Security-Conscious Password Behavior from the End-User's Perspective

CSIAC Report | September 26, 2019

Author: Anna Lena Fehlhaber, IT Security department, Leibniz University, Hanover, Germany, fehlhaberlena@sec.uni-hannover.de

Video Podcast Companion URL: https://www.csiac.org/podcast/security-conscious-password-behavior

Keywords

Password Security, Human in the Loop, Cybersecurity, Human Behavior

Introduction

Even though technical solutions for security problems are widespread, there are no adequate security measures against precarious user behavior. Even if hashing and encrypting are used correctly in masking the passwords, attackers can bypass these strongpoints by going for the weakest link. Most likely this will happen through sharing a password, using an already leaked password, or creating an feasibly guessable password (Olmstead & Smith, 2017). Furthermore, people seem to feel safe in cyberspace, even if they engage in risky behaviors (Vozmediano, San-Juan, Vergara & Lenneis, 2013).

Research Field

User authentication by text-based password is still common for various applications. Contrary to the relevance of secure user behavior while choosing and handling the password, academic researchers tended to neglect this topic for the last few years, so the problem of human decision-making in text-based password creation remains mostly uninspected.

After highlighting the human factor as a potential error in cybersecurity, along with many empirical studies regarding this topic, various strategies were offered to counter this threat (Shay et al., 2012; Fahl et al., 2013; Ur et al., 2012; Garfinkel & Miller, 2005; Sheng, Broderick, Hyland & Koranda, 2015). While most of these strategies, advices and technical solutions concerning weak passwords, remain unknown to the wider public, some solutions were adapted in common practice, e.g. password management tools. The mentioned password managers generate plenty of strong and unique passwords for each website a user may require a password for, and all of them can be easily accessed with just one master password. In contrast to most user-generated passwords, passwords created by password managers are pseudo-random and hard to predict. Users who try to generate a strong password often fail this task, because they use strategies a computer might easily bypass, such as adding special characters and numbers at the end of their password, as well as using a capital letter in the beginning (Ur et al., 2012). The mentioned password managers or even a program generating pseudo-random strings can lead to safer passwords regarding the possibility to be cracked. For end users, aspects of usability and intelligibility seem to determine the acceptance of software supporting password purposes, yet the usage of password management tools is the exception rather than the norm (Olmstead & Smith, 2017).

Most people have not altered their password-related behavior, it is widely known that people are prone to create passwords which are easily guessed, and engage in unsecure practices, such as reusing passwords across different accounts (Wang, Jan, Hu, Bossart & Wang, 2018; Hunt, 2019; Stobert & Biddle, 2014). Furthermore, false lore and myths about secure password creation seem to endure, conveying an illusion of security from a users' perspective (Ur et al., 2015; Ur et al., 2016). This article will identify common ideas about secure passwords by surveying 98 participants regarding their password strategies and habits, as well as asking them to estimate the security of their strategies and encouraging them to rate the security of the other strategies collected in this study.

Methodology

Participants

Out of 119 college students all claiming to be interested in cybersecurity, 98 participants completed the study. The sample consisted of 57.7% male students and 42.3% female students, with 61.2% attending a bachelor's program, and 38.8% registered in a master's program. Within the sample, about 1/3 of students were enrolled in an IT engineering study program, the remaining 2/3 of students' study business sciences, social sciences or natural sciences. Less than 5% are pursuing their teacher´s certificate.

The study included only students who showed interest in cybersecurity, potentially limiting the overall external validity of the study. Furthermore, it seems noteworthy, that preceding studies have stated no significant limitation of ecological validity by using students for password experiments and studies (Fahl et al., 2013). Because a general awareness and the willingness to reflect about password strategies were necessary to conduct the study design, addressing interested students offered the best chance to obtain a relatively large pool of participants with different backgrounds.

Privacy and Data Protection

Due to the strict data protection law applied in Germany, the participants written approval was obtained before as well as after the study. Additionally, all participants could withdraw their consent at any time while the study was conducted without suffering any consequences, deleting their data from the study´s data pool entirely.

During the study, pseudonyms were used to guarantee anonymity, allowing no inference with any individual participant.

Evaluation of Reliability

There were two mechanisms implemented in the study design to assure reliability:

- Before the interrogation, participants had to conduct a test instruction to verify their understanding of the task.
- After the study, participants were asked to disclose any false answers, emphasizing once more that there will be no negative consequences. In case of confirmation, associated data was deleted from the pool.

Additionally, because password strategy can be perceived as a rather sensitive topic, people were individually asked to explain their strategies for the first part of the study in a guided interview, while the rating of strategies was mutually conducted in a team environment afterwards. To prevent interference, spoken communication was forbidden during this stage of the study, and the participants couldn't see each other's choices due to the seating arrangements. Their individual answers were to be stated by display of one- or two-colored cards; the options were 'totally safe' (green), 'totally unsafe' (red) and 'not sure' (green and red at the same time).

Findings

In the first part of the study, participants were asked about known strategies to create a password in a guided interview, later scientifically categorized and analyzed. Although people were only asked which strategy they know, 68 of 98 mentioned strategy they themselves use.

Questions regarding the creation of their passwords were phrased carefully, emphasizing the need not to mention the password itself. Furthermore, participants were asked how they tend to handle their password, e.g. dealing with their password in daily routine.

33.6% of study participants believed that their password behavior is not safe at all, neglecting the choice of a safe password creation strategy and rating themselves problematic password handlers, claiming to be lacking knowledge. 29.6% were sure to have chosen a safe password creation strategy and to have safely handled the password. Intriguingly, most of them (21 of 29 participants) claimed to manage their passwords safely, but revealed during the interview that they wrote it down in some text editor to remember, saved it manually to the clipboard or let browser plugins handle their passwords. When asking the participants if they shared their passwords with close friends or family members, 14.3% agreed, and declared that this does not make their password less safe, as they trust those few who have access to their passwords.

	Safe Password handling	Weak Password handling
Safe password creation: 31 participants	29 participants	2 participants
Weak password creation: 67 participants	34 participants	33 participants

Fig. 1: Self-Evaluation of password creation and handling regarding security in the participants´ perspective, n=98

In the second part of the study, all password creation and handling strategies suggested were collected in a large pool and offered to the participants to rate according to their understanding of safety.

The collected ideas and strategies for password creation and password handling are listed below:

- Usage of a whole sentence without semantic sense, e.g. "I like to look for crocodiles in winter."
- Usage of the beginning letters of a sentence without semantic sense, e.g. "Iltlfciw."
- As many numbers as possible
- As many special characters as possible
- As long as possible
- Use pre-generated passwords sent per e-mail
- No names within the password
- Use of a password manager
- Generate a password in a browser online
- Wipe over the keyboard to generate a password

Participants were especially unsure about using whole sentences or acronyms for password creation. However, 39 participants considering whole sentences and 56 participants considered acronyms as totally safe strategies.

While length and the usage of special characters indicated a safe password for more than 60% of the participants, the use of as many numbers as possible and avoidance of names was considered a poor strategy by 64.7% of the participants.

The usage of pre-generated passwords sent per e-mail when creating an account on the internet was rated unsafe by 2/3 of the participants, the remaining third were unsure about safety aspects using this strategy.

The generation of passwords online or locally by password management software was believed to be totally safe by approximately 82%. The strategy of wiping over the keyboard was assessed as safe by 86.2%, leaving 7.8% to be unsure and 2% to regard this as an insecure strategy for password creation.

In regards to their quality, there were distinctly fewer ideas collected for managing passwords.

Participants suggested:

- Use of a (secure) master password over a long time
- Active search for leaked passwords to ensure the own password was not leaked
- Use of the same (insecure) password over a long time
- Use of the clipboard while handling the password
- Note the password in a text file on their terminal device
- Note the password manually on a slip of paper
- Share the password with close friends or family

More than 96% stated, that using the same password over a long time as an insecure strategy, another 93% believed to put it down in a text file to be insecure.

92.3% of the participants were not sure about the safety level regarding a secure master password, the remaining participants believed a secure master password, even if used over a long period, to be safe.

The use of the clipboard, e.g. copying and pasting the password, was rated as totally secure by 36.3% of the participants, leaving another 40.2% unsure in regards to this strategy´s safety, while the remaining participants thought this to be an insecure solution.

The active search for leaked passwords was deemed safe by most participants (91 of 98) after explaining the possibility, by means of questions regarding this statement even after, this option was not familiar to any of them. Sharing a password with close friends or family was deemed unsafe by 22 participants, while another 21 claimed this to be a secure strategy, leaving the rest of the participants indecisive.

Summary

The results of the study reveal that nearly a third of participants thought to have created and handled their password safely, at the same time uncovering poor strategies in most cases from a technical point of view in both areas. Only 6.5% of the participants who had thought to have created their password safely acknowledged their password handling to be lacking.

Same can be reported for those who rated their password creation strategy as relatively risky. While thinking their handling of the passwords should be secure enough, about 70% of the participants interviewed revealed their own password strategy without even being asked.

Though 68.37% claimed to use a weak password, only half of them admitted that their password handling also needs improvement. Those participants who admitted to use insecure passwords more often claimed to use a weak strategy in password handling as well.

The findings concerning password handling implicate the participants' knowledge of some strategies, e.g. the usage of a weak password over a long time as being unsafe, while still actively using this strategy. For common threats, e.g. regarding the clipboard use when handling a password, participants were mostly unaware of risks.

Contrary to expectations, sharing a password with a close friend or family member was not rated unsafe by most participants, indicating that concepts relying on trust serve as an important influencing factor in safety decision making.

Summarizing, while most of the participants seem to reflect on their password creation, the knowledge for safe password handling seems missing in most cases. This issue is especially highlighted by the findings of the study's second part, where the participants were asked to rate the strategies regarding security. While most participants agree that e.g. password management tools or the pseudo-random generation of a password is safe, they were divided by their understanding of safe password handling, or even acted contrary to their belief when identifying an unsafe strategy.

Independent of their own perception in both parts of the study, most commonly used password and creating and handling strategies are insufficient from a technical perspective, still indicating the need to educate end-users and to allow more clarification. Nevertheless, even those who recognized or estimated using insecure strategies have not approached this problem sufficiently, leaving questions regarding motives for their behavior unclear. Therefore, it is necessary to create a deeper understanding as well as to conduct further research on strategies, behaviors, and security awareness.

References

Fahl, S., Harbach, M., Acar, Y., & Smith, M. (2013). On the ecological validity of a password study. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13),* Article No. 13.

Garfinkel, S.L., & Miller, R.C. (2005). Johnny 2: a user test of key continuity management with S/MIME and Outlook Express. In *Proceedings of the 2005 symposium on Usable privacy and security (SOUPS '05),* pp. 13-24.

Hunt, T. (2019). Pawned Passwords list Version 4. Retrieved from https://haveibeenpwned.com/Passwords.

Shay, R., Kelley, P.G., Komanduri, S., Mazurek, M.L., Ur, B., Vidas, T., Bauer, L., Christin, N., & Cranor, L.F. (2012). Correct horse battery staple: exploring the usability of system-assigned passphrases. *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS 2012),* Article No. 7.

Sheng, S., Broderick, L., J Hyland, J., & Alison Koranda, C. (2015). *Why Johnny still can't encrypt: evaluating the usability of email encryption software.* Retrieved from https://www.researchgate.net/publication/228900555_Why_Johnny_still_can't_encrypt_evaluating_the_usability_of_email_encryption_software.

Stobert, E., & Biddle, R. (2014). The password life cycle: user behavior in managing passwords. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS '14),* pp. 243-255.

Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., & Christin, N. (2012). How does your password measure up? The effect of strength meters on password creation. In *USENIX Security Symposium,* pp. 65-80.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., & Cranor, L. (2015). "I added '!' at the end to make it secure": Observing password creation in the lab. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS '15)*.

Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., & Cranor, L.F. (2016). Do Users' Perceptions of Password Security Match Reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), pp. 3748-3760.

Vozmediano, L., San-Juan, C., Vergara, A.I., & Lenneis, A. (2013). Risk perception in digital contexts: questionnaire and pilot study. *International e-Journal of Criminal Science, 4 (7),* Retrieved from http://www.ehu.eus/ojs/index.php/inecs/article/view/13224/11934.

Wang, C., Jan, S.T.K., Hu, H., Bossart, D., Wang, G. (2018). The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18)*, pp. 196-203.