Interactive Stories for Security Education: A Case Study on Password Managers

Carlo Sugatan and Florian Schaub
University of Michigan School of Information

Abstract

Password managers allow us to generate unique passwords that protect our online accounts and improve our password management. Despite being one of the most highly recommended security tool, adoption of password managers remains low. The low adoption may be attributed to how it is generally better to learn concepts through a feedback loop. That is, we are informed, make a decision, and ultimately experience the consequences of our decisions. This feedback loop is often absent in how security advice is given. Interactive stories have the potential to remedy the absence of a feedback loop by having the reader experience the consequences of their decisions and learning from the outcome. This study explores the potential of using interactive stories to simulate security consequences to convey lessons and risks. Through participatory design, a survey, and an online cognitive test, we developed and validated an interactive story focused on password managers. Our preliminary results show promise for using interactive stories in the security education ecosystem.

1 Introduction

As online interactions becomes more ubiquitous and complex, users struggle to identify the risks and threats of their online behaviors. [15, 16]. Generally, people best learn concepts through a feedback loop [15]. That is, we are informed, make a decision, and experience the consequences of that decision. However, this feedback loop is often absent in security advice. It is easier for users to reject security advice, such as using two-factor authentication, if they never experienced having their personal accounts compromised [16]. Interactive stories have the potential to remedy the absence of a feedback loop by having the reader experience the consequences of their decisions and learning from the outcome. Previous studies have shown the effectiveness of stories in teaching security lessons and even influencing protective user behaviors [3, 11, 12, 15, 16, 20, 26]. We propose using an interactive story in order to effectively simulate security consequences. An interactive story, also known as a Choose-Your-Own Adventure story, is a form of genre that positions the reader to influence a nonlinear narrative. The reader engages with the actions and dialogues to influence the final outcome of a story [17]. We imagine interactive stories to be a great addition in teaching security and privacy, especially in the context of classrooms and workplace training. We conducted participatory design sessions and deployed a baseline knowledge survey about password managers in order to create an effective narrative for the story. In addition, we conducted online cognitive interviews in order to test the comprehensibility of the interactive story. Our preliminary findings show the promise of using interactive stories as an educational intervention in security education.

2 Related Work

2.1 Negative Experiences in Security

Negative experiences contribute to how users make decisions on what security practices they should adhere to. For example, Vaniea et al. found that negative experiences regarding installing updates on Windows computers prevented users to install new updates, regardless of whether it was an important update for security [19]. Indeed, we often learn best if we are able to make a decision and observe or experience the consequences of that decision [15]. Rader demonstrated that users who learned about threats through past experiences were more motivated to engage in security protection behaviors such as creating strong passwords, compared to those who never experienced a security-related threat [14, 15]. Motivating users

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Boston, MA, USA.

to follow security advice is difficult if the user faces no threats in the moment. How do we demonstrate the risks associated with poor online behavior and management to those who feel no real threat?

2.2 Interactive Stories

An interactive story or Choose-Your-Own-Adventure story positions the reader as a director in which they may influence the ending of a story. Prior work has shown the efficacy of interactive stories in changing behaviors such as improving asthma control among children or improving patients' confidence in managing their hospital stay [22, 24]. Users often have no control over the decisions of the characters in video games or comics. While this may be effective in changing some behaviors, it does not fully capture what it means to control and experience the decisions you make. Zou et al. investigated the inaction of users after the Equifax data breach which reveals that awareness is not enough to trigger action or modification of security behaviors [26]. Interactive stories around security contextualizes the learning experience as it simulates what it may feel like to experience a security threat based on the users' decisions. These types of narratives evoke psychological responses not typically found in traditional methods of advice dissemination [17]. This puts the reader as a main character with a responsibility to take action. Dincelli used a similar approach in order to determine what security threats one is susceptible to [5]. This works expands on Dincelli's work in the context of simulating security experiences in order to increase adoption of password managers.

3 Interactive Story Generation and Test

We used a mixed-method approach using participatory design and deploying a baseline knowledge survey in order to inform the narrative of the story. The participatory design created character themes, narrative themes, and consequences themes while the survey revealed the common misconceptions and perceived factors (security, trust, necessity, risks, cost). Afterwards, we conducted an online evaluation study in order to test the comprehensability of the story. We discuss the methods in more detail in the following sections.

4 Participatory Design

Participatory design (PD) is a design approach that actively involves stakeholders in the design process of a particular product [8]. Prior work has shown the effectiveness of PD in games when users were involved as informants that influenced the game levels and challenges [4]. In addition, participatory design has been used in security and privacy in order to inform device control and user interfaces [21,23]. Using participatory design allowed us to facilitate the creation of the interactive story based on participants' knowledge and background rather than the authors' security background.

Three workshops, each with three participants, were conducted in November 2019. Participants were recruited through a university email list as well as through social media websites such as Twitter and Facebook. Participants were invited in groups at a time, and were grouped based on whether or not they had experience using a password manager. This group separation allowed different conversations about password managers to take place based on the groups' experience. It also ensured that people created stories from their own experiences and knowledge about password managers, rather than someone else's experiences with password managers. Participants were compensated $15 for an approximately one-hour workshop session. The study was exempted by the University of Michigan Institutional Review Board.

Participants were tasked to create their own interactive stories about convincing others to use password managers. The activity had them create characters, a setting, character goal(s), decisions, and different types of endings or consequences. Each participant had an opportunity to present their work to everyone, which was audio and video recorded for a qualitative content analysis [9].

4.1 Participatory Design Results

The results of the participatory design shaped the content of the story. Namely, the character themes, narrative themes, and the consequences themes.

Participants We recruited 9 participants, with 4 men and 5 women. No participant had experience with a third-party password manager such as 1Password or LastPass, but rather, use built-in password managers such as Chrome Password Storage and Apple Keychain. All of the participants have some college education, with a Master's degree being the highest obtained degree. Participants were relatively young, with 28 years old being the oldest.

Character Themes All participant-created storyboards included two characters in some sort of relationship (i.e., husband and wife, or brother and sister). Often, the extra character served to be an agent in guiding and convincing the main character to adopt a password manager. This aligns with Redmiles et al.'s edutainment study in which they found the theme of using a "trustworthy, personified security advisor" to deliver security advice and instructions [6].

Narrative Themes The major narrative focuses on the goal to conveniently access accounts. This may reveal the underlying mental model of utilizing password managers for convenience, which is aligned with previous studies [1, 7, 25], in which most participants expressed that convenience was a main contributor of adoption of password managers. This finding is important because it may be effective to showcase how password managers can be convenient to use, rather than solely focusing on the security aspect.

Consequence Themes In line with the narrative theme, most consequences focused on inconvenience such as resetting passwords rather than the possibility of a data breach. However, we decided to still include security consequences for a compelling ending and implemented the notion of inconvenience as a main narrative instead.

5 Baseline Knowledge of Password Managers Survey

The participatory design sessions were helpful in creating the narrative and content of the story. However, the specific lessons to convey regarding password managers remained ambiguous. Thus, we conducted a survey to elicit baseline knowledge about password managers. This survey helped further inform the interactive story in identifying the gaps or misconceptions of people's knowledge surrounding password managers. The survey looked at 1) perceived security, 2) perceived trust, 3) perceived necessity and acceptance, 4) perceived ease of use, 5) perceived cost, 6) perceived risks, and 7) features of password managers. These factors were summarized from previous password manager adoption studies [1, 2, 7, 25]. These factors help us understand where the knowledge surrounding password manager lies.

Our Qualtrics survey was deployed in March 2020 via Prolific [13] and received 200 responses. Participants were compensated $2.00 for a 6 minute survey. The survey queried participants' perceptions and experiences of password managers. These perception questions were phrased as true or false statements and were randomized in the final deployment of the survey. Additionally, the survey queried demographics such as age, gender, education, income, and technology experience. The study was exempted by the University of Michigan Institutional Review Board.

5.1 Baseline Knowledge of Password Managers Survey Results

Participants Overall, 67% respondents have experience with password managers, while only 36% have never used a password manager. In addition, 86.5% do not have an IT background, while 13% have an IT background. Participants' age ranges included 18-24 (30.7%), 25-34 (37.6%), 35-44 (19%), 45-54 (3.4%), and 55+ years (5.4%). 51% were women, 43.5% were men, and 0.4% identified as non-binary. 1.5% received an education below a high school diploma, 17% are high school graduates, 21.5% have some college background but no degree, 7.5% received an associate's degree, 35.5% with a Bachelor's degree, 15.5% with a Master's degree, and 2.5% with a professional degree. The percentages do not add up to 100 because some preferred not to answer the questions.

Significance of Perceived Factors We conducted a chi-square test to find any relationship between those with or without password manager experience to the perceived factors. Overall, we found significant relationship between password manager experience and perceived trust, necessity and acceptance, ease of use, cost, and risks. In other words, those without password manager experience seem to believe that password managers are unnecessary, difficult to use, expensive, risky, and not trustworthy. Therefore, this survey helped informed the lessons to be covered in the interactive story, namely about its convenience, installation, cost, and security.

5.2 Story Details

We used Twine to build out the interactive story, which is an open-source tool for developing interactive stories [18]. A professional artist was hired to illustrate the scenes.

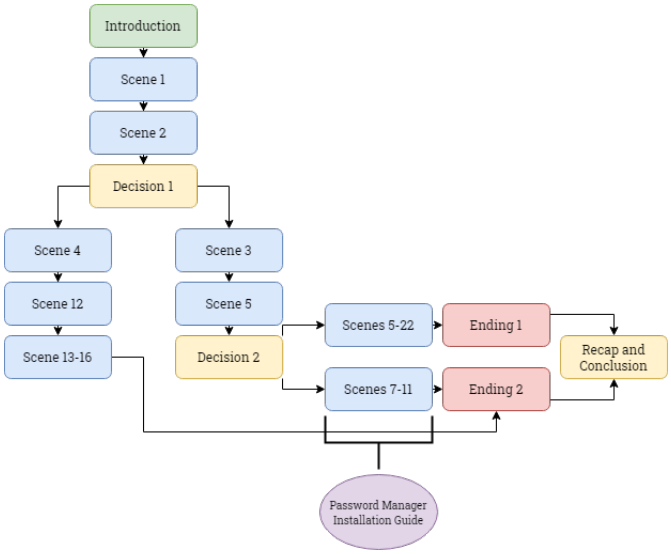

Figure 1: Story branch of the interactive story

Synopsis Lesley and Katie are best friends wanting to purchase tickets for their favorite band. Lesley forgets her password to purchase tickets on the concert website. Katie suggests Lesley to start using a password manager to manage her passwords. Katie promotes the convenience and usability, but Lesley remains apathetic. Will Lesley take Katie's advice? What risks will she face and will they make it to the concert before the tickets are sold out?

Decisions The major decision a reader will make is whether to start using a password manager or not. If the reader chooses to adopt a password manager. There will be multiple trade-offs that may encourage the reader to abandon the password manager setup in preference for discounted concert tickets. These decisions allow the readers to reflect on the decisions while facing trade-offs.

Consequences There are two consequences in the story. If the reader decides to adopt a password manager, they would

receive the "good" ending in which Lesley is protected by a hack on the concert website because she used a strong, unique password on that website. If the reader chose to decline to use a password manager, they would receive the "bad" ending where Lesley's account is compromised because she used the same password across multiple websites. This ending showed the risks that can result from reusing passwords across multiple accounts. These consequences will allow the reader to reflect on their decisions while understanding why these events occurred due to their security choices.

Password Manager Installation Guidance Beyond highlighting consequences, another benefit of the interactive story is experiencing the setup process of a password manager. As seen from previous literature regarding password manager adoption [1, 2], many people feel as if the setup process of password managers is intimidating and difficult. Therefore, a major design decision was to include several scenes and illustrations regarding the installation process of password managers. The goal was to help the reader to be less intimidated in approaching the setup process, and therefore, increase the likelihood of adoption in the future.

Conclusion While the specific ending may be different for the different branches, the last scene that concludes the story is shown for both branches. The last scene summarizes the benefits of using a password manager, further emphasizing the lessons learned in the interactive story. In addition, the last scene concludes by showing a list of free and paid password managers. This reduces the friction in having readers adopt a password manager. This allows the reader to see the benefits, learn security lessons, and immediately have the opportunity to accept this advice.

Figure 2: Example of scenes from the interactive story

6 Evaluation

The goal of the evaluation study was to pre-test the efficacy of the interactive story in providing awareness and comprehension about password managers. Participants were invited to an online cognitive interview where they were free to express any concerns, improvements, and comments regarding the story's content, lessons, illustrations, and ways to improve [10].

A recruitment message was sent through the University of Michigan School of Information email lists in order to recruit participants. The online cognitive interview was conducted in April 2020 with 8 participants. Participants were instructed to "think aloud" as they went through each page of the interactive story. The cognitive interviewing technique allowed participants to provide insights regarding their interpretation and comprehension of the interactive story. This was important to ensure lessons are effectively communicated. Participants were compensated $10 for being a part of the online evaluation study. The study was exempted by the University of Michigan Institutional Review Board.

7 Results of the Evaluation Study

This section describes three main points that were commonly cited during the evaluation study. These findings look specifically at the effectiveness and comprehensibility of the story.

The Use of Trustworthy Agents The supporting characters, referred to as security agents, guided the main character in the process of installing a password manager. Overall, the security agents were effective in explaining the process of installing password managers, evidenced by the asking how participant's were able to articulate the installation steps. This is consistent with previous studies showing how secondary characters can help with explaining security concepts [6].

Describing Password Managers After completing the interactive stort, all participants were able to articulate what a password manager is, its functionality, and the benefits of using one. All participants were confident that password managers would protect them and keep their passwords safe. One participant stated "So, from what I understand, the password managers will use some type of encryption technology to keep your passwords safe." After follow-ups, most participants said that the interactive story helped improve their knowledge and trust with password managers.

Improvements There were several suggestions that can be implemented in the future to improve the interactive story. Many felt that the use of animations may improve the interactions. Many found the installation guide long, so summarizing the the guide may be helpful. Implementing animations and shortening the story will help with attention, thus, amplifying the effects of the lessons and risks.

8 Conclusion and Future Work

This study was a necessary precursor to conduct further validation studies to compare the efficacy of the developed interactive story against other modes of security advice.

The preliminary results suggest that there is a strong potential to use interactive stories to simulate security consequences in order to teach security lessons, and ultimately, to change and promote safer security behaviors.

References

[1] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? 01 2016. https://doi.org/10.14722/eurousec.2016.23011.

[2] Salvatore Aurigemma, Thomas Mattson, and Lori N. K. Leonard. So much promise, so little use: What is stopping home end-users from using password manager applications? In *HICSS*, 2017. https://core.ac.uk/download/pdf/77239955.pdf.

[3] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. The effect of social influence on security sensitivity. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, SOUPS'14, pages 143–157, Berkeley, CA, USA, 2014. USENIX Association. http://dl.acm.org/citation.cfm?id=3235838.3235851.

[4] Ann DeSmet, Deborah Thompson, Thomas Baranowski, Antonio L. Palmeira, Maïté Verloigne, and Ilse de Bourdeaudhuij. Is participatory design associated with the effectiveness of serious digital games for healthy lifestyle promotion? a meta-analysis. In *Journal of medical Internet research*, 2016. https://doi.org/10.2196/jmir.4444.

[5] Ersin Dincelli and Indushobha Chengalur-Smith. Choose your own hacking adventure: Contextualized storytelling to enhance security education and training. 08 2019.

[6] Candice Schumann Rock Stevens Peter Sutor Michelle L. Mazurek Elissa M. Redmiles, Angelisa Plane. Can edutainment change software updating behavior?, 2017. https://www.ndss-symposium.org/ndss2017/ndss-2017-poster-session/can-edutainment-change-software-updating-behavior.

[7] Michael Fagan, Yusuf Albayram, Mohammad Khan, and Ross Buck. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, 7:12, 03 2017. https://doi.org/10.1186/s13673-017-0093-6.

[8] Kim Halskov and Nicolai Brodersen Hansen. The diversity of participatory design research practice at pdc 2002–2012. *International Journal of Human-Computer Studies*, 74:81 – 92, 2015. https://doi.org/10.1016/j.ijhcs.2014.09.003.

[9] Ole R. Holsti. *Content analysis for the social sciences and humanities*. Reading, Mass., Addison-Wesley Pub. Co., 1969.

[10] Jacqueline P. Leighton José-Luis Padilla. *Understanding and Investigating Response Processes in Validation Research: Cognitive Interviewing and Think Aloud Methods Chapter*. Social Indicators Research Series, 2017.

[11] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, 2015. USENIX Association. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang.

[12] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM Conference on Interaction Design and Children*, IDC '18, page 67–79, New York, NY, USA, 2018. Association for Computing Machinery.

[13] Prolific. Online participant recruitment for surveys, 2020. https://www.prolific.co/, Last accessed on 2020-03-19.

[14] Emilee Rader and Rick Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 12 2015. https://doi.org/10.1093/cybsec/tyv008.

[15] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 6:1–6:17, New York, NY, USA, 2012. ACM. http://doi.acm.org/10.1145/2335356.2335364.

[16] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288, May 2016. http://doi.acm.org/10.1145/2335356.2335364.

[17] Brett Shelton. Designing and creating interactive fiction for learning. 01 2005. https://www.researchgate.net/publication/228959393_Designing_and_creating_interactive_fiction_for_learning.

[18] Twine. What is twine?, 2020. https://twinery.org/, Last accessed on 2020-04-05.

[19] Kami E. Vaniea, Emilee Rader, and Rick Wash. Betrayed by updates: How negative experiences affect future security. In *Proceedings of the SIGCHI Conference*

on Human Factors in Computing Systems, CHI '14, page 2671–2674, New York, NY, USA, 2014. Association for Computing Machinery. https://doi-org.proxy.lib.umich.edu/10.1145/2556288.2557275.

[20] Rick Wash and Chis Fennell. Emotional impact: How stories affect password behavior. 2018. https://bitlab.cas.msu.edu/papers/workshop/2018/08/12/security-stories-soups.html.

[21] Susanne Weber, Marian Harbach, and Matthew Smith. Participatory design for security-related user interfaces. 01 2015.

[22] Tami Wyatt, Xueping Li, Yu Huang, and Rachel Farmer. Developing an interactive story for children with asthma. *Computers, Informatics, Nursing (Accepted)*, 01 2013. https://doi.org/10.1016/j.cnur.2013.01.006.

[23] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[24] Langxuan Yin, Lazlo Ring, and Timothy Bickmore. Using an interactive visual novel to promote patient empowerment through engagement. In *Proceedings of the International Conference on the Foundations of Digital Games*, FDG '12, pages 41–48, New York, NY, USA, 2012. ACM. http://doi.acm.org/10.1145/2282338.2282351.

[25] Shikun Aerin Zhang, Sarah Pearman, Lujo Bauer, and Nicolas Christin. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association. https://www.usenix.org/conference/soups2019/presentation/pearman.

[26] Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub. "i've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, SOUPS'18, pages 197–216, Berkeley, CA, USA, 2018. USENIX Association. http://dl.acm.org/citation.cfm?id=3291228.3291245.