Individual Differences and Perceived Password Security Management

Lin Kyi
Carleton University

Sonia Chiasson
Carleton University

Elizabeth Stobert
Carleton University

Abstract

Security systems and security education programs cannot be assumed to work equally well for all users, who may have different demographics, security knowledge, and dispositions. In this study, we investigated how perceived password security management (PPSM) is impacted by individual differences such as gender, age, education, security knowledge, and personality. We surveyed 102 participants about their PPSM in relation to their gender, age, security knowledge, and personality traits. We found that PPSM in younger individuals, those with less security knowledge, and those with certain personality traits such as neuroticism may contribute to increased security vulnerability.

1 Introduction

Security failures may not only be due to the user's actions or the poor usability of security systems, but rather due to the assumption that the same security system and education will work equally well for everyone. Every user is different, and their individual differences may influence how they perceive password management tasks. The way the task of password management is perceived can impact security behaviours [16], therefore it is important to identify vulnerable groups to create targeted solutions. We define *perceived password security management (PPSM)* as how users assess their own password management habits, including how much effort they put into the task of managing passwords, and how successful they think they are [24].

Who Are You?! Adventures in Authentication (WAY) 2020.
August 7, 2020, Virtual Conference.

Our study explored whether relationships exist between individual traits and PPSM. Personality traits, specifically the Five Factor Model, have been associated with broader security behaviours, such as workplace security compliance [12, 13], and phishing vulnerability [9]. Demographic traits also have been associated with security behaviours [7], and most of these traits are easily identifiable by the user themselves or by others. However, little work has examined password management practices and their relation to individual differences.

We were interested in how different users perceive their own security management practices and risks to identify vulnerable user groups for further work on targeted security solutions. We identified some relationships between individual traits and security management behaviours, but our results suggest that personality traits may not be a strong indicator of success in password management.

2 Background

The way users perceive the importance of security and their security-related skills can impact their security behaviours. Gratian et al. looked at how individual characteristics correlated to security behaviour intentions [7]. They found that individual differences accounted for between 5% to 23% of security behavioural intention variance in participants [7]. Individuals who are more conscientious, agreeable, and emotionally stable tend to be more risk-averse, compliant with security policies, and take security more seriously [12]. In contrast, users who are more open and extroverted were observed to be less compliant with security policies, and took more security-related risks if they had benefits [12].

Security systems are often built for average users. Unfortunately, most users are not "average" users, and systems need to consider individual differences to be effective [5]. Egelman and Peer argued that secure decisions are more likely to be made if the security messages and user interfaces are targeted at individual traits, instead of for the average user [5].

One approach to individualizing security is to personalize

security education [3]. The mismatch between current security education and the user's understanding of security can be reduced by adapting security education to the user's needs [3]. This is important, considering that the perceived threat of attacks, perceived effectiveness of passwords, and password self-efficacy impact a user's intent to comply with security guidelines [16].

Users with more confidence in their ability to stay secure have been shown to behave more securely [27]. These individuals are more likely to implement security patches, follow security guidelines, and adopt recommended security applications [27].

Users perceive security risks and actions to address risks differently, and previous research has recommended that targeted methods for improving security perceptions and behaviours be implemented. However, identifying which types of users are more prone to different perceptions of security, and suggesting targeted solutions is lacking. In this study, we build upon previous research by identifying individual traits which can impact perceptions of security management, and suggesting targeted security recommendations.

2.1 The Five Factor Model of Personality

The Five Factor Model (FFM, also called the Big Five Model) is the most prevalent model of personality, and describes five factors which cover most personality traits [15]. The FFM has been proven to be reliable and valid [14], and related to broader security behaviours [12], making it a suitable measure of personality for this study .

The five personality traits identified are:

Openness: High intellect, imaginative, and is open to new experiences.

Conscientiousness: Reliable, organized, and plans out actions.

Extraversion: Sociable, dominating, has a positive affect, and energetic.

Agreeableness: Altruistic, warm, kind, and nurturing.

Neuroticism: Negative affect, prone to quick mood changes, and less emotionally stable [15]. The opposite of Neuroticism is known as "Emotional Stability."

3 Study

We surveyed participants on their self-reported perceived password security management, and compared these results to their demographics (age, gender, and security knowledge) and FFM scores to see how individual differences impact PPSM.

There were three main parts to our survey:

1. **Demographics:** This section included questions about age, gender identity, and self-reported computer security knowledge.
2. **Perceived Security Management survey:** To measure perceived password security management, we used the *Perceived Security Management* section of Stobert and Biddle's Password Life Cycle survey [23] and adapted it to fit the purpose of this study. This survey used Likert scale questions, where participants rated responses from 1 (Never/Strongly Disagree) to 5 (Always/Strongly Agree).
3. **International Personality Item Pool Sample 50 Item (IPIP-50) survey:** The final section of our survey was a commonly used personality survey which is used to assess participants' Five Factor scores [19]. This survey used Likert scale questions, rating from 1 (Very Inaccurate) to 5 (Very Accurate). Participants' personality traits were scored according to the IPIP-50 guidelines [19]. An individual's FFM scores are assessed by taking a personality survey, and the results are calculated to create a measure of how the user scored in each personality trait.

This study was approved by Carleton University Research Ethics Board. In total, it took participants around 15 minutes to complete the survey. Participants were paid USD $2.00.

3.1 Participants

We recruited 102 participants through Prolific.co. Participants had to be over 18, English-speaking, and have experience using computers. The demographics of Prolific users are not well-studied, but it has been shown to provide more reliable and honest responses compared to MTurk [18].

Most participants claimed to know a bit about computer security. For this study, we looked at the general population and their level of computer security knowledge, not at experts.

We had an almost even split between male (49%) and female (51%) participants. Most participants were young, with 81% being under 40 years old. Participants were from a variety of educational and occupational backgrounds. English was the most commonly spoken mother tongue (66%), followed by Portuguese (8%).

We calculated participants' FFM personality scores. The mean score (out of 50) for Openness was 36.8, Conscientiousness was 33.9, Extroversion was 26.7, Agreeableness was 38.2, and Neuroticism was 30.8. Our participants' FFM scores were similar to previously-observed FFM patterns [6]. There was some collinearity between individual traits and personality scores, such as women being more agreeable ($r_s(100) = 0.212, p = 0.033$), men being more knowledgeable about security ($r_s(100) = -0.209, p = 0.035$), and conscientiousness and openness being correlated ($r_s(100) = 0.327, p = 0.001$). However, this collinearity is normal, and commonly seen in population distributions [12].

Table 1: Summary of Identified Factors

Factor Name	Variance Explained	Number of Items	Loadings
1. Difficulties with password management	21.55%	3	0.69 - 0.85
2. Self-evaluation of password management	10.73%	2	0.76 - 0.77
3. Security attention budgeting	9.75%	3	0.56 - 0.63
4. Perceived need for security	6.19%	1	0.96
5. Evaluation of vulnerability	4.94%	1	0.71

3.2 Analysis

We first ran an exploratory factor analysis (EFA) to identify the different aspects of PPSM. We used a promax rotation and the principal axis factoring method. We only included items with factor loadings above 0.55, as per the recommendation for our sample size [8]. After the factors were identified, we created factor scores for each factor using the regression method.

We ran a Shapiro-Wilk test for normality for the individual traits to assess which correlation method we should use. Since our sample was not normally distributed, we ran a Spearman correlation between the PPSM factor scores and the individual traits of personality, age, gender, and security knowledge. Correlation does not imply causation, but a correlation analysis is helpful for exploring relationships between concepts, and for understanding Likert scale data [17].

4 Results

The exploratory factor analysis identified five factors from our PPSM survey which accounted for 53.16% of variance. Table 1 summarizes the factors.

Factor scores were created from the factors, and a Spearman correlation was used to identify relationships between the five factors within PPSM, and the individual traits of age, gender, security knowledge, and personality. Our analysis was intended to explore the relationship between the PPSM factors and individual traits. The correlations highlighted here are intended to serve as a basis for future *a priori* hypothesis testing [4].

Factor 1 (Difficulties with password management): Those with more self-reported security knowledge were less likely to find password management to be a difficult task ($r_s(100) = -0.375, p < 0.001$), and individuals scoring higher on the Neuroticism trait were more likely to report difficulties with password management ($r_s(100) = 0.217, p = 0.029$).

Factor 2 (Self-evaluation of password management): We found that those with more security knowledge ($r_s(100) = 0.261, p = 0.008$), those who are more conscientious ($r_s(100) = 0.305, p = 0.002$), and those who are more open ($r_s(100) = 0.198, p = 0.049$) were more likely to agree that they are doing a good job with keeping their accounts secure.

Factor 3 (Security attention budgeting): This factor refers to the ability to budget the level of attention given to different accounts based on their importance. Individuals who were more agreeable reported more security attention budgeting ($r_s(100) = 0.278, p = 0.005$), in addition to those who are more open ($r_s(100) = 0.318, p = 0.001$).

Factor 4 (Perceived need for security): Conscientious individuals were more likely to believe there is a greater need for security ($r_s(100) = -0.236, p = 0.017$), whereas those who are more neurotic were less likely to believe security is important ($r_s(100) = 0.207, p = 0.036$).

Factor 5 (Evaluation of vulnerability): Individuals who are younger felt less at-risk for security attacks ($r_s(100) = -0.215, p = 0.030$), which is factor 5 in the model.

We did not find any significant results for gender or extroversion.

5 Discussion

We found significant correlations between individual traits and aspects of self-reported PPSM. Age, self-reported security knowledge, and some personality traits had stronger relationships to perceived security management.

Individuals with more security knowledge were not as burdened by password management, and were more likely to think they were keeping their accounts secure compared to other groups. This fits in with previous research, showing that security experts often display more secure behaviours, and have a better understanding of how to behave securely [10].

We found that gender had no significant relationships with any of the perceived security management factors, contrary to previous research which found that women tend to have less security self-efficacy and show less secure behaviours [2]. We found that men tend to report having higher security knowledge than women, so it could be that security knowledge (or belief in one's security abilities), and not gender, explains these differences in security perceptions between women and men.

We found that younger individuals felt less threatened by security attacks than older individuals. This finding fits with previous literature indicating that younger individuals are more likely to engage in riskier security behaviours [21]. Additionally, older individuals may have more valuable online accounts, such as bank accounts, which may make them feel more threatened by attacks.

Those who are more agreeable and conscientious are more likely to have respect for rules and policies, and therefore more likely to follow them [22]. We found this finding in our results.

However, the results for extroversion, openness, and neuroticism are less clear. Previous research has found that extroverts and open individuals are less likely to perceive security as important [12]. However, our study found that extroversion is not significantly associated with any factors, and the results for openness may indicate they take security seriously, contrary to the previous research. Additionally, previous research found that individuals who are more neurotic are more likely to take security seriously [12], but our study found that neurotic individuals have more trouble with security and did not find security to be important.

A possible explanation for the differences in the results for personality between our study and Johnston et al.'s study is that Johnston et al. grouped the FFM traits into meta-traits, so conscientiousness, agreeableness, and emotional stability became the meta-trait of *stability*, and openness and extroversion became *plasticity*, whereas our study looked at each personality trait individually. Additionally, Johnston et al. studied employees and their security perceptions and behaviours, whereas we looked at the general population.

5.1 Targeted Security Recommendations

Based on our findings, we have created security recommendations based on each identified factor within PPSM.

Factor 1 (Difficulties with password management): Users who struggle with password management, such as those scoring higher on the Neuroticism trait, may benefit from advice on abstract ideas about what makes a good password and how to keep passwords secure [1], rather than focusing on password policies and password characters [26]. User interface elements, such as password meters, can help users who are struggling come up with more secure passwords [25]. Additionally, introducing password managers to those struggling with password management can provide a secure and usable method of keeping passwords secure.

Factor 2 (Self-evaluation of password management): Those who believe they are doing a good job with password management, such as those with more security knowledge, and those who are more conscientious, can still improve their security behaviours by keeping up to date on security recommendations and education.

Factor 3 (Security attention budgeting): Users who struggle with budgeting their attention across accounts should receive more guidance on how to assess the value of various accounts. Many users' mental models of valuable accounts often do not fit with those of security experts, therefore more education on budgeting is important for those who struggle with this [26].

Factor 4 (Perceived need for security) and Factor 5 (Evaluation of risk): For individuals who do not believe they are vulnerable or attacks and/or do not believe security is important, such as younger individuals, and those who are more neurotic, education focusing on understanding threats can be beneficial [11,26]. For instance, understanding the different types of password attacks and the dangers of password reuse may change mental models of security. Security-related fear appeals, such as emphasizing the severity of a threat, or a user's likelihood of vulnerability, have also been shown to be effective in improving security mental models [11].

5.2 The FFM and Security Management

Although we identified a few correlations between individual traits and perceived password management, the pattern of findings in our study was unclear, especially for the personality traits. The FFM is an extensively validated model of personality that is prevalent in the field of personality psychology. These traits have been shown to correlate to security rule breaking and risk aversion [12]. However, our results suggest that there is no strong relationship between the personality traits in the FFM and users' perceived password management.

While personality measurement is well-established, the measurement of perceived security management is less standardized. Although successfully used in a previous study, the life cycle questionnaire [24] may not be effective at assessing perceived security management to a degree of granularity that is needed to distinguish differences based on personality management.

Measuring perceived security management is inherently difficult. Users do not get substantial feedback about the effectiveness of their security behaviours, and may form inaccurate impressions based on coincidence. Additionally, users typically have little expertise in security, and may not understand how their actions do (and do not) affect their security outcomes. Finally, all humans are prone to the *fundamental attribution error* [20], which leads them to self-credit their successes while blaming their failures on outside events. Another possibility is that the lack of differences points to a floor effect - the password management

task is so difficult that all users report difficulties, regardless of personality type.

6 Conclusion

The traditional "one size fits all" approaches to security do not equally benefit everyone, and more attention could be paid on providing targeted help to different groups with different vulnerabilities. We found that individuals with less security knowledge, those who are younger, and/or those who score higher on the Neuroticism trait may be more vulnerable to security failures.

The results of our study suggest that the FFM may not have significant explanatory power for analysing perceived password security management at this time. One possibility is that other individual traits might contribute more, and we suggest that further work is needed to investigate this space and validate the relationships between security and individual traits and the interventions we suggest.

Acknowledgments

The authors acknowledge funding from Natural Sciences and Engineering Research Council of Canada (NSERC) through the Discovery Grant (Chiasson, Stobert) and Canada Research Chair programs (Chiasson).

References

[1] Password Advice - Schneier on security, https://www.schneier.com/blog/archives/2009/08/password_advice.html, 2009.

[2] Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69:437–443, 2017.

[3] Farzaneh Asgharpour, Debin Liu, and L Jean Camp. Mental models of security risks. In *International Conference on Financial Cryptography and Data Security*, pages 367–377. Springer, 2007.

[4] Ralf Bender and Stefan Lange. Multiple test procedures other than bonferroni's deserve wider use. *Bmj*, 318(7183):600, 1999.

[5] Serge Egelman and Eyal Peer. The myth of the average user: Improving privacy and security systems through individualization. In *Proceedings of the 2015 New Security Paradigms Workshop*, pages 16–28, 2015.

[6] Lewis R. Goldberg, Dennis Sweeney, Peter F. Merenda, and John Edward Hughes. Demographic variables and personality: the effects of gender, age, education, and ethnic/racial status on self-descriptions of personality attributes. *Personality and Individual Differences*, 24(3):393–403, March 1998.

[7] Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther. Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73:345–358, 2018.

[8] Joseph F Hair, William C Black, Barry J Babin, Rolph E Anderson, Ronald L Tatham, et al. *Multivariate Data Analysis*, volume 5. Prentice Hall Upper Saddle River, NJ, 1998.

[9] Tzipora Halevi, James Lewis, and Nasir Memon. A pilot study of cyber security and privacy related behavior and personality traits. pages 737–744, May 2013.

[10] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, 2015.

[11] Allen C. Johnston and Merrill Warkentin. Fear appeals and information security behaviors: An empirical study. *MIS Q.*, 34(3):549–566, September 2010.

[12] Allen C Johnston, Merrill Warkentin, Maranda McBride, and Lemuria Carter. Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, 25(3):231–251, May 2016. Publisher: Taylor & Francis.

[13] Maranda McBride, Lemuria Carter, and Merrill Warkentin. Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions*, 5(1):1, 2012.

[14] Robert R McCrae and Paul T Costa. Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology*, 52(1):81, 1987.

[15] Robert R McCrae and Oliver P John. An introduction to the five-factor model and its applications. *Journal of Personality*, 60(2):175–215, 1992.

[16] Florence Mwagwabi, Tanya McGill, and Michael Dixon. Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In *2014 47th Hawaii International Conference on System Sciences*, pages 3188–3197, January 2014.

[17] Geoff Norman. Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education*, 15(5):625–632, 2010.

[18] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70:153–163, 2017.

[19] International Personality Item Pool Sample 50-Item Questionnaire. https://ipip.ori.org/, Accessed Feb. 2020.

[20] Lee Ross. The intuitive psychologist and his shortcomings: Distortions in the attribution process. In *Advances in experimental social psychology*, volume 10, pages 173–220. Elsevier, 1977.

[21] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference*, pages 373–382, 2010.

[22] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, 2015.

[23] Elizabeth Stobert and Robert Biddle. The password life cycle: User behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 243–255, 2014.

[24] Elizabeth Stobert and Robert Biddle. The password life cycle. *ACM Transactions on Privacy and Security (TOPS)*, 21(3):13, 2018.

[25] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, et al. How does your password measure up? The effect of strength meters on password creation. In *21st USENIX Security Symposium*, pages 65–80, 2012.

[26] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "I added'!'at the end to make it secure": Observing password creation in the lab. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 123–140, 2015.

[27] Lixuan Zhang and William C McDowell. Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3-4):180–197, 2009.

Appendix A: Survey Questions

Demographics

1. My gender is:
   (a) Male
   (b) Female
   (c) Other
2. My age is:
   (a) Under 20
   (b) 21 - 30
   (c) 31 - 40
   (d) 41 - 50
   (e) 51 - 60
   (f) 60+
3. What is your mother tongue/first language?
4. What is your highest level of completed education?
   (a) High school
   (b) Trade school or apprenticeship
   (c) Community College
   (d) Undergraduate degree
   (e) Graduate or Professional degree
5. (If Q4 c, d, or e are answered, this questions is shown) What is/was your field of study?
6. What is your occupation?
7. How knowledgeable are you about computers?
   (a) Not at all
   (b) Somewhat
   (c) Very knowledgeable
8. How knowledgeable are you about computer security?
   (a) Not at all
   (b) Somewhat
   (c) Very knowledgeable

Perceived Password Security

On a scale from 1 to 5, where 1 is never and 5 is always, please rate your agreement with the following statements:

1. I think that I am doing a good job protecting my accounts.
2. I am aware that I could do more do protect my accounts.
3. I am doing my best to protect my accounts.
4. I do not have time to pay attention to security.
5. I do not feel that my accounts are likely to be attacked.
6. I do not know whom to trust for security advice.
7. I do not know where to look for help with passwords and security.
8. I have a standard person that I ask for help with computer security problems.
9. Keeping track of my passwords is difficult.
10. I give some accounts more "security attention" than others.
11. It is hard to decide where to focus my "security attention".
12. My "security attention" is limited.
13. Some accounts deserve more "security attention" than others.

Five Factor Personality Survey

We used the *International Personality Item Pool Sample 50-Item survey (IPIP-50)*, which can be found at https://ipip.ori.org/new_ipip-50-item-scale.htm.