Selected Papers of Internet Research 15:
The 15th Annual Meeting of the
Association of Internet Researchers
Daegu, Korea, 22-24 October 2014

DOES PERSONALITY AND SECURITY EXPERTISE PREDICT PASSWORD STRENGTH?

James Dodson
University of Leicester

Duncan Hodges
University of Oxford

Monica Witte
University of Leicester

Sadie Creese
University of Oxford

Despite alternative authentication methods, passwords remain the most common method of restricting access to online information and services[1]. It is important to develop ‘strong’ passwords (i.e., passwords that are difficult to guess) in order to prevent hackers from accessing important personal information (e.g., bank account details). Despite a wealth of public advice available on protecting online data, many individuals still choose weak passwords or engage in risky password practices such as sharing their passwords with others[2-6]. This is, in part, because choosing memorable, long and strong passwords is difficult and unintuitive for humans[7].

Researchers have found that individuals are generally aware of what constitutes a secure password and what good password management entails[8-9]. Nonetheless, it has been found that individuals tend to trade off their security concerns and strong password management with convenient, memorable and ultimately less secure passwords[1,10-12].

Given that public campaigns have not helped to change online security behaviour to an acceptable level and increasingly the public are needing to protect online content (as commercial, financial and government services continue to move online), more research is urgently needed to help gain some understanding as to why some individuals continue to make bad decisions regarding password choice. This study sought to add to the literature on the types of people who make poor password choices. If we can identify who is more likely to make these decisions then we might be better able to

Suggested Citation (APA): Dodson, J., Hodges, D., Witte, M., & Creese, S., (2014, October 22-24). *Does personality and security expertise predict password strength.* Paper presented at Internet Research 15: The 15th Annual Meeting of the Association of Internet Researchers. Daegu, Korea: AoIR. Retrieved from http://spir.aoir.org.

create appropriate campaigns to alter poor online security behaviour as well as target campaigns to the most appropriate people.

This study aimed to examine whether some types of people are more likely to create 'strong' passwords. In particular, we were interested in personality characteristics and security expertise. Personality characteristics included: impulsivity, locus of control and self-monitoring. We hypothesised the following:

H1: Security experts will be more likely to create secure passwords compared to non-experts.

H2: Individuals who score low on impulsivity are more likely to create secure passwords.

H3: Individuals who score high on self-monitoring are more likely to create secure passwords.

H4: Individuals who score high on internal locus of control are more likely to create secure passwords.

The study first gained ethical approval from the college's ethics committee. In order to test our hypotheses we devised an online questionnaire. Participants were unaware that we were interested in password choice and instead were told that the study aimed to learn about their Internet usage, cyber security knowledge and personalities. In order to access the study, participants were asked to "create a password for the sole use of this study". For ethical purposes, participants were asked to create a password that they had not used elsewhere.

Password strength was assessed by two of the most common password attacks that the public face: dictionary and keyspace attacks[13]. The metric calculated how many of these lists the participant's password appeared. If a participant's password appeared on those lists at all, then their password is considered extremely weak and vulnerable to a brute force dictionary attack. Comparatively, the keyspace metric indicated the cost of cracking a password using a rainbow table in what is commonly known as a Time-Memory Trade Off attack[14]. A larger keyspace will take longer to crack using a rainbow table whereas a smaller keyspace will take less time to crack. A Log_{10} transformation controlled for the exponential nature of the keyspace metric.

Three hundred and fifty-five participants completed the online questionnaire. They were recruited through the mailing lists and social media presences of a professional association or network. Two hundred and thirty-five experts on cyber security issues (209 male, 26 female) were recruited from a nationally recognised professional computer association in the UK and 120 non-experts (21 male, 99 female) were recruited from several nationally recognised associations and networks for the arts, humanities and social sciences in the UK.

Overall, it was found that cyber security experts created more secure passwords compared with non-experts, insofar that experts' passwords were less susceptible to both dictionary and keyspace attacks. Specifically, non-experts' passwords were more likely to be in common attack dictionaries than experts' passwords. Similarly, non-experts chose passwords with a smaller keyspace metric that is more easily cracked than experts.

Our hypotheses, which considered the relationship between personality characteristics and strength of password choice, were only partly supported. None of the personality characteristics predicted whether a password was susceptible to the more advanced keyspace attack. However, individuals high on internal locus of control were more likely to create a secure password more resistant to a dictionary attack compared to those with a low internal locus of control.

Although not all our hypotheses were fully supported, the results reveal a more complex picture about individual differences and password choice. They tell us that having a greater knowledge about security issues is important. Importantly, however, personality plays a role in choice of password. As we would expect, those who take a more fatalistic approach were less likely to choose a secure password. These individuals might have felt that given they believe they have little control over what happens in their lives that hackers will break into their accounts no matter what password they select. The implications for these findings with respect to future educational and media campaigns will be discussed as well as the future studies we have planned to further this work.

References

1. Bhuyan, S., Greenstein, J. S., & Juang, K. A. (2013). Evaluating the Usability of System-Generated and User-Generated Passwords of Approximately Equal Security. In: *Human Aspects of Information Security, Privacy, and Trust* (pp. 3-12). Springer Berlin Heidelberg.

2. Carstens, D. S. (2009). Human and social aspects of password authentication. In: M. Gupta & R. Sharman (Eds.), *Social and human elements of information security: Emerging trends and countermeasures* (pp. 1-14). Hershey, PA, US: Information Science Reference Global.

3. Hoonakker, P., Bornoe, N., & Carayon, P. (2009, October). Password authentication from a human factors perspective: Results of a survey among end-users. In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (p. 459-463). SAGE Publications.

4. Lorenz, B., Kikkas, K., & Klooster, A. (2013). "The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups. In: *Human Aspects of Information Security, Privacy, and Trust* (pp. 276-283). Springer Berlin Heidelberg.

5. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers *& Security*, 24(2), 124-133.

6. Zviran, M., & Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information System*s, 15, 161-186.

7. Herley, C., van Oorschot, P. C., & Patrick, A. S. (2009). Passwords: If we're so smart, why are we still using them? In: *Financial Cryptography and Data Security* (pp. 230-237). Springer Berlin Heidelberg

8. Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29(3), 233-244.

9. Von Zezschwitz, E., De Luca, A., & Hussmann, H. (2013). Survival of the Shortest: A Retrospective Analysis of Influencing Factors on Password Composition. In: *Human-Computer Interaction–INTERACT 2013* (pp. 460-467). Springer Berlin Heidelberg.

10. Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., ... & Egelman, S. (2011, May). Of passwords and people: measuring the effect of password-composition policies. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2595-2604). ACM.

11. Proctor, R. W., Lien, M. C., Vu, K. P. L., Schultz, E. E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers*, 34(2), 163-169.

12. Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., Cook, J., & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65(8), 744-757.

13. Creese, S., Hodges, D., Jamison-Powell, S., & Whitty, M. (2013). Relationships between Password Choices. Paper presented at *Perceptions of Risk and Security Expertise. In: Human Aspects of Information Security, Privacy, and Trust* (pp. 80-89). Springer Berlin Heidelberg.

14. Hellman, M. (1980). A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory, 26*(4), 401-406.