Individual Differences and Perceived Password Security Management

Lin Kyi, Sonia Chiasson, & Elizabeth Stobert

Carleton University
Ottawa, Canada

WAY Workshop 2020

Introduction

- How password management is perceived can impact security behaviours
- **Perceived Password Security Management (PPSM):** how users assess their own password management habits
- Do relationships exist between users' individual traits and PPSM?
- We identified some relationships between individual traits and PPSM

Background

- Personalizing Security:
  - Reduce mismatch between security education and user understanding by adapting education to user’s needs [1]
  - Users with more confidence in security abilities often behave more securely [2]

- Individual Differences:
  - Account for 5-23% of security behavioural intention variance [3]
  - Some personality traits make people more/less compliant and risk averse [4]

Five Factor Model (FFM)

- FFM is the most broadly-used model of personality
  - Related to broader security behaviours [2]
- 5 personality factors:

Openness	High intellect, imaginative, open to new experiences
Conscientiousness	Reliable, organized, plans out their actions
Extraversion	Sociable, dominating, energetic, has a positive affect
Agreeableness	Altruistic, warm, kind, nurturing
Neuroticism (the opposite is “Emotional Stability”)	Negative affect, prone to quick mood changes, less emotionally stable

Methodology

- We surveyed users on self-reported *perceived password security management,* and compared these results to their *individual traits*
    - Individual traits: *age, gender, security knowledge, FFM personality scores*

- 3-part survey:
    - **Demographics:** self-reported age, gender identity, self-reported computer security knowledge
    - **Perceived Security Management:** adapted from Stobert and Biddle's Password Life Cycle survey [5]
    - **International Personality Item Pool Sample 50 Item (IPIP-50) survey**: commonly-used personality survey used to assess FFM scores

Participants

- *N* = 102
- *Age:* 81% under 40 years old
- *Gender:* 49% male, 51% female
- *Security knowledge:* most claimed to know a bit about security

- Personality mean scores (out of 50):
  - *Openness:* 36.8
  - *Conscientiousness:* 33.9
  - *Extroversion:* 26.7
  - *Agreeableness:* 38.2
  - *Neuroticism:* 30.8

- Collinearity between certain FFM traits and demographics is normal [2]

Analysis and Results:
Exploratory Factor Analysis

- EFA conducted to identify which aspects of PPSM are related to each other

F1: **Difficulties with password management**	3 items	21.55% variance
F2: **Self-evaluation of password management**	2 items	10.73%
F3: **Security attention budgeting**	3 items	9.75%
F4: **Perceived need for security**	1 item	6.19%
F5: **Evaluation of vulnerability**	1 item	4.94%

Analysis and Results: Spearman Correlation (1/2)

- Correlated factors to individual traits (personality, age, gender, security knowledge)

- F1: **Difficulties with password management**
    - More self-reported security knowledge felt password management was less difficult (*rs*(100) = -0.375, *p* < 0.001)
    - Those who are more Neurotic felt password management was more difficult (*rs*(100) = 0.217, *p* = 0.029)

- F2: **Self-evaluation of password management**
    - More self-reported security knowledge (*rs*(100) = 0.261, *p* = 0.008), more Conscientious (*rs*(100) = 0.305, *p* = 0.002), and more Open (*rs*(100) = 0.198, *p* = 0.049) more likely to agree they are doing a good job keeping accounts secure

Analysis and Results: Spearman Correlation (2/2)

- F3: **Security attention budgeting**
  - Agreeable (*rs*(100) = 0.278, *p* = 0.005), and Open (*rs*(100) = 0.318, *p* = 0.001) individuals claim to budget their security attention more often
- F4: **Perceived need for security**
  - Conscientious individuals were more likely to believe there is a greater need for security (*rs*(100) = -0.236, *p* = 0.017)
  - Neurotic individuals were less likely to believe security is needed (*rs*(100) = 0.207, *p* = 0.030)
- F5: **Evaluation of vulnerability**
  - Younger individuals felt less at-risk for security attacks (*rs*(100) = -0.215, *p* = 0.030)
- No significant findings for gender and extraversion

Results Summary

- Age, self-reported security knowledge, and some personality traits had stronger relationships to PPSM
  - **Security knowledge:** felt less burdened by password management, believed they were keeping accounts more secure
  - **Younger** individuals felt less threatened by attacks
  - **Agreeable** and **conscientious** individuals are more likely to follow and respect security rules
  - **Extraversion, openness,** and **neuroticism** findings are less clear

Targeted Security Recommendations

- Advice on abstract ideas about good password management
  - Factor 1: Difficulties with password management

- Keep up to date with security recommendations
  - Factor 2: Self-evaluation of password management

- Guidance on how to assess the value of their accounts
  - Factor 3: Security attention budgeting

- Education focusing on understanding security threats
- Fear appeals to improve mental models and behaviours
  - Factor 4: Perceived Need for Security
  - Factor 5: Evaluation of vulnerability

Discussion

- Relationships between PPSM and individual traits were less clear than expected

- Password Life Cycle questionnaire less-validated than FFM
    - Measuring password management perceptions is difficult

- Security may produce a floor effect
    - Password management is difficult for almost everyone

Conclusion

- We identified relationships for age, some personality traits, and security knowledge in relation to PPSM
- Personality traits may not be a reliable indicator of success in password management
- Future work might look at password behaviours instead of perceptions
- This is a work in progress - let us know if you have suggestions!

References

1. 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.
2. 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.
3. 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.
4. 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.
5. Elizabeth Stobert and Robert Biddle. The password life cycle. *ACM Transactions on Privacy and Security (TOPS)*, 21(3):13, 2018.

Thanks for listening!

Questions?

Feel free to contact me at
Lin.Kyi@carleton.ca