INDIVIDUAL DIFFERENCES ON INTENTIONS TO USE STRONG PASSWORDS

Lixuan Zhang, Hull College of Business, gzhang@aug.edu
William C. McDowell, East Carolina University, mcdowellw@ecu.edu
Todd Schultz, Hull College of Business, tschultz@aug.edu

ABSTRACT

This paper examines the influence of individual differences among internet users regarding intentions to use strong passwords. Several hypotheses are developed and applied to address this question based upon data collected from 182 participants (college students from three universities in the southern United States). Gender, consideration of future consequences, and number of internet passwords are established as statistically significant indicators of password protection intentions.

Keywords: Password protection, computer efficacy, end user security, gender differences

INTRODUCTION

The growth of e-commerce, social networking, and online resources has increased the quantity of passwords each online user must acquire and use (for this paper our use of online focuses on internet users on the web). Despite research into alternative approaches, login ID and password combinations are the most common mechanisms employed to control access to online data and provide security 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 eight 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 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 ecommerce website could be compromised in less than 4 hours and almost a third of these passwords would last less than one minute (Gazier and Medlin, 2006).

Given the popular usage of passwords as well as their vulnerability, companies and website 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).

People differ in the weight they attach to the importance of passwords. Some people manage their passwords diligently by using strong passwords and updating them frequently. Others consider it as a nuisance and an overhead cost since it does not enhance any productivity. For example, a study in 2006 found that 58.3% of the respondents had only alphabetic characters; about a third had letters and numbers and fewer than 2% had special characters (Gazier and Medlin, 2006). Personal and meaningful information, such as names of family members or birthdates, are often contained in users' passwords A study conducted in Britain found that one third of respondents used names of athletes, singers, movie stars or fictional characters whereas only ten percent picked passwords with a random string of letters, numbers and symbols (Andrews, 2002). Another problem with passwords is that after users choose their passwords, they rarely change them. Researchers found that 79.6% of the users never changed their passwords and less than 5.5% of them changed their passwords more often than once a year (Zviran and Haga, 1999).

Recent years have witnessed the use of personality traits in the IS studies (McElroy, Hendrick, Townsend and DeMarie, 2007; Nov and Ye, 2009). However, few studies have examined the effect of personality trait in online security behavior. This study assumes that there are stable individual differences in intrinsic motivation to engage in strong passwords usage. The purpose of the study is to test if some individuals are more prone to use strong passwords than others. Previous research has examined users' password management strategies (Gaw and Felten, 2006), users' behavior associated with password security (Bryant and Campbell, 2006) the core characteristics of user-generated passwords (Zviran and Haga, 1999) and users' motivation to use strong passwords (Zhang and McDowell, 2009). Although these studies provide rich insights on users' password

behaviors, few of them examine the individual differences in the use of passwords.

Even with enforced password guidelines and password change schedules, developing an understanding of users' intentions to support the security system can aid in the security system itself. The old wag about 'What's in the middle of security' being U R (you are) is too true; the system is only as good as the willingness of the participants. Further, rigidly enforced security guidelines may deter otherwise will customers and participants. Web developers must balance the need for security with demands at least reasonably aligned with what users will tolerate.

In this study, we examine two individual factors affecting password intent: consideration of future consequences and gender. In addition, another factor: number of online passwords is also investigated. The rest of this paper is organized as follows. The study presents related literature about these three factors followed by hypotheses. Data are analyzed, and results are discussed. Finally, theoretical implications of this research are presented along with future research direction.

LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

Consideration of Future Consequences

One personality trait that may relate to self protective behavior is consideration of future consequences (CFC). The construct for CFC is proposed by Strathman et al (Strathman, Gleicher, Boninger and Edwards, 1994). It measures the extent to which individuals consider the potential future outcomes of their current behavior and the extent to which they are affected by these outcomes. Individuals who are low on CFC focus more on immediate needs and concerns and act accordingly, while individuals high on CC focus more on future consequence of their actions and these consequences to guide their actions.

There is ample evidence that CFC influences people's behavior and attitude. Individuals high in CFC were less in favor of offshore oil driving due to their greater interest in environment. When the benefits were framed in the future and the disadvantages were framed in the present, high CFC individuals were more in favor of oil drilling. Conversely, individuals low in CFC were more in favor of oil drilling when the benefits were framed as immediate and disadvantages were framed as distant (Strathman et al., 1994). The researchers also demonstrated that CFC is significantly related to health concerns, cigarette use and environmentalism behavior (ibid.).

Similar results have been found in health-related area. For example, CFC is found to be important in the processing health communication about sunscreen use, cancer screening and Type 2 diabetes screening (Orbell and Kyriakaki, 2008; Orbell, Perugini and Rakow, 2004; Orbell and Hagger, 2006). High-CFC Individuals weigh long-term outcomes more heavily and are more persuaded when positive outcomes of protective health behaviors were presented in the future and negative outcomes were presented in the present. In contrast, low-CFC individuals were more persuaded when positive outcomes were outlined as immediate and negative outcomes as distant (Orbell and Kyriakaki, 2008; Orbell, Perugini and Rakow, 2004; Orbell and Hagger, 2006). In other research areas, researchers have found that CFC is significantly related to academic achievement and goal attainment among college students (Joireman, 1999), fiscal responsibility (Joireman, Sprott and Spangenberg, 2005) and impulsive sensation seeking (Joireman, Anderson and Strathman, 2003).

CFC plays a natural role in individuals' protective behavior on the Internet. Behaviors performed to protect personal information on the Internet typically incur immediate costs but distant and uncertain benefits. In the context of passwords, immediate costs occur. Individuals have to spend time and efforts in going through the inconvenience of choosing a strong password to use and remembering it. When they have multiple online accounts with multiple passwords, it would be more difficult for them to come up with a new password than just reuse old ones. In the meantime, the benefits of using strong passwords are in such a distant future and individuals low in CFC may not take future consequence into account. Therefore, we propose:

H1: Individuals high in CFC will have stronger intention of implementing online password protection.

Gender

Another individual difference that may play a role self-protective behavior on the Internet is gender. Compared with males, females are portrayed as more cautious and less aggressive. In particular, females have a lower preference for risk than males (Hudgens and Fatkin, 1985; Johnson and Powell, 1994). Some argue that gender difference in risk taking vary with contexts so gender differences should not be interpreted as a general traits (Beomiley and Curley, 1992), however, females are found to have significantly lower preference for risk irrespective of contextual factors (Power and Ansic, 1997). A meta-analysis on gender differences in risk taking (Bynes, Miller and Schafer, 1999) clearly support the idea that males are more likely to take risks than females. However, certain situational factors (intellectual risk

taking and physical skills) yield larger gender difference than others (e.g. smoking).

There is also considerable gender difference on the behaviors on Internet. Earlier studies show that females were less interested in the Internet than males. They spend less time online and are less likely to purchase online than males (Bartel-Sheehan, 1999). One possible reason is that females are more concerned with the risks of buying online. Even after controlling for the Internet usage, females still perceive higher risks than males in an online environment. They tend to perceive greater severity in credit card misuse, fraudulent sites and loss of privacy. They perceived a significantly likelihood of negative outcomes in credit card misuse, fraudulent sides and shipping problems (Gabardine and Strahilevitz, 2004). However, studies also find that they are less likely to adopt protective behaviors to protect their privacy online (Bartel-Sheehan, 1999).

Powell and Ansic (1997) linked the difference to motivational theory. Females have a greater desire for security so they have a lower risk preference. They tend to focus on actions that avoid the negative consequences to gain security. The natural assumption is that females would be more cautious in using their passwords to protect their online security. Therefore, we propose:

H2: Females will have stronger intention of implementing online password protection than males.

Number of Online Passwords

With the popularity of the Internet, online users have more and more passwords for different accounts. They may have passwords for bank accounts, multiple credit cards accounts, social networking sites and various email accounts. The more online passwords the users have, the more effort they may need to spend to manage the passwords.

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 seven plus or minus two 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. In the case of password choices, users tend to favor quick decisions based on heuristics to conserve cognitive efforts. Therefore, when it comes to passwords for multiple accounts, the users are more likely to reuse previous passwords or make a slight modification on previous passwords. Therefore we hypothesize:

H3: The number of online passwords is negatively related to the intention of implementing online password protection.

METHODOLOGY

The hypotheses were tested with data obtained using an online survey instrument. The items measuring CFC was borrowed from (Strathman et al., 1994). The instrument has been used widely and has been demonstrated to have adequate validity and reliability. Gender was coded as 0 and 1 where 0=Males and 1=Females. Number of online passwords is measured by using a categorized item where 1= 0-5 online passwords, 2 = 6-10 online passwords, 3 = 11-15 online passwords, 4 = 16-20 passwords and 5 = more than 20 passwords. 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 the 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 et al. 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 online 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, 7 have 16- 20 passwords and 8 have more than 20 passwords. One respondent did not report the number of online passwords being used.

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) is significantly different from prior passwords; 4) does not contain your name or user name; 5) not a common word or name; 6) have at least one symbol character in the second through sixth positions."

RESULTS

Multiple regression analysis was an effective tool for predicting the single dependent value. With gender established as an indicator variable, a straightforward application of least squares was appropriate (e.g., see Hair, et al., 1998).

In this study, intention was used as the dependent variable with the gender, CFC and the number of online passwords as independent variables. Although the overall model was significant ($F= 4.59$ and $p <0.01$) the 5.6% adjusted R square indicates that much of the variation in intention is due to factors outside this particular model. Within the model

- H1 is supported. Individuals high in CFC are more likely to use strong passwords.
- H2 is supported. Women are more likely to use strong passwords than men.
- H3 is also supported. The number of online passwords is negatively related to the intention of implementing online password protection.

Table 1 depicts the regression results.

Dependent variable: Intention			
Variables	**Std Beta**	**t-value**	**p-value**
CFC	0.156	2.136	0.034
Gender	0.153	2.113	0.036
#online passwords	-0.164	-2.245	0.026

Table 1: Regression Results

DISCUSSION AND CONCLUSION

The study examines three factors affecting online users' password protection intentions. The results indicate that CFC, gender and number of online passwords are all significantly related to use of strong passwords. CFC is studied widely in health psychology and our finding indicates that CFC is a direct antecedent of online users' strong password implementation intention. Many online users are reluctant to protect their security online by using passwords because the benefits are in the future while the costs are immediate and heavy. Understanding the role of CFC can help IT administrators create better messages to persuade the users to adopt strong passwords. When advantages are framed in the future and the disadvantages were framed in the present, high CFC individuals were more in favor of self-protective behaviors (Orbell and Kyriakaki, 2008). Low CFC individuals were more in favor of self-protective behavior when the benefits were framed as immediate and disadvantages were framed as distant. Therefore, IT administrators should take temporal framing into consideration when they design a communication message about IT security policy on password usage.

The study finds that females are more likely to implement online password protection. This is in line with previous research indicating gender difference in risk perception. Females desire for security so they are more concerned about their online privacy and security. In terms of passwords usage, females may perceive more risks about weak passwords and are more likely to implement passwords protection. This suggests that IT administrators may want to focus on the risks of password breaches when targeting female users, as they may be easily disturbed by possible negative outcomes. However, previous research shows that although the females are more concerned with their privacy, they are less likely than to change their behavior on-line. This study only investigates the gender difference in terms of intention of implementing online passwords. Future studies can study the actual password behavior across genders.

Number of online passwords is found to have a negative significantly relationship with password protection intentions. The more online passwords the users have, the less likely the users are willing to implement passwords protection. Unfortunately, as Internet is rooted in each individual's life, users are bound to have more and more passwords to use and remember. New passwords mechanisms need to be implemented to reduce improve the quality of passwords. Yan, Blackwell, Anderson and Grant (2004) recommend 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) suggest using passwords consisting of meaningful chunks to improve password recall. Another type of password, 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.

Understanding the role of individual factors is important in formulating IT security policies. To date, few studies have examined personality traits in users' Internet security behavior. This study examines impacts of CFC and gender and finds them both to be direct antecedents on online passwords implementation intention. Future studies can examine other types of personality factors. For example, unrealistic optimism or regulatory focus may affect people's intention to use strong passwords. The study also finds that number of online passwords being is found to have a negative relationship with online passwords protection. Another direction for future research would be to investigate other factors such as

Internet experience, time spent on the Internet each day or number of unique passwords.

REFERENCES

Andrews, L.W., (2002). "Passwords reveal your personality," Psychology today. Accessed from http://www.psychologytoday.com/articles/pto-20020101-000006.html on Feb 17, 2009.

Bartel-Sheehan, K. (1999). "An investigation of gender differences in on-line privacy, concerns and resultant behaviors," *Journal of Interactive Marketing*, 13, 4, 24-38

Bromiley, P., and Curley, S. (1992). "Individual differences in risk taking," In: Yate, J.F. (ed). *Risk Taking Behaviour, Wiley*, Chichester, UK.

Bryant, K., and Campbell, J. (2006) "User behaviors associated with password security and management," *Australian Journal of Information Systems*, Vol.14, No.1, pp.81-100.

Bynes, J.P., Miller, D.C., and Schafer, W.D. (1999). "Gender differences in risk taking: A meta-analysis," *Psychological Bulletin*, 125,1,367-383

Carstens, D.S., Malone, l., and Bell, P. (2006). "Applying chunking theory in organizational human factors password guidelines," *Journal of Information, Information Technology, and Organization*, Vol.1, pp.97-114.

Campell, J., Kleeman, D., and Ma, W. (2007). "The good and not so good of enforcing password composition rules," *Information Systems Security*, Vol.16, No.1, pp.2-8.

Dhamija, R., and Perrig, A. (2000)."Déjà vu: a user study using images for authentication," in *Proceedings of 9th USENIX Security Symposium*, Denver, Colorado, pp.45-58.

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

Garbarino, E., and Strahilevitz, M. (2004). "Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation," *Journal of Business Research*, 57, 768-775.

Gaw, S., and Felten, E.W. (2006). "Password management strategies for online accounts," Proceedings of the *Second Symposium on Usable Privacy and Security*, Pittsburg, Pennsylvania, pp.44- 55.

Gazier, J.A., and Medlin, B.D. (2006) "Password security: an empirical investigation into E-commerce passwords and their crack times," *Information Systems Security*, Vol.15, No.6, December, pp.45-55.

Hair, J.F., Anderson, R.L., Tatham, R., and Black, W. (1998). *Multivariate Data Analysis*, 5th edition, Prentice Hall. New York.

Hudgens, G., and Fatkins, L. (1985) "Sex differences in risk taking: Repeated sessions on a computer simulated task," Journal of Psychology, 119, 3, 1970-2206.

Johnson, J., and Powell, P. (1994). "Decision making, risk and gender: Are managers different?" *British Journal of Management*, 5, 123-138.

Joireman, J.A. (1999). "Additional evidence for validity of the Consideration of Future Consequence Scale in an academic setting," *Psychological Reports*, 84, 1171-1172.

Joireman, J.A., Anderson, J., and Strathman, A. (2003). "The aggression paradox: understanding the links among aggression, sensation seeking and the consideration of future consequences," *Journal of Personality and Social Psychology*, 84, 1287-1302

Joireman, J.A., Sprott, D.E., and Spangenberg, E.R. (2005). "Fiscal responsibility and the consideration of future consequences," *Personality and Individual differences*, 39, 1159-1168.

Lopes, A. B., and D. F. Galletta. (2006). "Consumer perceptions and willingness to pay for intrinsically motivated online content," *Journal of Management Information Systems*, Vol. 23, No.2, pp.203-31.

McElroy, J.C., Hendrickson, A.R., Townsend, A.M., and DeMarie, S.M.(2007). "Dispositional factors in Internet use: Personality versus cognitive style," *MIS Quarterly*, 31, 809-820.

Nov, O., and Ye, C. (2009). "Resistance to change and the adoption of digital libraries: an integrative model," *Journal of the American Society for Information Science and Technology*, 60,8, 1702-1708.

Orbell, S., and Hagger, M. (2006). "Temporal framing and the decision to take part in Type 2 diabetes screening: Effects of individual differences in consideration of future consequences on persuasion," *Health Psychology*, 25, 537-548.

Orbell, S., and Kyriakaki, M. (2008). "Temporal framing and persuasion to adopt preventive health behavior:

moderating effects of individual differences in consideration of future consequences on sunscreen use," *Health Psychology*, 27, 6, 770-779

Orbell, S., Perugini, M., and Rakow, T. (2004). "Individual differences in sensitivity to health communications: consideration of future consequences," *Health Psychology*, 23, 4, 388-396.

Powell, M., and Ansic, D. (1997). "Gender differences in risk behaviour in financial decision-making: an experimental analysis," *Journal of Economic Psychology*, 13, 605-628

Strathman, A., Gleicher, F., Boninger, D.S., and Edwards, C.S. (1994). "Consideration of future consequences: weighing immediate and distant outcomes of behavior," *Journal of Personality and Social Psychology*, 66 (4), 742-752.

Tanner, J.F., Hunt, J.B. & Eppright, D.R. (1991). "The protection motivation model: a normative model of fear appeals," *Journal of Marketing*, Vol. 55, pp. 36–45.

Wang, J., and M. Wallendorf. (2006). "Materialism, status signaling and product satisfaction." *Journal of the Academy of Marketing Science*, Vol.34, No.4, pp. 494-506.

Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2004). "Password memorability and security: empirical results," *IEEE Security & Privacy*, pp.25-31

Zhang, L., and McDowell, W. (2009). "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords," *Journal of Internet Commerce*, 8, pp.180-187.

Zhang, X., Prybutok, V. R., and Koh, C.E. (2006). "The role of impulsiveness in a TAM-based online purchasing behavior model," *Information Resource Management Journal*, Vol. 19, No.2, pp. 54-68.

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