used alphabetic characters for their passwords, while only .7 percent used all numeric, alphabetic, and alphanumeric characters as a basis for their passwords (Zviran and Haga 1999). A study in 2006 still yielded a disappointing finding: 58.3 percent of the respondents had only alphabetic characters; about a third had letters and numbers, and fewer than 2 percent had special characters (Cazier and Medlin 2006).

Information Contained in Password

Personal and meaningful information, such as names of family members or birthdates, are contained in the majority of users' passwords. Since most passwords are generated on the spot, online users often choose familiar terms (Andrews 2002). A study conducted in Britain revealed that people choose personal terms as their passwords such as spouse's name, children's names, birth date, or phone numbers. One-third of respondents used names of athletes, singers, movie stars, or fictional characters, whereas only 10 percent picked passwords with a random string of letters, numbers, and symbols (Andrews). In another study, 75.5 percent of respondents use personal information as part of their passwords (Tamil et al. 2007).

Frequency of Password Update and Password Reuse

Another problem with passwords is that after users choose their passwords, they rarely change them. An early study found that 79.6 percent of the users never changed their passwords, and less than 5.5 percent of them changed their passwords more often than once a year (Zviran and Haga 1999). In one study among people who changed their passwords, 44 percent changed them less than once a year (Bryant and Campbell 2006). Users often reuse their passwords in multiple accounts. Reusing a password is similar to revealing a password, which makes all accounts with the same passwords vulnerable (Ives, Walsh, and Schneider 2004). If users reuse a password across many accounts, a hacker can access many accounts if the password is cracked. Although users had more accounts over time, they did not have more unique passwords (Gaw and Felten 2006). The Florêncio and Herley study (2007) showed that an average user has 6.5 passwords, each of which is shared across 3.9 different sites.

Overall, users tend to use short passwords, passwords composed of only letters, and passwords with personal and meaningful information. In addition, they tend not to update their passwords, and they reuse the same passwords across multiple accounts. The fact that users have poor password practices may be due to humans' cognitive limitations. According to Miller (1956), there is a severe limitation to the amount of information that humans are able to process and remember for a short term. The short-term capacity is around 7 ± 2 items. To remember a long sequence of items, these items must be divided into chunks such as familiar words or meaningful combinations. Due to the cognitive limitations, users are often less than optimal decision-makers when it comes to reasoning about risk (West 2008). In the case of password choices, users tend to favor quick decisions based on heuristics to conserve cognitive efforts. To adopt strong password practices, users have to be strongly motivated. In the following section, we will examine the factors that may motivate users to engage in good password practices in the lens of the PMT.

THEORETICAL MODEL AND HYPOTHESIS DEVELOPMENT

The PMT was proposed to explain how people cope with potential threats (Rogers 1975). The theory has been widely used to explain and predict a variety of protective behaviors, especially health-related behaviors. Based on the expectancy-value theory, the PMT provides a detailed account of the social cognitive process underlying protective behaviors. The theory consists of two processes: the threat-appraisal process and the coping-appraisal process. The threat-appraisal process evaluates the maladaptive behavior and consists of three factors: perceived severity, perceived vulnerability, and fear arousal. The coping-appraisal process evaluates a person's

ability to cope with the threat. Factors in the coping-appraisal process are response cost, self-efficacy, and response efficacy. In this study, self-efficacy was not investigated, since using strong passwords and updating passwords does not require much technical skill.

The outcome of these processes is a decision to initiate, continue, or discontinue a specific behavior. Therefore, measures of behavioral intention are the typical dependent variable in the PMT. Two meta-analyses of the PMT show that it has been useful in predicting health-related intentions (Floyd, Prentice-Dunn, and Rogers 2000; Milne, Sheeran, and Orbell 2000). This study examines how the PMT variables will affect intentions of implementing strong password practices. Figure 1 depicts the theoretical model of the study.

Perceived Severity

Perceived severity assesses how severe a person believes a threat will be to his or her life. The more seriously a person perceives the negative consequence, the more he or she will adopt recommended actions. Computer users develop a perception of threat after assessing problems in their computing environment. If they do not perceive a threat as severe, then no protection motivation would be aroused, and there would be no change

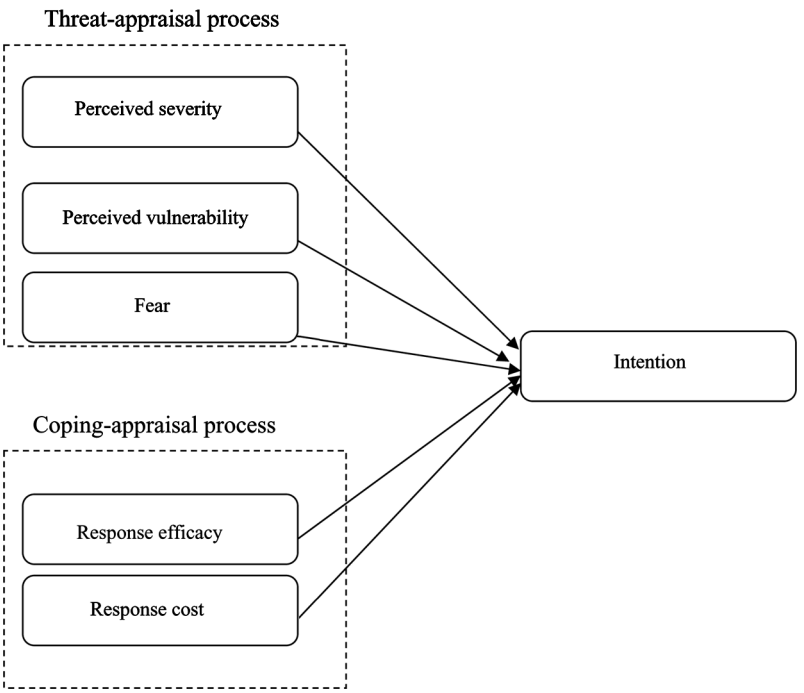

FIGURE 1 Theoretical model.

in behavioral intention. Using the PMT, researchers show that perceived severity is significantly related to protective behaviors such as enabling security measures of a home wireless network (Woon, Tan, and Low 2005) or installing anti-malware software (Lee and Larsen 2009).

On the Internet, passwords provide protection to company intranet accounts, bank accounts, social networking accounts, e-mails, and many others. The breach of passwords can lead to personal data exposure. The content of e-mails, personal journals, photos, and documents can be exposed to a hacker or the public. The exposure of accounting data can even lead to financial losses or identity theft. If the password of a company network was stolen, it could lose its sensitive and confidential data. Thus, it is hypothesized that if a person perceives a higher degree of severity from password breaches, he or she will be more motivated to protect online passwords.

H1: Perceived severity is positively related to the intention of implementing online password protection.

Perceived Vulnerability

Perceived vulnerability concerns the susceptibility a person has to a threat. Passwords can be compromised in many ways. First, hackers can employ a variety of techniques to attack users' passwords. For example, hackers can use a dictionary-based attack, a technique of using a program to guess passwords by searching possible combinations including common words, slang, and popular phrases. Since computer users tend to choose poor passwords, dictionary-based attacks are very efficient (Campbell et al. 2007). Passwords can also be guessed after learning an individual's personal information such as a birthday, spouse or partner's name, or pet's name.

People tend to believe that they are less vulnerable to risks than others. For example, most people believe that they are better than the average driver and that they will live longer than average life expectancy (Slovic, Fischhoff, and Lichtenstein 1986). Therefore, it is not surprising to find that people perceive themselves at less risk of computer vulnerability than others. Users believe that only people with important information or people who have annoyed the attackers should be concerned with any computer risks (Weirich and Sasse 2001). It is expected, however, that those individuals who do have a high degree of perceived vulnerability will be more concerned with password protection. Thus, it is hypothesized that people who perceive themselves as vulnerable to password breaches will be more motivated to protect their passwords.

H2: Perceived vulnerability is positively related to the intention of implementing online password protection.

Fear Arousal

Fear arousal refers to the extent of fear that is triggered by the threat. Fear is an emotional response to threats that can cause a change in attitude or behavioral intention (LaTour and Rotfeld 1997). While perceived severity and vulnerability are cognition focused, fear is emotion focused. Fear arousal will increase the relevance of the threat-relevant message, producing behavioral changes consistently and reliably. Early studies suggested a curvilinear relationship between fear arousal and persuasion, where a moderate level of fear arousal leads to maximum persuasion (Janis 1967, McGuire 1969). However, most studies found a positive linear relationship between fear and compliance with the recommended action (Sutton, 1982; Milne et al. 2000).

It is assumed that fear increases the intention to use safe password practices. If online users are very nervous about the prospect of having passwords guessed or cracked by others, they may be more likely to spend more effort in safeguarding and updating their passwords. Thus, it is hypothesized that those who do have a higher level of fear arousal will be more interested in their password protection.

H3: Fear arousal is positively related to the intention of implementing online password protection.

Response Cost

Response cost, a factor in the coping-appraisal process, measures the perceived costs (e.g., time, money, effort) that a person has to pay in taking the protective behavior. Consequently, response cost decreases the probability of selecting the recommended action. In information security, researchers find that the hindrance of implementing security practices is negatively related to people's attitudes toward security policy (Herath and Rao 2009).

In this study, response cost refers to the time and effort spent in creating strong passwords and updating them. Most people have gone through the frustration of forgetting passwords and trying to retrieve them. Creating strong passwords and updating them regularly adds an additional layer of inconvenience. In addition, a wide variety of online accounts makes the response cost higher. This is the reason why people reuse their passwords for multiple accounts—to minimize the cognitive cost of using the strong passwords. Thus, it is hypothesized that higher perceived response cost is negatively associated with password protection intention.

H4: Response cost is negatively related to the intention of implementing online password protection.

Response Efficacy

Response efficacy is another factor comprising the cope-appraisal process. Response efficacy evaluates how effective the recommended coping response is in reducing the threat. In order to implement protective behavior, individuals should be confident that the protective behavior is effective in protecting them against the threat. In a study related to the use of anti-spyware tools, Gurung, Luo, and Liao (2009) found that response efficacy is positively related to protection behavior.

A study investigating the cracking time of passwords showed that the majority of passwords that were cracked in less than a minute were all alphabetical characters only. All passwords with special characters took at least an hour to crack (Cazier and Medlin, 2006). This shows that strong passwords can better protect online accounts. In addition to using strong passwords, regular password updates also help to protect online accounts from malicious hackers. People will be more involved in online password protection behavior if they are certain that the extra effort they invest in making password secure are worthwhile.

H5: Response efficacy is positively related to the intention of implementing online password protection.

METHODOLOGY

The research model was tested with data obtained using an online survey instrument. To ensure the content validity of the survey, three researchers evaluated the survey instrument. All items were borrowed or adapted from existing scales. The three items measuring perceived severity were adapted from Plotnikoff and Higginbotham (2002). Respondents were asked to rate the level of severity for three scenarios of password breach. Items measuring perceived vulnerability were adapted from Pechmann and colleagues (2003), and items measuring fear were adapted from Milne, Orbell, and Sheeran (2002). The three items measuring response cost were adapted from Woon and colleagues (2005). Respondents were asked to rate their perceived costs in using strong passwords, updating passwords frequently, and using unique passwords for each online account. Items measuring response efficacy were adapted from Maddux and Rogers (1998). Respondents were asked to rate their perceived benefit in implementing strong password practices. Items used to measure the independent variables are listed in the appendix. All items were measured on a 5-point Likert-type scale. The dependent variable "Intention" was measured by three items: "I will update my passwords frequently," "I will use strong passwords," and "I will use unique passwords for different online accounts."

Data were gathered using an online survey from 182 students in three universities from the southern United States. The majority of the students are undergraduate students majoring in business. The student sample was deemed appropriate, since the study focuses on online password use, and students are among the most active Web users. Researchers tend to use student samples for theory testing (e.g., Lopes and Galletta 2006; Wang and Wallendorf 2006), which fits the purpose of this study. In addition, as indicated in the previous study, the decision-making processes of students are consistent with that of other populations (Zhang, Prybutok, and Koh 2006). Of the students, 86 are male, and 97 are female. On average, they have about 10.58 years of Internet experience. Regarding the number of passwords they use online, 43 of them have 0–5 online passwords, 86 of them have 6–10 passwords, 38 of them have 10–15 passwords, and 15 have more than 16 passwords.

At the beginning of the survey, the following definition of a strong password, adapted from guidelines from Microsoft for strong passwords, was provided to the respondents:

> *A password is strong if (1) it is at least seven characters long; (2) it contains characters from letters, numerals, and symbols; (3) it is significantly different from prior passwords; (4) it does not contain your name or user name; (5) it is not a common word or name; and (6) it has at least one symbol character in the second through sixth positions.*

Principle component analysis using a Varimax rotation was used to assess the dimensionality of the items measuring the independent variables. Principle component analysis is appropriate when the primary concern is to predict the minimum number of factors needed to account for the maximum portion of variance in the original data (Hair et al. 1998). The Varimax rotation procedure aids in the analysis by rotating the factors so that the factors tend to load higher on a smaller number of variables, allowing for easier interpretation of the resulting factors (Kaiser 1960). The criteria of an eigenvalue of at least one was used to assess the number of factors to extract, and the dimensionality of each of the factors extracted was assessed by examining factor loadings (Hair et al.). Items with a factor loading of greater than .5 on the factor with which they are hypothesized to load were considered adequate indicators of the factors (Hair et al.). Items that had factor loadings of .3 or greater with another factor were considered to have cross-loaded, and thus were not unique indicators of a given factor. As shown in Table 1, items are loaded on their respective factors. In the latter case, the item was dropped as the measure was not considered to be unidimensional. For this set of data, the factor analysis yielded five distinct factors based on the "eigenvalue ≥ 1.0" criteria. The total variance explained by the model is 74.16 percent.

The second aspect of construct validity assessed is the reliability of the measures. One of the most commonly used indicators of reliability is internal

TABLE 1 Factor Analysis

	Severity	Fear	Response efficacy	Vulnerability	Response cost
Severity3	**0.952**	0.129	0.032	0.082	−0.005
Severity1	**0.943**	0.182	0.043	0.054	−0.046
Severity2	**0.919**	0.191	0.033	0.092	−0.013
Fear3	0.143	**0.930**	0.094	0.128	0.027
Fear2	0.118	**0.929**	0.063	0.097	0.035
Fear1	0.233	**0.830**	0.121	0.059	0.136
ResponseEfficacy3	−0.018	0.040	**0.912**	0.044	0.001
ResponseEfficacy2	0.019	0.104	**0.887**	0.062	−0.037
ResponseEfficacy1	0.089	0.094	**0.781**	0.001	0.054
Vulnerability3	0.062	0.113	−0.018	**0.816**	0.009
Vulnerability2	0.063	−0.009	0.128	**0.797**	0.063
Vulnerability1	0.065	0.143	−0.010	**0.763**	0.169
ResponseCost2	0.114	−0.045	−0.027	0.037	**0.795**
ResponseCost1	0.046	0.125	0.082	0.219	**0.722**
ResponseCost3	−0.222	0.076	−0.022	−0.004	**0.494**
Cronbach's alpha	0.917	0.838	0.959	0.728	0.701
Variance explained	27.12%	14.88%	13.16%	10.89%	8.12%

consistency, which assesses how consistently individuals respond to items within a scale (Cronbach 1951). Cronbach's alpha is often used to assess the internal consistency of a multi-item measurement scale. Cronbach's alphas for all five factors extracted are above .70, which indicates the measures are internally consistent. Table 1 shows the factor analysis results along with Cronbach's alpha, factor means, and standard deviations.

RESULTS

Multiple regression analysis was conducted to test the hypotheses. This methodology allows the determination of whether a relationship exists between several independent variables and a dependent variable. The objective of the multiple regression analysis is to use the independent variables to predict the single dependent value. Using a mathematical procedure called least square, the regression line can be estimated when the sum of the squared prediction errors is minimized (Hair et al. 1998).

In this study, intention was used as the dependent variable with the five PMT variables as independent variables. The overall model was significant ($F = 9.06$, $p < 0.001$) with an 18.2 percent adjusted R square. Table 2 shows the results of the regression. Among the five variables, fear, response cost, and response efficacy are significantly related to intention. Therefore, H3, H4, and H5 are supported. Perceived severity and vulnerability are not significant predictors. Hypotheses H1 and H2 are rejected. Table 2 depicts the regression results.

TABLE 2 Regression Results (Dependent Variable: Intention)

Variables	Standardized beta	*t*-value	*p*-value
Severity	.03	0.41	.68
Vulnerability	.085	1.227	.22
Fear	.276	3.735	.000
Response cost	−.145	−2.042	.043
Response efficacy	.294	4.306	.000

DISCUSSION

Using the PMT, this study investigates the factors affecting online users' password protection intentions. Overall, the results indicate that factors in the coping-appraisal process are more important than factors in the threat-appraisal process in predicting the intention of implementing a strong password practice. Among the threat components of the PMT, this data suggests that perceived severity is not related to password protection intentions. Online users who perceive a severe consequence of password breaches do not necessarily intend to take more effort to protect their passwords.

Evidence for the effects of severity on intentions in previous PMT research has been inconsistent. For example, although researchers have shown significant effects of perceived severity on intention and behavior (Workman, Bommer, and Straub 2008; Gurung et al. 2009; Woon et al. 2005; Herath and Rao 2009), there is also evidence that shows that the severity is not significantly related to intention (Wurtele and Maddux 1987; Beck and Lund 1981). A meta-analytic review of the PMT finds the weakest association between severity and intention among all PMT variables (Milne et al. 2000).

Perceived vulnerability is also not associated with password protection intention. According to the PMT, the higher probability a user perceives a threat to be, the more likely he or she will intend to undertake the necessary measures. For example, perceived vulnerability is an important predictor of the intention to adopt virus protection measures (Lee, Larose, and Rifon 2008). However, other research also showed a non-significant relationship between perceived vulnerability and behavior intention (Murgraff, White, and Phillips 1999; Herath and Rao 2009; Woon et al. 2005).

Other researchers also found that the threat-appraisal factors of the PMT are less significantly related to behavioral intentions than coping-appraisal variables (Plotnikoff and Higginbotham 2002). One possible explanation is that the threat may not generate enough motivation for people to comply with the recommended action. In this study, the subjects had very low levels of perceived severity and vulnerability of password breaches. Since there was no immediate visible threat, they were not motivated to spend efforts on

protective behaviors. However, this does not mean that the threat components are not important in the adoption of preventive behaviors. Individuals may not reduce any threat if they do not feel the threat is severe and that they are vulnerable to the threat.

The one threat-appraisal factor that is positively related to password protection intentions is fear. This is consistent with previous research (Tanner, Hunt, and Eppright 1991; Plotnikoff and Higginbotham, 2002). Previous research on information technology security using the PMT model have ignored the role of fear (e.g., Workman et al. 2008; Woon et al. 2005; Herath and Rao 2009; Lee and Larsen 2009). It is found in this study that fear is the most important threat-appraisal variable. When computer users are scared of the consequences of password breaches, they will take measures to reduce the fear. Compared to perceived severity and vulnerability (which are cognition focused), fear, as an emotional response, is a more effective weapon. Information systems researchers have examined how fear influences the persuasiveness of IT security communication (Xu, Rosson, and Carroll 2007). Getting computer users emotionally nervous about their information security is helpful in motivating them to comply with security policy, which includes using strong passwords and updating them frequently.

This study finds that response cost has a significant negative relationship with protection intention. Consistent with previous research, response cost is also negatively related to attitude of security policy (Herath and Rao 2009), adoption of anti-malware software (Lee and Larsen 2009), and implementation of security measures (Workman et al. 2008). When users perceive inconvenience and have to pay a price of time and effort, they are usually reluctant to adopt the recommended action. In this study, the response cost is measured by the difficulty of remembering passwords, which is the major weakness of passwords as confirmed by numerous studies. It is found that response cost serves as a major deterrent of the motivation to protect passwords. In the modern business climate, computer users have many accounts that need passwords; however, users can only be expected to use four or five passwords effectively (Adams and Sasse 1999). Therefore, users will inevitably have a huge mental burden if they practice using strong passwords.

Similar to previous research (Gurung et al. 2009; Herath and Rao 2009), response efficacy was found to have a positive statistically significant relationship with password protection intentions. Online users hold different views about the effectiveness of available security measures. When they perceive the security measures are adequate, they would be more likely to adopt them. The subjects who believe that the measures taken to develop protecting passwords are effective are more motivated to implement them. If users believe that their online accounts are vulnerable no matter what passwords they use, they will be less motivated to invest effort and time to practice using strong passwords.

LIMITATIONS

There are several limitations of the study. First, the study examines the online password in general but does not distinguish between high-value and low-value Web sites. While response cost and response efficacy may be similar among different Web sites, perceived security, perceived vulnerability, and fear may be different. An online user may choose a strong password for an online banking site but may not be that cautious in choosing a password for a social chat site. Therefore, researchers should investigate online users' password choices among different Web sites. Second, our sample consists of a convenience sample of undergraduate business students and may pose a problem of external validity. The students may not have a strong incentive to use strong passwords because they do not have a great deal of financial assets or sensitive information to protect. Future studies using working professionals, especially professionals working in financial industries, may yield different results. However, previous research does indicate that students and non-students had similar risk attitudes toward Internet shopping (Su 2003).

THEORETICAL AND PRACTICAL IMPLICATIONS

This study makes several theoretical and practical contributions. While some literature has addressed users' password behaviors, this article provides a sound theoretical model to examine the behavioral intentions of strong password usage. The security level of the password mechanism largely depends on users' willingness to make efforts to behave in accordance with strong password policies. However, they have to be persuaded to do so. The PMT posits that people engage in two processes when considering protective behavior: the threat-appraisal process and the coping-appraisal process. After online users evaluate the seriousness of the threat as well as consider the costs and value of coping strategies, they will make a rational choice to either adopt the protective behavior or not. In our case, the coping-appraisal process plays a major role in online users' intentions of implementing good password practices.

The study also presents interesting results for security professionals. One of the most significant variables that deter users from adopting a good password practice is response cost, in this study, the difficulty of remembering passwords. Since passwords mostly serve as a mechanism to help users access main tasks, passwords add to users' cognitive load. Therefore, passwords are usually chosen on the spot, and familiar passwords, short passwords, and old passwords are often chosen primarily for the ease of later retrieval. Many researchers have proposed new password mechanisms to help reduce the response costs and improve the quality of passwords. Yan

and coworkers (2004) recommended the use of mnemonic phrases, where the first letters of each word in a phrase are used as a password. Carstens, Malone, and Bell (2006) suggested using passwords consisting of meaningful chunks to improve password recall. Another type of password, the graphical password, is gaining popularity due to people's superior memory for pictures over texts (Dhamija and Perrig 2000). Online users need to be educated and instructed to use new mechanisms for their passwords.

Users should be educated about the benefits of good password practices. Only when they are well aware of the security benefits offered by strong passwords are they willing to invest time and effort to make their passwords stronger. Therefore, on the Web page, when users are asked to choose passwords, a comparison on the crack time between weak and strong passwords could be offered so that users are more likely to put more thought in their password choices.

This article also suggests that fear appeal should be emphasized in the communication message to motivate strong password usage. The stronger the fear appeal, the greater the intention to adopt good password practices. For example, the message could elaborate on the negative consequences of failure to follow good password practices. Vivid information, such as stories and pictures, could be used so the contents of the message can be emotionally close to the audience.

In conclusion, this article has empirically examined various factors to motivate users to protect vital and important information through the use of passwords. Fear, response cost, and response efficacy are important predictors of intentions to use good passwords. When choosing passwords, the gain of safety is hard to quantify, while the cost of selecting strong passwords is real and immediate. That is why users often discount long-term risks and losses. To solve the problem, security professionals should take measures to reduce the response cost and increase the response efficacy of using strong passwords. Communication messages with fear-arousing stimuli could be designed to persuade users to better protect themselves by implementing a good password practice.

REFERENCES

Adams, A., and M. S. Sasse. 1999. Users are not the enemy. *Communications of the ACM* 42 (12): 41–46.

Andrews, L. W. 2002. Passwords reveal your personality. *Psychology Today*. http://www.psychologytoday.com/articles/pto-20020101-000006.html (accessed February 17, 2009).

Beck, K. H., and A. K. Lund. 1981. The effects of health threat seriousness and personal efficacy upon intentions and behavior. *Journal of Applied Social Psychology* 11:401–415.

Bryant, K., and J. Campbell. 2006. User behaviors associated with password security and management. *Australian Journal of Information Systems* 14 (1): 81–100.

Campbell, J., D. Kleeman, and W. Ma. 2007. The good and not so good of enforcing password composition rules. *Information Systems Security* 16 (1): 2–8.

Carstens, D. S., L. Malone, and P. Bell. 2006. Applying chunking theory in organizational human factors password guidelines. *Journal of Information, Information Technology, and Organization* 1:97–114.

Carstens, D. S., R. P. McCauley-Bell, and R. F. DeMara. 2004. Evaluation of the human impact of password authentication practices on information security. *Information Science Journal* 7:67–85.

Cazier, J. A., and B. D. Medlin. 2006. Password security: An empirical investigation into e-commerce passwords and their crack times. *Information Systems Security* 15 (6): 45–55.

Cronbach, L. J. 1951. Coefficient alpha and the internal structure of tests. *Psychometrika* 16:297–334.

Dhamija, R., and A. Perrig. 2000. Déjà vu: A user study using images for authentication. *Proceedings of 9th USENIX Security Symposium*, August 14–17, 45–58. Denver, CO.

Florêncio, D., and C. Herley. 2007. A large-scale study of web password habits. *Proceedings of WWW 2007*, May 8–12, Banff, Alberta, Canada.

Floyd, D. L., S. Prentice-Dunn, and R. W. Rogers. 2000. A meta analysis of research on protection motivation theory. *Journal of Applied Social Psychology* 30: 407–429.

Gaw, S., and E. W. Felten. 2006. Password management strategies for online accounts. *Proceedings of the Second Symposium on Usable Privacy and Security*, July 12–14, 44–55. Pittsburgh, PA.

Gurung, A., X. Luo, and Q. Liao. 2009. Consumer motivation in taking action against spyware: An empirical investigation. *Information Management and Computer Security* 17 (3): 276–289.

Hair, J. F., R. L. Anderson, R. Tatham, and W. Black. 1998. *Multivariate data analysis.* 5th ed. New York: Prentice Hall.

Herath, T., and H. R. Rao. 2009. Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems* 18:106–125.

Ives, B., K. R. Walsh, and H. Schneider. 2004. The domino effect of password reuse. *Communications of the ACM* 47 (4): 75–78.

Janis, I. L. 1967. Effects of fear arousal on attitude change: Recent development in theory and experimental research. In *Advances in experimental social psychology* (Vol. 3), ed. L. Berkowitz, 166–224. San Diego, CA: Academic Press.

Kaiser, H. F. 1960. The application of electronic computers to factor analysis. *Education and Psychological Measurement* 20:141–151.

LaTour, M. S., and H. J. Rotfeld. 1997. There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself. *Journal of Advertising* 26:45–59.

Lee, D., R. Larose, and N. Rifon. 2008. Keeping our network safe: A model of online protection behavior. *Behavior and Information Technology* 27:445–454.

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

Lopes, A. B., and D. F. Galletta. 2006. Consumer perceptions and willingness to pay for intrinsically motivated online content. *Journal of Management Information Systems* 23 (2): 203–231.

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

McGuire, W. J. 1969. The nature of attitudes and attitude change. In *Handbook of social psychology,* Vol. 3, 2nd ed., eds. G. Lindzey, and E. Aronson, 136–314. Reading, MA: Addison-Wesley.

Miller, G. A. 1956. The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review* 63:81–97.

Milne, S., S. Orbell, and P. Sheeran. 2002. Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology* 7:163–184.

Milne, S., P. Sheeran, and S. Orbell. 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.

Murgraff, V., D. White, and K. Phillips. 1999. An application of protection motivation theory to riskier single-occasion drinking. *Psychology and Health* 14:339–350.

Pechmann, C., C. Zhao, M. E. Goldberg, and E. T. Reibling. 2003. What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message theme. *Journal of Marketing* 67:1–18.

Plotnikoff, R. C., and N. Higginbotham. 2002. Protection motivation theory and exercise behavior change for the prevention of coronary heart disease in a high-risk, Australian representative community sample of adults. *Psychology, Health and Medicine* 7 (1): 87–98.

Rogers, R. W. 1975. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology* 91:277–287.

Slovic, P., B. Fischhoff, and S. Lichtenstein. 1986. Facts versus fears: Understanding perceived risks. In *Judgment under uncertainty: Heuristics and biases*, eds. D. Kahneman, P. Slovic, and A. Tversky, 463–489. New York: Cambridge University Press.

Su, B. 2003. Risk behavior of Internet shopping: comparison of college students' versus non-student adults. *Proceedings of the 5th International Conference on Electronic Commerce*, September 30–October 3, 181–185, Pittsburgh, PA.

Sutton, S. R. 1982. Fear-arousing communications: a critical examination of theory and research. In *Social psychology and behavioral medicine*, ed. J. R. Eiser, 303–337. London: Wiley.

Tamil, E. M., A. H. Othman, S. A. Z. Abidin, M. Y. I. Idris, and O. Zakaria. 2007. Password practices: A study on attitude towards password usage among undergraduate students in Klang Valley, Malaysia. *Journal of the Advancement of Science and Arts* 3:37–42.

Tanner, J. F., J. B. Hunt, and D. R. Eppright. 1991. The protection motivation model: A normative model of fear appeals. *Journal of Marketing* 55:36–45.

Wang, J., and M. Wallendorf. 2006. Materialism, status signaling and product satisfaction. *Journal of the Academy of Marketing Science* 34 (4): 494–506.

Weirich, D., and M. A. Sasse. 2001. Pretty good persuasion: A first step towards effective password security in the real world. *Proceedings of the 2001 Workshop on New Security Paradigms*, Cloudscrofl, NM, September 10–13.

West, R. 2008. The psychology of security. *Communications of the ACM* 51 (4): 34–41.

Woon, I. M. Y., G. W. Tan, and R. T. Low. 2005. A protection motivation theory approach to home wireless security. *Proceedings of the 26th International Conference on Information Systems*, Las Vegas, NV, December 11–14, 367–380.

Workman, M., W. H. Bommer, and D. Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior* 24:2799–2816.

Wurtele, S. K., and J. E. Maddux. 1987. Relative contributions of protection motivation theory components in predicting exercise intentions and behavior. *Health Psychology* 6:453–466.

Xu, H., M. B. Rosson, and J. M. Carroll. 2007. "Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View," Workshop on *Usable IT Security Management, Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh, PA.

Yan, J., A. Blackwell, R. Anderson, and A. Grant. 2004. Password memorability and security: Empirical results. *IEEE Security and Privacy*, 2:25–31.

Zhang, X., V. R. Prybutok, and C. E. Koh. 2006. The role of impulsiveness in a TAM-based online purchasing behavior model. *Information Resource Management Journal* 19 (2): 54–68.

Zviran, M., and W. J. Haga. 1999. Passwords security: An empirical study. *Journal of Management Information Systems* 15 (4): 161–185.

APPENDIX Constructs Operationalization

Constructs	Items	Source
Perceived severity	How severe do you think the consequence will be if . . . 1. someone guessed your passwords? 2. someone cracked your passwords? 3. someone obtained your passwords? (ranging from "not severe at all" to "very severe")	Adapted from Plotnikoff and Higginbotham (2002)
Perceived vulnerability	What are your chances of . . . 1. someone guessing your passwords? 2. someone cracking your passwords? 3. someone obtaining your passwords? (ranging from "Very Unlikely" to "Very Likely")	Adapted from Pechmann et al. (2003)
Fear	1. The thought of having someone guess my passwords makes me nervous. 2. The thought of having someone crack my passwords makes me nervous. 3. The thought of having someone obtain my passwords makes me nervous. (ranging from "Strongly Disagree" to "Strongly Agree")	Adapted from Milne et al. (2002)
Response cost	1. If I use strong passwords, they will be difficult for me to remember. 2. If I update my passwords often, they will be difficult for me to remember. 3. If I use unique password on each account, they will be difficult for me to remember. (ranging from "Strongly Disagree" to "Strongly Agree")	Adapted from Woon et al. (2005)
Response efficacy	I can protect my online accounts better . . . 1. if I use strong passwords, 2. if I update my passwords often, 3. if I use unique passwords for each online accounts. (ranging from "Strongly Disagree" to "Strongly Agree")	Adapted from Maddux and Rogers (1983)