The Design and Development of an Interactive Story for Security Education: A Case Study on Password Managers

by

Carlo Sugatan

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science in Information
University of Michigan
2020

Thesis Committee:

Professor Florian Schaub, Chair
Professor Barry Fishman

ACKNOWLEDGEMENTS

I extend my greatest gratitude to my advisor, Florian Schaub, for agreeing to take me up as his first MTOP student and continually mentoring and fostering me throughout this journey. I have become a better researcher and student from your constant feedback, encouragement, and brilliance.

I like to thank the University of Michigan School of Information's Engaged Learning Office for providing funding to support this work. I would like to thank Barry Fishman for agreeing to be part of the committee and providing his expertise and feedback.

I would also like to thank my friends and colleagues from the University of Michigan School of Information and SPI (Security, Privacy, Interaction) Lab. Your feedback, intellect, encouragement, and company has made my time as a student at University of Michigan one of the best.

Of course, I am thankful for my sisters, Arlene and Rochelle, for their support, humor, love, and interest in my work.

I don't know where I would be without the support of my partner, Connor, who was always there to support and encourage me. I dedicate this work to you. I love you.

Last, but not least, I want to express my gratitude to my parents, Gorgonia and Ricardo, for their love and support. I stand on the shoulders of giants. Constantly guided, constantly steadied. Thantk you.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

LIST OF TABLES

Table

ABSTRACT

The Design and Development of an Interactive Story for Security Education: A Case Study on Password Managers

by

Carlo Sugatan

Chair: Florian Schaub

Password managers allow us to generate unique passwords that ultimately protect our accounts and improve our password management. Despite being one of the most common security advice, adaption of password managers remain low. The complexity and magnitude of security advice leave users pondering about the best decision to keep themselves safe online. Indeed, it is generally better to learn concepts through a feedback loop, where we are informed, make a decision, and ultimately experience the consequences of our decisions. This feedback loop is absent in the traditional way security advice is given. In this thesis, I explore the potential of using interactive stories (Choose-Your-Own Adventure stories) to simulate security consequences to convey lessons and risks. Through participatory design, survey methods, interviews, and learning science principles, I developed and validated a comprehensive and effective interactive story to be used in security education. The results of this thesis show a promising approach of using interactive stories in the security education ecosystem.

CHAPTER I

Introduction

Given the complexity and multitude of security advice, users struggle to determine how to stay digitally secure. As online navigation becomes more ubiquitous, both digital experts and non-experts struggle to understand the risks involved with online behaviors, leading to poor management of data security [4, 5]. The issue arises as users struggle to identify the perception of risks and threats of their online behaviors. Generally, people best learn concepts through a feedback loop. That is, we are informed, make a decision, and experience the consequences of that decision. However, this feedback loop is often absent in information security experiences. It is easier for users to reject a security advice such as using two-factor authentication if they never experienced having their personal accounts compromised [6].

In order to effectively simulate security consequences to convey lessons, I propose using an interactive story (Choose-Your-Own Adventure story). An interactive story is a form of digital entertainment that positions the reader as a director in which they may influence a nonlinear narrative. The reader engages with the actions and dialogues to influence the final outcome of a story [7].

In this thesis, I seek to answer the following research questions:

- RQ1: How effective are interactive stories in being used as an educational intervention in order to teach lessons about password managers?
- RQ2: What are effective ways to create a comprehensible interactive story in order to encourage others to start using a password manager?

While answering these questions, I describe the iterative design process involving participatory design sessions and user testing (Chapters 3, 5, 6) and identify gaps in people's knowledge about password managers (Chapter 4). Finally, I present the final, validated interactive story that came out of this study.

I conducted a series of sessions with users to develop a comprehensible and effective interactive story. First in Chapter 3, I ran participatory design sessions with nine users in which they were tasked to create a storyboard for an interactive story to encourage others to use a password manager. The results from this study informed the content of the interactive story. Namely, the characters, narrative, and consequences themes. The results suggest focusing on the *convenience* of password managers as well as focusing on the *inconvenience* of account lockouts rather than something drastic such as a hack or data breach.

In chapter 4, I deployed an online survey examining the baseline knowledge of password managers. This survey helped further inform the interactive story in identifying the gaps or misconceptions of people's knowledge surrounding password managers. The results from this study suggest to focus around correcting mental models of the security aspect and features of password managers. I shift the focus around teaching lessons about reusing passwords, and focusing on the benefits of the auto-fill feature. This study also informed the design decision of integrating a password manager installation guide in the story to dispel the misconception that installing a password manager is difficult and technical.

To ensure that the interactive story is comparable to the traditional advice of password managers typically written in text form, I conducted a systematic liter-

ature review on password managers in Chapter 5 looking at behavioral inhibitors, perception factors, failed adoption reasons as well as password manager text advice from media outlets. This helped inform how to structure the story by identifying the main inhibitors and barriers in adoption as well as the phrasing of password manager advice. Finally in Chapter 6, I conducted an online, cognitive interview to evaluate the comprehensability of the interactive story. This study helped prove if the interactive story was successful in conveying the risks and consequences of not using a password manager as well as the overall security lesson to improve adoption rates of password managers.

1.1 Contributions

This work makes several contributions in security education:

- First, I developed and validated a comprehensible and effective interactive story to be used for security education. This interactive story was created from the combination of different sessions from real users as well as using learning science principles in order to inform, educate, and delight readers. In doing so, I provide a graphical security education material that can be used to train or teach security lessons.

- Secondly, I provide findings regarding people's general knowledge and misconceptions regarding password managers. We found that there are significant relationships regarding those with password manager experience with perceived trust, necessity and acceptance, ease of use, cost, risks, and reported features. This can further inform how password manager advice can be improved by focusing on these perceived factors in order to correct people's misconceptions about password managers.

- Lastly, I provide a participatory workshop session as a method in creating interactive stories in the context of teaching security lessons. These sessions can be fully adopted by others to educate users on other security and privacy lessons such as using two-factor authentication, cyberbullying, and surveillance. The workshop sessions may also bring up conversations surrounding the security or privacy topic, which can further improve peoples knowledge of that particular topic.

CHAPTER II

Related Work

I discuss related work on security advice and how security practices are adopted to understand what factors influence users to act digitally secure. I also present related work on security education, interactive stories, and learning science to understand ways they are used in security educational and how they are effective in changing behaviors.

2.1 Security Advice

There are many factors that influence users' acceptance and rejection of security advice which leads to differences in security knowledge, mental models, and online behaviors [5, 6]. Herley proposed that the rational choice of rejecting security advice is situated where the costs to adopt a security behavior is greater than the potential benefit that users can gain [8]. Arguably so, humans, or users, are the weakest link connecting the security of systems [9]. Intrinsically, security experts remedy the human link issue with security education [8, 10, 11]. In fact, the US-Cyber Emergency Response Team (US-CERT) has a page detailing security advice that ranges from mobile device security to network defense. This page contains 72 links with 1,000 words on each page of a link [12]. Further, it has been shown that there is a discrepancy between security behavior of experts and non-expert's, which affects

the prioritization of which security advice people should, or can, follow [13]. Indeed, security experts constantly disagree between what the best security advice people should implement. Some experts believe core education is needed, while others believe that users will always choose the unsafe route in making security decisions [11]. It is difficult to rely solely on advice sources to influence behavior change as users will rationalize their decisions that will benefit them, which may not often be the best case [8].

2.1.1 Security Advice Knowledge

Wash's work in conceptualizing security threats show that regular computer users decide which security advice to implement into their lives based on practicality. As a result, if users don't fully understand the threats of a security risk, they would choose to ignore the advice that they believe would not help them. This fact calls for more structured security education interventions where efforts should not only focus on the recommendations of security advice, but also, at informing users why certain security advice or decisions are necessary [14].

Redmiles et al. conducted a large-scale empirical analysis of security advice to investigate users' security knowledge, behaviors, and beliefs. Users accept security advice based on the trustworthiness of the advice source while rejecting the ones that seem too complex. There is also a gap in security behaviors based on users' socioeconomic background, where they may not receive quality advice and tend to practice fewer security practices [6]. In fact, less than 25% of security advice are readable at the standard level which decreases the accessibility of users with lower technical background or education [15]. The current climate of security advice is hindered by the lack of consensus, comprehensibility, and and efficacy of security advice. Therefore, it is important to find ways to effectively deliver security advice to improve security behaviors across populations.

2.2 Mental Models of Security Behaviors

There has been numerous research around identifying, understanding, and influencing mental models of security behaviors. It is important to understand people's mental models of the Internet in order help experts make decisions in supporting people's expectations and understanding of how systems work. This can help inform education, policies, and even interface design [16, 17]. Several studies have looked at people's mental models of the Internet and security in general. Firstly, Wash illustrated folk models centered around security threats of home computers while Kang et al. studied users' mental models of the internet. Mental models of the internet differ across educational backgrounds and personal experiences, which reveals differences in perceptions of security threat and risks [14, 18, 19]. Kang et al. concluded that, despite the differences in mental models of the Internet, there is no direct relationship between technical backgrounds and protective actions. However, there is a difference between *awareness* and protective actions.

2.2.1 Factors Influencing Mental Models

Wash et al. discovered demographic differences in security beliefs and behaviors. For example, while older people and people with higher education often practice protective actions, they believe they are rarely a target of security attacks. Younger and less educated people, however, are less likely to implement protective actions regarding viruses and hackers because they feel as if there is nothing they can do to protect themselves. Vaniea et al. found that the lack of awareness and understanding prevented some users from updating computers to patch security issues [20]. It also has been shown that even visual cues and contextual information inform our mental models. Friedman et al. presented how people's understanding of web security is influenced by the lock icon [17]. These different mental models regarding security creates a division of vulnerability, and therefore, make security education and com-

munication challenging [14]. While it may not be as important for users to understand the technical intricacies of how the Internet works, it is imperative for users have a basic understanding of the potential Internet problems in order for them to identify consequences of their security decisions [18].

2.3 Influences of Security Behaviors

While learning about security advice and mental models of security behaviors are important, reviewing factors that influence security behaviors carry the foundation for this thesis. Multiple studies have focused on how users are influenced in adopting a security behavior. Rader et al. demonstrated that learning security behaviors rely heavily on informal learning through experiences, stories, and advice sources because there are no formal ways to learn these best practices [4, 21]. Rader et al. and Zou et al. demonstrated how people become cognizant of security-related incidents based on stories and advice told by family and friends. In addition, these stories serve as a catalyst to behavior change. These narratives informally teach lessons within close connections [4, 22]. This is important because the fluid way this type of information travels helps us find ways to better communicate lessons to help people make better security decisions [4]. Similarly, Das et al. found that observability and social sensitivity of other's security experiences is a compelling trigger to influence behavior modifications [23, 24]. The observability of other's experiences not only encouraged better security behaviors, but also discouraged unsafe ones. For example, people would be more inclined to use a passcode on their mobile device after seeing other people implement this practice. Similarly, users will be reluctant to reuse the same passwords if they've heard negative experiences regarding people's accounts being hacked [23]. Overall, learning security behaviors rely heavily on the people around us.

2.3.1 The Role of Experiences in Security Education

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 if it was an important update on computer patches for security. Experience remains as an effective method in teaching lessons. In the security space, users rely on others to "indirectly learn what can't be directly experienced" [21]. The problem emerges at this lack of experience to effectively gauge the severity of security risks and consequences. This form of learning becomes difficult as any sort of feedback is often absent in security-related experiences. We learn best if we are able to make a decision and observe or experience the consequences of that decision. Rader demonstrated that users who learned about threats through past experiences were more motivated to secure themselves compared to those who never experienced a security-related threat [4, 21]. Security measures should not emerge only when something goes awry [25]. Prior work has laid foundations in understanding how users learn and make decisions regarding their security behaviors online. However, motivating users 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?

2.4 Security Education

Researchers have laid groundwork in security education to motivate users to take up best security practices to protect themselves online. In this thesis, I look specifically at targeted educational interventions about security education. Methods such as games, cartoons, comic books, infographics, and a tabletop card game all have been created to educate users regarding their online behaviors [26–32].

Games. There are multiple gameful design interactions regarding cybersecurity. First, there has been many interventions in teaching others how to avoid phishing attacks. Kumaraguru et al. developed an email-based anti-phising education system that teaches users how to correctly identify false URLs. This study showed that security notices weren't as effective as compared to embedded training on how to avoid phishing attacks. Additionally, this study looked at learning science literature to inform the educational game design [27]. Similarly, Asanka et al. looked at key elements in a game design framework to help users avoid security mishaps through motivation. They found that perceived threat, safeguard effectiveness, safe guard cost, self-efficacy, perceived threat, and perceived susceptibility elements should be added in a game framework to avoid phishing attacks. [26]. Often times, security education approaches focus on theories and concepts. However, interactive pedagogical strategies can be more effective in influencing security behaviors. Ryoo et al. proposed a security educational environment for security education. In the study, they created a 3D virtual world simulator that replicated network attacks [33]. Similarly, Google released a web platform called "Be Internet Awesome" that educates and helps kids navigate online through a series of mini games that teaches about scams, passwords, cyberbullying, and good internet behaviors [34]. On the other hand, there are physical games that teaches about cybersecurity. Denning et al. created a tabletop card game centered around cybersecurity that is meant to be used inside classrooms [32]. Overall, games and media prove to be an effective medium in raising awarness about security issues as well as influencing safer behaviors.

Comics and Cartoons. A more static approach in security education involves comics and cartoons. Zhang-Kennedy et al. applied persuasion through instructional design principles to increase the comprehension and awareness regarding security behaviors. The results showed that the visual and interactive components of the comics aided with the comprehension and understanding of the security topics, which is of-

ten seen as traditionally boring and dry for some people. Even in other disciplines, comic books are effective because the graphical nature increases comprehension and memorization [35]. Srikwan and Jakobsson designed cartoons to improve the understanding of security risks with the goal of producing long-term effects of the lessons, which was fairly effective. More importantly, by designing comics or cartoons, the advice may reach a wider audience and readership [29]. This shows that there is potential in applying comics in security education in order to teach users about security behaviors.

Stories. Stories are a unique way of educating others about security lessons. Several studies have shown this to be effective, especially stories about negative experiences [4, 5, 18, 22, 23, 36]. As shown by Redmiles et al., negative events portrayed in fictional narratives were effective in teaching about security behaviors. Similarly, the work on social influence from Das et al. showed that negative experiences were a common catalyst for conversations about security conversations [23]. Fennell and Wash conducted a study looking at the emotional impact of stories with regards to password behavior. They found that participants who reported general feelings of nervousness or frustration end up changing password behaviors as a result [36]. This is also supported by the work from Vaniea et al., where they found that negative experiences affect people's motivations at installing Windows updates [20]. This is useful because it informs us that the framing of stories to teach security lessons is important and effective. Redmiles et al. deployed an entertainment education video (e.g. edutainment) to observe how this form of security advice delivery may be effective in changing software updating behavior [37]. Prior work in health education suggests that this type of narrative is effective for behavior change. For example, some studies looked at how *edutainment* videos were successful in reducing drunk driving and the use of condoms [38, 39]. Finally, Rader et al. conducted a study looking at non-expert's sources of information regarding security decisions. They found that these

information is often communicated through stories, where the stories often influence non-expert's security behaviors and decisions [4]. Stories are effective because they evoke emotion and sociability, which makes lessons easily remembered [40]. Overall, stories prove the effective ways of communicating security risks. However, how do we expand this to security education in a formal way?

2.5 Password Managers

This thesis is a case study for increasing awareness and adoption of password managers through security education. Why password managers? A study from Ion et al. looked at comparing expert and non-expert security practices. In that study, only 10% of non-experts used a password manager compared to the 45% of experts who do. In addition, non-experts reported writing and reusing passwords, three times more than non-experts [13]. The low adoption of password managers is also supported by Humphries's work looking at workplace password behaviors [41]. Generally, there are low adoption rates of password managers among non-experts. Thus, this thesis builds upon previous work around the low adoption rates of password managers, and find ways to fill this gap through security education. It is important to understand why people reject to use a password manager. There has been previous work looking at this issue.

2.5.1 Usability of Password Managers

Several users brought up the issue with technical knowledge and usability issues of password managers [42–44]. A study from Chiasson et al. showed that non-experts' incomplete mental models regarding password managers influenced their misunderstanding of password manager mechanisms. For example, participants reported that completing a task, such as generating a stronger password, was easy. However, they actually failed to complete the appropriate protection mechanism, in which their new

passwords were not actually strong nor secure. In addition, findings from Karole et al. show that the participant's lack of understanding of password managers influenced their distrust with the tool. The issue with awareness is common among other studies, and shows the importance of education and interventions about security tools [42, 45]. This is also supported by research regarding mental models and making rational decisions, in which the incomplete mental models or the cost-benefit outcome surrounding passwords and password managers may hinder overall appropriate behavior change [8, 14, 18, 19].

2.5.2 Factors Influencing the Adoption of Password Managers

Aurigemma et al. examined the poor adoption rates of password managers, despite high intentions reported by users. They found that the issues were related to trust, cost, and threat apathy. Additionally, those who reported high intentions to use a password manager did not adopt one due to the lack of immediacy and time [45]. This study is important because investigating the high intentions but low adoption rate of password managers may help find the underlying theoretical and practical understanding of the poor adoption rates.

Why does a security tool proven to be useful still lack high adoption rates [45, 46]? Many researchers are turning to behavioral change theories to investigate this issue closely [47]. Using self-determination theory to encourage password manager adoption maybe useful. In other words, looking at users' autonomy, relatedness, and competence may be factors to influence adoption. Alkadi and Renaud conducted an experiment investigating this and found that if all self-determination factors were satisfied, then adoption was high. The existing research discussed previously show us that 1) mental models, 2) experience, 3) security sensitivity, and 4) awareness are contributing factors in adoption of security tools. In this thesis, we explore ways we can educate users regarding password managers to increase awareness, correct mental

models, and simulate experiences through the use of interactive stories.

2.6 Learning Science

In this section, I provide an overview of the motivation of using interactive stories to simulate security consequences to change behaviors. Additionally, I list out the use of instructional design principles from the learning science field to look at how this can inform the design of the interactive story. Learning sciences theory suggests that games that are goal-oriented, challenging, contextual, and interactive are effective for teaching [48]. This work shifts the focus on goal-orientation and interaction, which are just as effective in the context of stories.

2.6.1 Interactive Story

An interactive story, or known as Choose-Your-Own-Adventure story, is a genre that positions the reader as a director in which they may influence the nonlinear narrative. Prior work has shown the efficacy in changing behaviors such as improving asthma control among children or improving patients' confidence in managing their hospital stay [49, 50]. In video games or comics, users have no control over the actions of the characters and may not always agree with the decisions the protagonists make. While this may be effective in changing some behaviors, it does not fully capture what it means to experience a security threat. 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 [22]. Interactive stories around security contextualizes the learning experience as it simulates what it may feel to experience a security threat based on the users' decisions. These types of narratives evoke psychological responses not typically found in traditional methods [7]. This puts the reader as a main character with a responsibility to take action. While these stories and other mediums can have a positive change in people's behavior and awareness

of a security issue, how likely will they remain aware of their online behaviors in the future? As shown by Zou et al., awareness is often not enough to trigger a change in behavior [22]. To date, interactive stories specifically has not been explored in the context of simulating security experiences.

2.6.2 Instructional Design Principles

Research has looked at the use of instructional design principles to inform the design and development of educational materials. Previous studies have shown that interactive environments are effective training methods and motivational tools [51, 52]. The goal of this thesis is to use interactive stories in order for people to learn about password mangers, its consequences, and hopefully encourage them to adopt using one. Thus, I implement these design principles in order to create an effective interactive story to be used for security education.

Immediate feedback principle. Providing immediate feedback is effective in learning, especially during knowledge acquisition to correct behavior [53]. Research has shown that immediate feedback in classrooms and training programs were effective in learning new skills, behaviors, and even judgement accuracy [54, 55]. The design of the interactive story takes this principle into use through experiences and consequences. People who read the interactive story will receive immediate feedback regarding their choices that impact the ending of the story. Based on the type of ending they choose, all readers will receive a lesson regarding password managers. This will allow them to understand their choices of security decisions and even correct any misconceptions about password managers.

Multimedia principle. The multimedia principle states that adding graphics improves learning overall [56]. The interactive story uses a combination of text and graphics to convey security lessons about password managers. Levering multimedia will make the story a more enjoyable read and encourages interactivity with the

readers.

Conceptual-procedural principle. Numerous research has been done looking at the effectiveness of games for teaching conceptual and procedural knowledge [51]. A concept is a representation of objects, ideas, and relationships as propositions (i.e. hacking) [51, 57]. A procedure, on the other hand, are steps in order to achieve a task or goal (i.e. changing your password) [57, 58]. This principle emphasizes using conceptual and procedural knowledge in an iterative process to increase learning [59]. We use this principle in the interactive story showing the concept of password managers and eventually detailing the steps on how to install and use one. This may be effective in raising awareness as well as demystifying the notion that password managers take technical expertise to use and install.

Contiguity principle. The contiguity principle states that the use of written instruction, or narrative, is most effective when used with pictures contiguously rather than in isolation [60]. The interactive story naturally has both images and text concurrently.

Segmentation principle. Segmentation principle states that learning through multimedia is more effective when it is presented in *segments*, or rather, when the content is broken into smaller chunks [61]. The interactive story uses this principle by going through the password manager setup, showing the process in each step, per scene, per illustration, at the convenience of the user's pace. Deeper learning can occur and in turn, allow readers to fully absorb the content of the story.

Personalization principle. Research has shown that by using a more conversational tone increases learning and retaining information. An example of this is guiding people through instructional material using "I", "we," "you," and "your" and making them feel involved in the conversation. [62, 63]. The interactive story naturally involves the reader, but also uses common and conversational language to tell the story.

Reflection principle. Reflecting on the lessons learned after the intervention is effective in retaining information, and even behavior change [64]. After interacting with the story, the readers will receive a quick debrief about password managers, lessons learned, and even ways to get started in installing one.

Story-based agent environment principle. Finally, the story-based agent principle looks at using characters to help guide readers through instructional materials. Having characters represented as guides, either visually or verbally, is effective in motivating people to learn [63]. The interactive story design uses supporting characters to guide the reader in installing and providing facts about password managers.

These instructional design principles help guide the design of the interactive story in order to raise awareness, reduce misconceptions, and hopefully encourage the adoption of password managers. While there are many ways to measure learning, this thesis focus on *knowledge acquisition*, or the ability to extract knowledge from instructional materials [65].

CHAPTER III

Participatory Design

3.1 Introduction

It is important to create an effective storyboard for the interactive story in which people can enjoy, relate to, or be convinced by. To do this, I conducted participatory design sessions in designing an interactive story. I present the results in this chapter. The primary objective of the participatory design was to create an effective story that people would find compelling in adopting a password manager. Participants were recruited through two groups: 1) those who have had experiences with password managers and 2) those who don't. I held three workshop sessions, with 3-4 participants in each with a total of 9 participants. In each session, I presented lessons about password managers and had participants express their concerns and opinions about the strengths and weaknesses of password managers, as well as their general experiences with passwords. Participants were put into groups of two and were briefed about interactive stories. Participants were given templates to create their own interactive stories. Each group had the opportunity to share their storyboards with the group. I analyzed each storyboard for common themes, decision options, lessons, and consequences. The storyboards were then combined with the major thematic characters, lessons, and consequences. This formed the basis of the design of the interactive story.

3.2 Participatory Design

Participatory design (PD) is a design approach that involves stakeholders in the design process of a particular product [66]. Prior work has shown the effectiveness of PD in serious games when users were involved as informants that influenced the game levels and challenges [67]. In addition, PD allows better game fit, in which user preferences are considered, which increases game effectiveness. [68]. Hont et al. conducted a study on teens with chronic illnesses and their parents in order to understand the way they articulate symptoms in order to inform the design of symptom-tracking tools in pediatric care [69]. Similarly, there also has been work focused on generating art from crowd-based events and communities [70, 71]. This shows how the use of artistic storyboards or illustration within participatory design can inform designs and artifacts. Carroll et al. used participatory design within community informatics in order to inform decisions and processes within workplace organizations and communities at large [72]. While different methods within participatory designs are used, they bring in new perspectives and keep the users as influencers in the decisions and designs. In this thesis, I use participatory design so that it can inform the interactive story's narrative based on participants' knowledge and background rather than my own security background or biases.

3.3 Methods

I conducted three workshops with 3 participants in each session throughout November 2019. The study was exempted by the University of Michigan Institutional Review Board. Below I discuss the recruitment process, workshop procedure, results of the qualitative analysis, and limitations of this work.

3.3.1 Procedure

Participants were invited in groups at a time, and were separated by those with experience using a password manager from those who don't. This group separation allowed different conversations about password managers to take place by allowing me to have a different conversation based on the groups' experience. For example, I was able to correct any misconceptions surrounding password managers with the group with no experience, while I was able to have a conversation about how and why people started using a password manager with those who have experience. This allowed participants in both groups to approach the storyboard activity in a more effective way. Separating the group also ensured that people created stories from their own experiences and knowledge about password managers, rather than someone else's experiences with password managers.

I presented a short introduction about password managers to help participants understand the context of the security advice. Participants also engaged in a short activity where they were able to share their personal experiences and opinions about what they find annoying regarding passwords. In addition, they were told to express their thoughts regarding the strengths and potential weaknesses of using password managers. Participants wrote these down on post-it notes and shared aloud to everyone, where both the participants and I engaged in discussions. This allowed me to debunk any misconceptions about password managers and emphasize on the benefits and features that participants have brought up.

Next, I briefed participants about interactive stories through examples and a short activity in creating interactive stories. See Appendix A for the Participatory Design Study Materials.

1. Creating characters

2. Choosing your settings

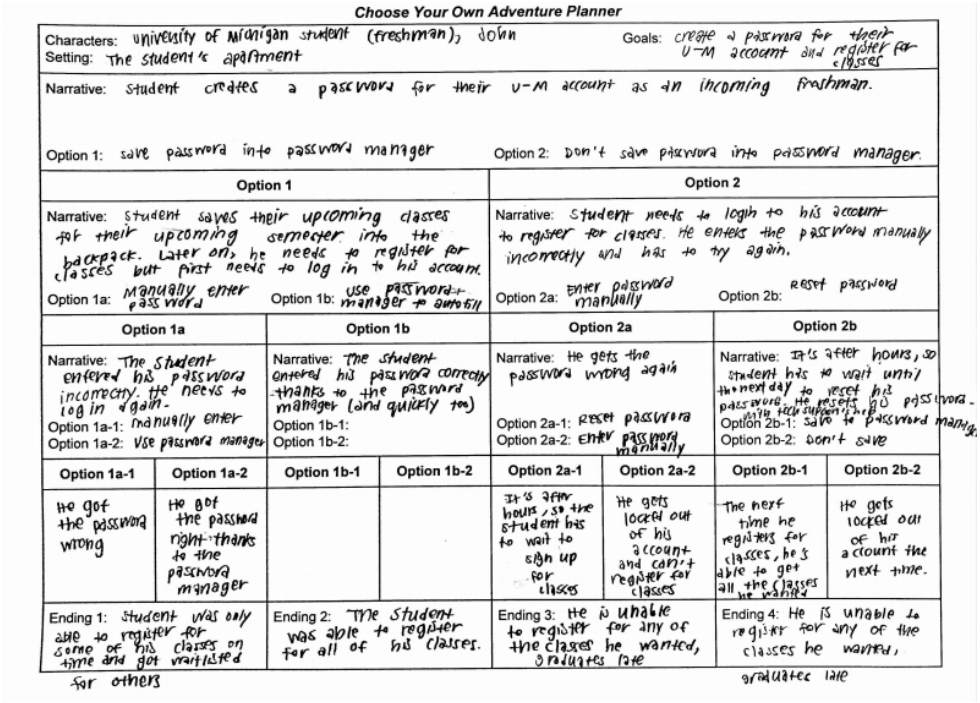
3. Creating character(s) goals

4. Making decisions and consequences of those decisions

5. Climax

6. Endings (plural!)

Participants were then given a template to create their own interactive stories. An example of this storyboard template is shown in Figure 3.1. Participants were also encouraged to draw or use their own methods, however, all participants opted to use the templates provided to them. Each group had an opportunity to present their work to everyone, which was recorded for analysis. The full participatory design workshop is included in Appendix A.



Choose Your Own Adventure Planner

Characters: University of Michigan student (freshman), John
Setting: The student's apartment
Goals: create a password for their U-M account and register for classes

Narrative: Student creates a password for their U-M account as an incoming freshman.

Option 1: save password into password manager
Option 2: Don't save password into password manager

Option 1

Narrative: Student saves their upcoming classes for their upcoming semester into the backpack. Later on, he needs to register for classes but first needs to log in to his account.

Option 1a: Manually enter password
Option 1b: use password manager to autofill

Option 2

Narrative: Student needs to login to his account to register for classes. He enters the password manually incorrectly and has to try again.

Option 2a: Enter password manually
Option 2b: reset password

Option 1a	Option 1b	Option 2a	Option 2b
Narrative: The student entered his password incorrectly, he needs to log in again. Option 1a-1: manually enter Option 1a-2: use password manager	Narrative: The student entered his password correctly thanks to the password manager (and quickly too) Option 1b-1: Option 1b-2:	Narrative: He gets the password wrong again Option 2a-1: Reset password Option 2a-2: Enter password manually	Narrative: It's after hours, so student has to wait until the next day to reset his password. He resets his password with tech support's help Option 2b-1: save to password manager Option 2b-2: don't save

Option 1a-1	Option 1a-2	Option 1b-1	Option 1b-2	Option 2a-1	Option 2a-2	Option 2b-1	Option 2b-2
He got the password wrong	He got the password right thanks to the password manager			It's after hours, so the student has to wait to sign up for classes	He gets locked out of his account and can't register for classes	The next time he registers for classes, he's able to get all the classes he wanted	He gets locked out of his account the next time.
Ending 1: Student was only able to register for some of his classes on time and got waitlisted for others		Ending 2: The student was able to register for all of his classes.		Ending 3: He is unable to register for any of the classes he wanted, graduates late		Ending 4: He is unable to register for any of the classes he wanted, graduates late	

Figure 3.1: Example of PD storyboard

3.3.2 Recruitment

I recruited participants interested in participating in a session to create an interactive story for an educational training material to promote safer online security behaviors. Participant recruitment was threefold. First, I sent out a recruitment message through the University of Michigan School of Information email lists. Secondly, I posted on online forums and social media posts such as Twitter, Facebook, Reddit, and Craigslist. Thirdly, I posted flyers around the University of Michigan buildings. Participants went through a screening process to determine if they have experience with using a password manager. Participants that were invited to the sessions were not included in future follow-up research of this study.[1] Participants were compensated $15 for an approximately one-hour workshop session.

3.4 Analysis

The presentation data was analyzed using qualitative content analysis [73]. Since all of the participants chose the interactive story template, I approached the analysis in a single method based on the template. First, all the recordings and post-it notes from the activities were transcribed. Next, each story description, characters, goals, story options, and consequences were coded. Lastly, I mapped out codes through affinity diagramming [74] and identified high-level themes of what participants find would be an effective story line in promoting the adoption of password managers.

3.5 Limitations

This study has several limitations related to the sample size. While recruiting 9 participants were helpful in getting a good set of storyboards, the participants themselves were mostly educated and were in relatively the same age group. As

[1] Evaluation Study in Chapter 4.

shown in Table 3.1, most participants had some sort of college education and were aged 19 to 28. Recruiting a more diverse set of participants, such as older participants, may help introduce some mental models in creating a convincing storyboard to adopt password managers not present in younger, more educated populations.

3.6 Results

In this section, I present the results of the participatory design sessions. First, I discuss the participant's demographics and level of experience with using password managers. An overview of these demographics is shown in Table 3.1. Second, I present the common themes regarding password annoyances that participants discussed during the group activity during the workshop session, as well as their thoughts regarding the benefits and risks of password managers. Third, I discuss the themes of the interactive story elements such as characters, goals, options, and consequences. I summarize the themes into the resulting interactive story that was designed in Chapter 5.

ID	Gender	Age	Educ.	Type of PW Manager Used
P1	M	28	M.S.	Chrome Password Storage
P2	W	21	S.C.	Chrome Password Storage
P3	W	23	B.S.	Chrome Password Storage, Apple Keychain
P4	M	-	B.S.	No experience
P5	M	19	H.S.	Chrome Password Storage, Apple Keychain
P6	M	26	B.S.	Chrome Password Storage, Apple Keychain
P7	W	24	M.S.	No experience
P8	W	-	B.S.	No experience
P9	W	24	M.S.	No experience

Table 3.1: Workshop Session: Participant Demographics

3.6.1 Participants

I recruited 9 participants with a balance between men and women, as well as password manager experiences. The balance of men and women was helpful in order to get both perspectives and mental models regarding password managers. Demographics for the 9 participants are shown in Table 3.1. No participant had experience with a third-party password manager such as 1Password or LastPass, but rather, use existing password managers such as Chrome Password Storage and Apple Keychain. All of the participants have some college education and were relatively young, with 28 years old (P1) being the oldest.

3.6.2 Password Experiences

In this section, I summarize the password experiences that participants expressed during the workshop session. Every participant had the opportunity to discuss opinions, annoyances, and thoughts regarding their password experiences. These results are aligned with previous research work as summarized in Chapter 2: Password Managers. Here, I explain these results and how this can help inform the design of the final interactive story.

Difficulty in remembering and creating passwords A good portion of the participants expressed that their main concern was that they have a difficult time remembering all their passwords. P3 mentioned: *"It's annoying trying to remember a one-off password for an account that I don't use often. I just use the 'forget password' all the time"* P2 mentioned that she always forgets her password on Slack and would use the email link process every time she tries to login. Many of the participants agreed in using the 'forget password' feature often, but felt like they had no other choice if they wanted to have unique passwords across multiple accounts without writing it down.

Additionally, all the participants agreed that having unique passwords across de-

vices is important, however, many sacrifice doing this practice for the sake of remembering. One participant mentioned: *"People say you need different passwords for different accounts, so it's tedious to remember all of them. I forget them (passwords) instantly unless I write it down."* The issue in trying to create unique passwords across multiple accounts creates a difficult situation for people, so they end up using the same passwords for most of their accounts. The issue with password creation and memorability lies in human memory which shows that it may be useful to rely on software to manage our passwords [75].

Florencio and Herley stated that an average person may have at least 25 accounts [76]. Nowadays, this may be much more. Indeed, the expectation to remember and create 25 or more unique passwords is demanding. A study conducted by Ur et al. also showed that participants may not be creating the most secure passwords in the first place [77]. Additionally, Wei et al. showed that people's passwords often were related to the type of service or website. For example, creating an account on a music site will often have passwords related to music [78]. We then cannot expect users to generate strong, unique passwords all the time.

As seen throughout the participatory design sessions, many participants used this frustration as the beginning point of their storyboards, in which their characters face the same dilemma before adopting a password manager. Thus, this design element help inform the final design of the interactive story.

Adhering to website password requirements Participants expressed concern regarding unique passwords, but especially around trying to adhere to different website's password requirements. Websites have different password requirements which can include adding capitalization, numbers, and special characters. Many participants expressed the frustration because sometimes they would need to include a special character or a number to a common password they use, in which they would end up forgetting. Previous research looked at the policies regarding enforced requirements

for creating passwords [79]. In fact, some studies have shown that password policies may not be as effective in increasing password security [80, 81]. Indeed, frustration and forgetfulness will occur if you break people's password practices to include a special character or to meet a specific length [78, 81]. While this finding isn't present in many storyboards, the frustration of creating unique passwords is similar. Thus, noting this frustration will be helpful in the design of the interactive story.

3.6.3 Benefits of Password Managers

In this section, I list out what participants had in mind about the benefits of password managers. Those without password manager experience speculated what they think the strengths of password managers are after my short presentation about password managers. These results will inform the interactive story in emphasizing the features of password managers to encourage others to try using a password manager.

Convenience using the auto-filling feature Most of the participants expressed the benefit of using the auto-filling feature of password managers. The auto-filling feature allows you to have the password manager auto-populate in the necessary fields, such as your username or email, and password in a click of button. Most participants loved this feature due to faster logins where it streamlines the login experience and eliminates the need to type long passwords. This convenience factor is supported by other research regarding adoption of password managers [42, 82, 83]. In fact, most of the participants included the auto-filling feature on their storyboards. Therefore, it is useful in emphasizing this feature in the interactive story.

Eliminating the need to remember passwords Participants eagerly expressed the convenience of eliminating the need to remember passwords shortly after discussing how difficult it is to remember multiple passwords. It was evident during the workshop session that expressing this concern and realizing that this can be solved

using a password manager illuminated the benefit of trying a password manager, especially for those who never used one. As previously stated from the research that Florencio and Herley conducted [76], most users have 25 or more accounts. By utilizing password managers, users are liberated from the hassle of remembering multiple, unique passwords.

Password Generation Most were surprised by the feature of password generation. None of the participants used a third-party password manager application, and mostly utilized Chrome Password Storage or Apple Keychain as a password storage, where they save their existing passwords. Only two participants said they used the password generator on Apple Keychain. While Chrome Password Storage also allows you to generate passwords, none of the participants in this study used this feature [84]. This shows that even users who use a password manager, do not fully understand it's features. [44]. However, once informed about the feature of password generation, participants said their passwords would be more secure since a password manager would allow them to create unique, complex passwords.

3.6.4 Risks of Password Managers

In this section, I list out the common risks that participants brought up regarding password managers. Those with and without password manager experience both had similar concerns with using password managers. This shows that even users who already use password managers still lack the understanding surrounding password managers. The study from Chiasson et al. showed that participants were not using password managers properly, and still maintained bad practices [44]. This finding is important to emphasize *how* to use a password manager, rather than just *encouraging* others to use a password manager.

Mistrust with Companies The most common concern participants had regarding

password managers is a general mistrust with what companies are doing with their passwords. P5 best illustrates this, *"What are password manager companies doing with my passwords and information? I am mostly concerned with my privacy."* Others had similar concerns regarding where and how their data is being securely stored in the password managers. Many participants also worry about the vulnerabilities that of password managers. P3 said, *"Password manager databases might be huge targets for hackers."* Another participant brought up the issue when password manager companies disappear, *"If a password manager company disappears one day, what is the protocol for users to gain access to their services?"* Additionally, participants are worried about the uncertainty about their passwords. P2 said *"I might feel a lack of control over my accounts if I don't know what my passwords are."* These findings align with previous research regarding password manager adoption, citing that security concerns and mistrust as common behavioral inhibitors of adoption [42, 82, 83].

The discussion surrounding mistrust was alleviated because I gave a short talk regarding the security of password managers and encryption. However, I was not able to address the issue with the feeling of uncertainty around the lack of control when using password managers.

Usability Issues Most of the participants without experience in using password managers brought up the issue with usability. Previous studies looked at the usability of password managers, stating that users don't fully understand how to use password managers [43, 44]. Interestingly, those with password experiences did not bring up usability issues. The issues surrounding usability included incompatibility with operating systems and devices, and the usability of the features such as if the auto-login always works or is usable.

Single Point of Failure Finally, all participants worry about the issue with having a single point of failure. Both participants with experience and those without expe-

rience brought this up. One participant mentioned, *"If someone has my master key, they will have access to all my information"*. Several research regarding password manager adoption cite this as one of the more common beliefs that hinders full adoption of password managers [42, 82, 83]. During the workshop session and discussion, I addressed their concern by speaking about the option of having two-factor authentication, explaining that the only way you can be compromised is if someone had physical access to your device *and* had your master password. I concluded that discussion by explaining how password managers mitigate high risks such as data breaches, while making lower risks worse, where if you do reveal your master password to someone else using your device, then your passwords can be compromised. All participants agree that this is the trade-off using password managers.

3.6.5 Password Manager Awareness and Adoption from Participatory Design

In this section, I describe the results from the post-session survey that participants took after the participatory design session. The post-session survey asked participants about how much the workshop session improved their knowledge of password managers, how likely they would start using a password manager, and when they would start using a password manager.

Most agree that the workshop session increased their understanding of password managers. Majority of the participants (7) felt that they have a stronger understanding of password managers after the participatory design session. No participant indicated “Disagree" or “Strongly disagree." Even those with password manager experiences agree that their knowledge around password manager increased. This shows that the method of using participatory design is useful in engaging and teaching participants, where they are free to discuss their thoughts and issues while collaborating with peers.

Participants were likely to adopt a password manager in the near future

Participants without password manager experience indicated that they will likely adopt a password manager in the near future. The participatory design was an effective catalyst to be informed about the benefits of password managers. However, there is still the gap in streamlining the process and reducing the friction in the adoption of password managers. The term "near future" is vague. As discussed in Fagan et al. and Alkaldi et al., people have low self-efficacy and suffer from the lack of immediacy in adopting a security tool, despite being aware of the convenience and benefits [83, 85]. Future work can possibly look at including a seamless way of introducing security tools in workshop sessions in order to increase the likelihood of adoption. However, this was not the goal of this part of the study.

3.6.6 Interactive Story Elements

In this section, I discuss the major themes of the interactive story elements. I discuss the main character themes, narratives, decisions, and consequences. These themes help shaped the final interactive story. In addition, this may be useful for recreating an interactive story for security education in the future.

Character Themes All storyboards included two characters in some sort of relationship (i.e. husband and wife, or brother and sister). No storyboard included a third character. I suspect that the exclusion of a third character may be limited by the storyboard template, or for the sake of participants in keeping the storyboard simple. Often, the extra character served to be an agent in guiding and convincing the main character to adopt a password manager. As seen in learning science education through the story-based agent environment principle, involving characters to help guide readers through instructional materials help with motivation and knowledge acquisition [60]. In addition, this aligns with Redmiles et al.'s study when they created an edutainment video regarding software updating. In that study, a theme

they found was the use of a "trustworthy, personified security advisor" to deliver the security practice and instructions [37]. While this was not presented to the participants, most used this principle in their storyboards.

Narrative Themes Three storyboards were centered around accessing banks, one about creating an account, one medical, and the rest around the convenience of shopping online. Overall, the major narrative focuses on the goal to *conveniently access accounts*. This theme may reveal the underlying mental model of utilizing password managers for convenience, which is aligned with previous research studies [42, 82, 83], where 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 simplify internet behaviors, rather than approaching a negative or alarming tone surrounding accounts and passwords.

Consequences Themes Contrasting to the narrative theme, most of the consequences focus on *inconvenience*. Many referenced consequences around inconvenience rather than anything drastic like hacking or a data breach. The study on edutainment by Redmiles et al. saw a similar pattern where participants emphasized on realistic examples of negative consequences [37]. By showcasing less drastic consequences, I shift the focus on realistic examples, in which readers may relate to. This may allow them to reflect on their own behaviors and find ways where they can improve this by adopting a password manager [64].

CHAPTER IV

Baseline Knowledge of Password Managers

4.1 Introduction

After the participatory design session, I wanted to investigate people's baseline knowledge of password managers in general. This would help further inform the interactive story to find the gaps or misconceptions of people's knowledge surrounding password managers. The survey of the baseline knowledge looked at different aspects of password manager facts as well as people's expectations of password managers. These factors included 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. In this section, I describe the study design of the baseline knowledge of password manager survey. I list out the the differences of people's knowledge based on their password manager experience and the password manager features most report by participants.

4.2 Methods for Baseline Survey

I deployed a computer-administered, closed-answer survey on Qualtrics to 200 respondents in March 2020 via Prolific [86]. The survey asked about common uses, facts, and misconceptions about password managers to get a baseline of people's knowledge.

See Appendix 2 for the Baseline Knowledge of Password Mangers Study Materials. The study was exempted by the University of Michigan Institutional Review Board. Below I discuss the survey development, recruitment process, results of the baseline survey, and limitations of this work.

4.2.1 Survey Development

Firstly, the survey asked participants if they have used or are using a password manager. If they had experience with password managers, the survey asked about their password manager experience: when they started using one, why they started, and what type of password managers they currently use or have used. Secondly, the survey queries participants' perception of password managers. These perceived questions were phrased as true or false questions and were randomized in the final deployment of the survey. Lastly, the survey asked standardized demographic questions regarding participants' age, gender, education level, and income. Additionally, I ask if they have ever worked in a "high tech" job position to ensure that those responding to the survey was not biased of highly technical participants. After developing the questions, I pilot tested the survey to a research group with five responses in order to improve or modify the survey questionnaire. Some questions were updated and worded better to reduce confusion and redundancy.

4.2.2 Recruitment for Baseline Survey

I recruited 200 participants for the baseline survey on the Prolific online research platform [86], which is an online participant recruitment panel used for surveys. For this study, age (18+) and language (English) were the screening criteria for participants in Prolific. Participants were compensated $2.00 for their time.

4.2.3 Statistical Analysis

I present descriptive statistics regarding participant's demographic information and baseline knowledge of password managers based on perceived factors. I conducted a chi-square test to find any relationship between those with or without password manager experience to the perceived factors. A chi-square compares two variables in a contingency table to see if they are related or differ from one another [87].

4.3 Limitations of Baseline Survey

I achieved a representative sample of participants in gender and education, however these survey results are not meant to be representative of the entire U.S. population. This survey may not report exact measures of people's baseline knowledge of password managers overall, however, this work still provides a strong foundation in gathering a preliminary baseline knowledge of password managers. Indeed, future work can look at getting a wider range of audience to further understand the perceived factors of password managers across the United States. In addition, the results from this survey are self-reported, which may not reflect the true baseline knowledge as some questions may have been interpreted differently and is prone to response bias.

4.4 Results of the Baseline Survey

In this section, I present the results of the baseline knowledge of password manager survey. First, I discuss the participant's demographics. An overview of the demographics compared to the census sample is shown in Table 4.1. Secondly, I present description of password manager experience, that is, when they started using one, why they started, and what type of password managers they currently use or have used. Next, I present statistical significance from the chi-square tests looking at the relationship of those with and without password experiences to the perceived factors.

Lastly, I present the reported features and implications of these results in the final design of the interactive story.

4.4.1 Participants

I collected 200 responds on the baseline survey. The demographics of the participants are shown in Table 4.1. The respondents of the baseline survey is representative of the U.S. Census sample in gender and education, with slight skew to more educated respondents on the survey. 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. The percentages do not add up to 100 because some prefered not to answer this question.

Metric	**Sample**	**Census**
Women, Men, Non-binary	51.0%, 43.5%, 0.4%	51.0%, 49.0%, N/A
Less than high school, High school,	1.5%, 17%	N/A, 28.6%
Some college, Associate	21.5%, 7.5%	19.0%, 5.5%
Bachelor's, Master's	34.5%, 15.5%	20.6%, 8.5%
Doctoral, Professional	0.00%, 2.5%	1.8%, 1.3%
18-24, 25-34 years	30.7%, 37.6%	9.3%, 14.0%
35-44, 45-54 years	19%, 3.4%	12.6%, 12.7%
55+ years	5.4%,	28.9%
< $20k	20%	[10.2%, 19.1%]
$20k - $35k	10.2%	[8.8%, 17.7%]
$35k - $50k,$50k - $75k	13.2%, 20.5%	12.0%, 17.2%
$75k - $100k, > $100k	8.8%, 20.5%	12.5%, 30.4%

Table 4.1: Gender, education, age and income demographics of survey participants compared to the Census. Statistics from [1–3]

4.4.2 What password managers are people using?

A majority of respondents use an existing password managers such as Chrome Password Storage and Apple Keychain rather than third-party password managers such as 1Password or LastPass. This is consistent with participants from the partic-

ipatory design. I suspect that using in-browser password managers is easier to adopt since people are already using the application such as Chrome Web Browser or own an Apple Device. The most common third-party password managers are 1Password, LastPass, and Dashlane, which is consistent with password manager usage statistics [88, 89].

4.4.3 Why did they start using a password manager?

The most frequent reasons of adopting a password manager are ease of use, convenience, and to manage passwords. The reason of adopting password managers related to ease of use and convenience is consistent with previous research studies [42, 82, 83]. Other reasons include the increased security and generation of unique passwords. All of these findings are also consistent with the study conducted in the participatory design, where convenience and password generation were the main benefits of using a password manager. This proves that the factors of convenience, ease of use, and password generation are important aspects people look at when deciding to adopt a password manager.

4.4.4 Significance of Perceived Factors

I measured the baseline knowledge in the following aspects: 1) Perceived Security, 2) Perceived Trust, 3) Perceived Necessity and Acceptance, 4) Perceived Ease of Use, 5) Perceived Cost, 6) Perceived Risks, 7) Features. These factors were summarized from previous password manager adoption studies [42, 45, 82, 83]. These factors help us understand where the knowledge surrounding password manager lies. Overall, there are significant relationships between password manager experience and perceived trust, necessity and acceptance, ease of use, cost, and risks. There was not a significant relationship between perceived security ($p = 0.5$) and reported features ($p = 0.14$).

Perceived Trust. Overall, most participants trust password managers, where 62% of the participants indicated that "I trust password managers to keep my data safe." while only 38% indicated that they trust themselves better in managing their own passwords rather than using a password manager. There is a significant relationship between the password manager experience and perceived trust, where more people without password manager experience do not trust password password managers, ($X^2(1, N = 200) = 53.78$,$\phi = 0.513$, $p < 0.001$). This is consistent with the findings from Chiasson et al. who found that incorrect mental models regarding mental models of password managers can hinder their adoption. Non-users are not willing to hand over their control to a security tool [44]. Lack of trust is also consistent in other password manager studies and the participatory design sessions, where users do not feel comfortable in storing their passwords in one place [42, 45, 83]. An interesting finding is that many participants mentioned how they are not aware about how their passwords are being stored or what the company is doing with their passwords. This opens an opportunity to showcase in the interactive story that trust is an essential component in password manager companies and that their files and passwords are actually encrypted and secured.

Perceived Necessity and Acceptance Interestingly, 51.5% of the respondents prefer to use a password manager over 48.5% of those that indicated they would rather rely on themselves to manage their own passwords. The split between these two indicates that for both users and non-users, there is still a large portion who would prefer to manage their own passwords without a password manager. Indeed, there is a significant relationship between the password manager experience and perceived necessity and acceptance, where more people without password manager experience do not feel that they need a password manager to manage their passwords, ($X^2(1, N = 200) = 54.89$,$\phi = 0.519$, $p < 0.001$). Aurigenna et al. showed that some of their participants indicated that they were satisfied with their current password

management system, whether it's relying on memory or writing it in a physical notebook [45]. Similarly, the usability of certain password managers hinders long-term adoption of password managers, as shown by Seiler-Hwang et al. looking at the usability of password managers [90]. While writing passwords down isn't necessarily the worst password management practice, it is still important to show value in password managers. I did not ask for any follow-ups as to why users of password managers still preferred to manage their passwords without a password manager. Despite this, it would be interesting to show the consequences in the interactive story to see if the perceived necessity and acceptance of using password managers changes.

Perceived Ease of Use Most participants indicated that password managers are easy to use (90%), convenient (91%), and easy to set up (82%). This finding is not consistent with previous usability studies [44, 90]. This may be because password managers have improved the usability of their products over time. Another reason is that many of the participants also indicated that they used browser-based, or built-in password managers, which are traditionally more simple to use. Interestingly, there is a relationship between password manager experience and perceived ease of use, where more people without password manager experience feel that password managers may not be that easy to use, ($X^2(1, N = 200) = 54.45$,$\phi = 0.517$, $p < 0.001$). As seen in previous literature as well as in the participatory design sessions, many users decide to adopt a password manager due to convenience rather than security [42, 83]. For those who indicated that that they do not think password managers are convenient nor easy to use may benefit from receiving the experience of the setup process and the use of a password manager in the interactive story. Therefore, this finding helps inform why the story should involve a character going through the set-up process to emphasize convenience.

Perceived Cost While most participants believe that that password managers are reasonably priced (76.5%), some (23.5%) disagree with this statement. There was

no significance between income and password manager adoption. The average cost of third-party password managers are around $2.99 to $4.99 per month with many of these offering free versions [91–93]. Those who disagree that password managers are reasonably priced may benefit from using free versions. Free versions often come with the basic functionalities such as password generation and auto-fills, which should satisfy the average user. Alkaldi et al. showed that financial cost is not a huge factor considering there are many free versions of password managers that people can use. However, they did not report if participants were aware of this [82]. Cost and prices were never brought up during the participatory design session either because I informed the participants of the free versions beforehand. Therefore, it is important to emphasize that financial costs is no bar to people's adoption.

Perceived Risks More interestingly, most participants, whether users or non-users indicated that password managers are vulnerable to hackers (65%) and that if someone hacks into their password managers, all of their hacks will be exposed (87.5%). In addition, there is a significant relationship between password manager experience and perceived risks, where more people without password manager experience feel that password managers are not not safe, ($X^2(1, N = 200) = 62.20, \phi = 0.552$, $p < 0.001$). Many other researchers have looked at the security of password managers, [94–96], signifying potential vulnerabilities of password managers. However, these studies were conducted about 5 years ago. A recent study by Oesch and Ruoti showed that many of these password managers, especially app-based one like 1Password and LastPass have significantly improved their security [97]. While vulnerabilities still exist, no security tool is fool-proof. An interesting note here is that 87.5% believe that once their password managers have been hacked, their passwords are compromised. This is a common misconception, since password managers encrypt the data inside the vaults. If a hacker opens your password manager vault, your data will by encrypted and safe [42, 97]. This is a great opportunity to emphasize secu-

rity and misconceptions of risks of password managers, so that people can further understand the safety in using one.

4.4.5 Reported Features

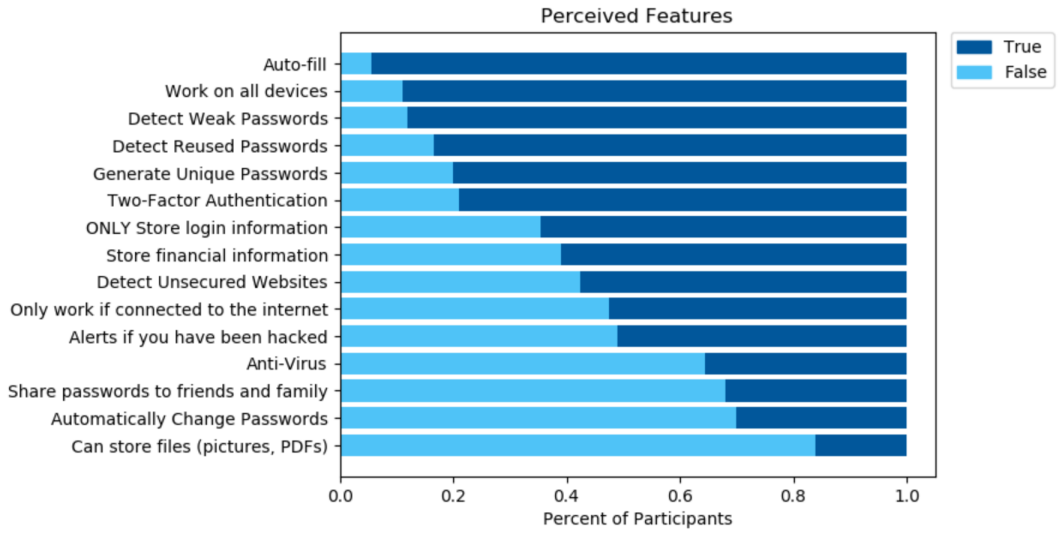


Figure 4.1: Graph of most and least reported features

Most participants reported that auto-fill, device compatibility, and ability to detect weak and reused passwords as the most common features in a password manager. Considering that most participants reported convenience as the main contributor of password manager adoption, it makes sense that auto-fill would be the most reported feature. Surprisingly, device compatibility is the second most common, but previous studies have shown that people are unaware of this feature and has been one inhibitor of full adoption [45, 82]. I suspect that password managers have made it's presence known in multiple devices. In addition, considering that many participants from this survey use Apple Keychain, it's safe to assume that they may use Apple Keychain on Apple laptops, tablets, or phones.

Interestingly, the least reported feature include built-in anti-virus, sharing pass-

words with friends and family, automatically changing passwords, and storing files. The only fake feature on this list is having password managers automatically change your passwords, which most participants reported as a false feature. Recently, many anti-virus software, such as Kaspersky Anti-Virus, are released with built-in password managers [98, 99]. Sharing passwords with friends and family and storing files are real features, sometimes at premium versions, of third-party password mangers. Indeed, most of the respondents use built-in password managers that may not have these additional features. This finding shows that there are some features that participants are not aware of. By educating users about different types of features of password managers, apart from the common ones, may motivate them to start using one. Figure 4.1 shows the detailed graph of reported features.

CHAPTER V

Designing the Interactive Story

5.1 Introduction

The results from the participatory design sessions and baseline knowledge survey help informed the design and development of the interactive story. In this section, I present the result of the final version of the interactive story before evaluation. I use the results of the themes that emerged from the participatory design storyboards (Chapter 3) such as the character themes, narrative themes, and consequences themes. In addition, I combine design session results of password annoyances, perceived risks and benefits with the baseline knowledge survey results (Chapter 4). I identify common misconceptions and reported features in order to emphasize what lessons should be learned. In addition, I conducted a literature review regarding password manager adoption and password manager text advice from media outlets. This helped inform how to structure the story while maintaining comparability with the text advice and interactive story. Based on the literature review, I identify the main inhibitors and barriers in adoption of password managers and the phrasing of password manager advice. These are then combined with the design sessions and baseline knowledge survey results. Finally, I use learning science principles (Chapter 2) to inform the overall structure and methods of designing the interactive story.

5.2 Procedure for Designing the Interactive Story

In this section, I detail the procedure of creating the final interactive story. I combine the results and themes that emerged from:

1. **Participatory design**: Implementing character themes, narrative themes, consequences themes, password annoyances, password risks and benefits. This is the backbone of the interactive story, in which informs the overall *content* of the story.

2. **Baseline Knowledge of Password Managers**: Implementing common misconceptions, perceived factors (trust, cost, etc.), and reported features. This informs which type of knowledge surrounding password managers should be *addressed* in the story.

3. **Common Password Manager Advice**: I examined the way text advice about password managers are framed in media outlets and on the internet in general. Specifically, I look at if the text advice follow a pattern in addressing the issues with passwords and if password managers are recommended in a negative or positive framing. This method is meant to ensure comparability of the text advice with the interactive story. This informs the *flow and framing* of the story.

4. **Instructional Design Principles**: The learning science literature identified many types of principles to make educational material effective. I use these principles to help *ensure effectiveness* in teaching a lesson about password managers, which in turn, to change security behaviors.

5.2.1 Mapping Password Manager Text Advice

I conducted a literature review as well as collected common password manager text advice from the media to ensure comparability with the password manager text advice with the interactive story. In addition, I combine these results with the password experience that participants discussed from the participatory design. The full mapping is shown in Figure 5.1. Based on the literature review, I combine the common reasons of failed adoption of password managers. Next, I combine behavioral inhibitors followed by perception factors of password managers. Each box correspond with one another. For example, the reasons of lack of knowledge is related to insufficient awareness and therefore, perceived necessity and acceptance. The final green box indicates how the interactive story will solve these issues.

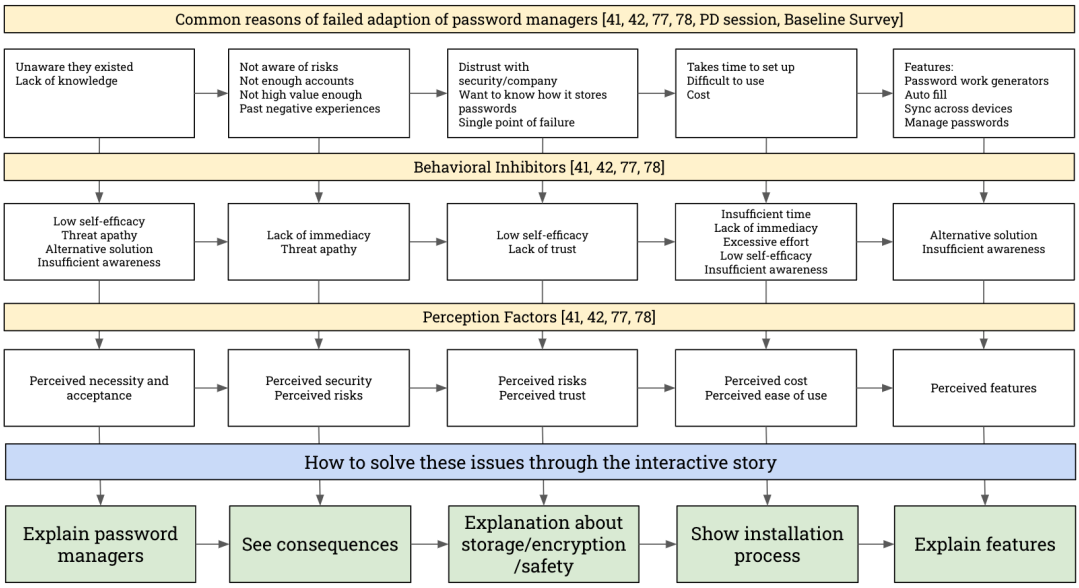


Figure 5.1: Mapping of password manager literature to interactive story flow

Principle	How I implemented this in the interactive story
Immediate feedback	Readers will have the chance to experience their decisions and consequences in the story. In addition, they will receive a lesson regarding password managers so they can understand their security choices.
Multimedia	The interactive story has both illustration and text.
Conceptual-procedural	Readers build their conceptual knowledge of password managers through another character's mental models. Next, building procedural knowledge by showing examples of the password manager features.
Contiguity	The text is placed right below the illustration.
Segmentation	The story is separated by scenes, where the readers will have to click a word or sentence to proceed to the next scene.
Personalization	The story uses conversational language and in a setting that is familiar. The use of characters of female and male characters would appeal for both genders.
Reflection	The ending of the story reflects on the benefits of the password manager and how the main character benefited from it. The reader is then forced to reflect on their choices in the story as well.
Story-based agent	Two supporting characters serve as "security agents" where they guide the main character through the setting up the password manager.

Table 5.1: Summary of Instructional Design applied in the interactive story

5.2.2 Developing the Interactive Story on Twine

I developed the interactive story though Twine, which is an open-source tool for creating and developing interactive stories. Twine is based off of HTML, CSS, and Javascript. I developed the story using Twine's Harlowe version 3.1.0 [100]. The final story was uploaded to Github [1]. Figure 5.2 shows a small section of the interactive story tree decisions.

The final interactive story adopted key elements from the participatory design, namely:

1. **Character Themes**: Most of the storyboards centered around two characters,

[1] https://carlosugatan.github.io/InteractiveStory/MTOP.html

with one serving as the agent to guide the main character. In the final interactive story, there are a total of three characters, one main character and two supporting characters. Depending on which branch the reader goes to, some may not see the third character. Readers will only see two characters at a given time, still sustaining the two-character model.

2. **Narrative Themes**: Most of the storyboards from the participatory design focused on *convenience*, namely convenience accessing accounts. This is consistent with previous findings [42, 83] where most users use a password manager for convenience. The story focuses on convenience such as managing passwords and using the auto-fill feature. However, I also wanted to emphasize the security aspect of it too.

3. **Consequences Themes**: The storyboards that participants created in the participatory design sessions focused on consequences surrounding *inconvenience*. Redmiles et al. showed that the consequences should focus on realistic examples [37]. For the interactive story, the focus looks at financial risk (1st story branch) or a dodged data breach (2nd story branch). The reason I went with more a concrete consequence because the point of the interactive story is to have readers experience the potential harmful consequences, in the hopes they may adopt a password manager.

5.3 Final Design of the Interactive Story

In this section, I discuss the design decisions and rationale of the final interactive story. The story was pilot tested by students from the Security, Privacy, and Interaction (SPI) Lab at the University of Michigan School of Information. The story went through numerous iterations based on the feedback regarding the content of the story, the effectiveness, the illustrations, and the consequences. The story went through two

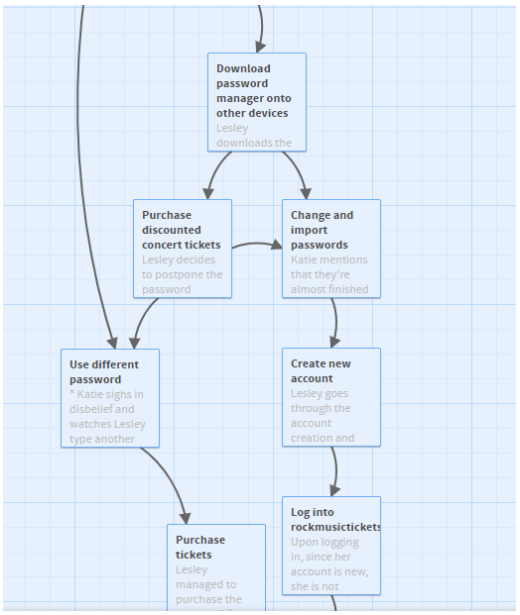


Figure 5.2: Mapping of the interactive story tree decisions on Twine

story and illustration changes. A professional artist was hired to illustrate the scenes. Some examples are seen in Figures 5.3 and 5.4.

5.3.1 Synopsis

Two rock music enthusiasts, Lesley and Katie, try to purchase concert tickets for their favorite band, the Mecha Coyotes. Lesley is clumsy and forgetful to a fault, and forgets her password to purchase tickets on the Rock Music Concert website. Katie suggests Lesley to start using a password manager to manage her seemingly common and related passwords. Katie is enthusiastic about password managers and promotes the convenience and usability, but Lesley remains apathetic. Will Lesley take Katie's advice or will she attempt to enter another password, one that she has used since she was sixteen? What risks will she face and will Katie and Lesley make it to the concert before the tickets are sold out?

5.3.2 Story Details

Characters The story involves three characters overall, however, based on the branch a reader goes to, they may not meet the third character. Readers will only see two characters at a time. Lesley is the main protagonist while Katie serves as the security expert. The third character is Lorenzo, who is Katie's brother. Lorenzo appears only if the reader chooses to not adopt a password manager and Lesley faces that consequence. Lorzeno also serves as an agent in being a security expert, in which he guides Lesley in installing a password manager. Katie has that same role, but the reader will only see those scenes if the reader chooses to use a password manager early in the story. The original story had two married couples but many people expressed that it was not inclusive enough due to the marriage. Instead, the character design changed into a friendship relationship instead. While there are two female protagonists, Lorzeno serves as a male character to balance the characters in the story, which allows the story to appeal for both genders.

Decisions The major decision a reader will make is in the scene where Lesley is given the option to take Katie's advice in using a password manager or have her attempt another login. If the reader chooses to search for a password manager, Katie will help Lesley set up the password manager, as shown in Figure 5.3. However, in that same branch, Lesley will receive a notification about discounted concert tickets. The readers will then be asked to choose whether to continue with the password manager setup or to purchase the discounted tickets. Purchasing the discounted tickets will continue to the final scenes where Lesley does not adopt in using a password manager. If the reader chooses to continue and finish the password manager setup, Lesley will no longer be able to purchase the discounted concert tickets but is still able to make it to the concert with Lesley. These decisions allow the readers to reflect on the decisions while facing trade-offs. The original story looked at purchasing flights to Italy, but the feedback I received mentioned that this may be more exclusionary since

not many people felt that the goal to plan a trip to Italy was very realistic to them. Thus, a more casual event, like a concert, was implemented into the story instead.

Consequences There are two consequences in the story. Both endings show Katie and Lesley enjoy their time at the concert. If the reader decides to have Lesley use a password manager, they would receive the good ending in which Lesley finds out that the Rock Music Concert website she used was hacked but Lesley knew the rest of her accounts weren't harmed because she used a different password on the website. If the reader chose to decline the password manager, they would receive the bad ending where Katie hacks into Lesley's account because Lesley mentioned that the password she used on the Rock Music Concert was the same password she used across Paypal and shopping sites. This ending showed the financial risks that can happen if people reused their password across multiple accounts. If the reader sees this ending, they will still see the password manager setup process because Lesley will contact her brother Lorzeno, who will help guide her throughout the process. These consequences will allow the reader to reflect on their decisions while understanding why these events occurred due to their security choices. The original story emphasized the bad practice of writing passwords down in a notebook and having that notebook stolen that would have caused the main protagonist financial consequences. However, writing passwords down in notebooks is not the worst practice, and many people felt that having an event like that occur seem a little far-fetched. Therefore, I opted to have Lesley's account hacked by highlighting the issue with password reuse, which is a common problem [42].

Password Manager Installation Guidance The greatest benefit in reading the interactive story is experiencing the setup process of a password manager. As seen from previous literature regarding password manager adoption [45, 82], many people feel as if the setup process of password managers are intimidating, long, and difficult. However, this is not the case. Therefore, a major design decision was to

include several scenes and illustrations regarding the installation process of password managers. Specifically, the story goes over 1) what password manager to choose as well as covering the different price models, 2) choosing a master password, 3) installing the password manager application on different devices, 4) and generating new passwords for your accounts. Doing this will allow the reader to be less intimidated in approaching the installation process, and therefore, increase the chances for them to start using a password manager 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 how and why Lesley benefited from 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 such as 1Password, LastPass, and Dashlane. 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.

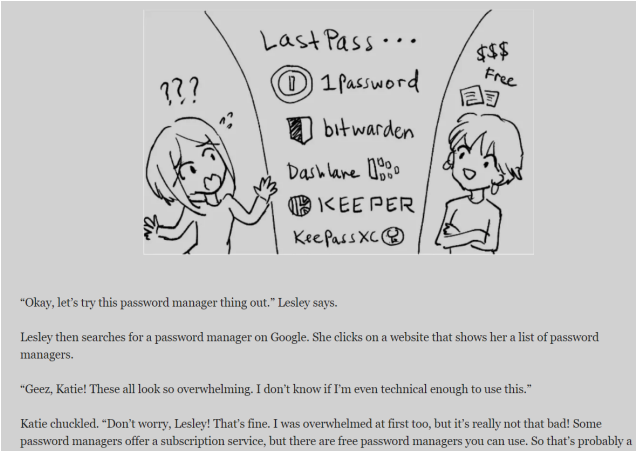


Figure 5.3: Example of one scene from the interactive story

CHAPTER VI

Evaluation of the Interactive Story

6.1 Introduction

In this chapter, I present the results from the online evaluation lab study. Ultimately, the goal was to pre-test the efficacy of the interactive story in increasing awareness and comprehension about password managers. Additionally, it aimed to provide evidence in utilizing interactive stories for security training and educational resources to assess people's understanding of the risks of their security choices, security tools, and to correct perceptions about their security decisions. Participants were invited to a cognitive interview where they were free to express any concerns, improvements, and comments regarding the story's content, lessons, illustrations, and ways to improve. This evaluation method looked at the knowledge acquisition of the convenience aspect, the security aspect, and the features of password managers. Based on the findings, the interactive story proved that comprehension about password managers increased. These findings demonstrate that the story is understandable and effective, which provides a basis to conduct further validation studies in the future such as an experimental study to compare the efficacy of the validated design of the interactive story against other modes of security advice.

6.2 Method for Evaluation Study

I conducted an online cognitive interview in April 2020, where participants were instructed to "think aloud" as they go through each page of the interactive story [101]. The cognitive interviewing technique allowed participants to provide insights regarding their interpretation and comprehension of the interactive story. This was important to evaluate the comparability with traditional security text advice as well as to pre-test the story to ensure lessons are effectively communicated .The study was exempted by the University of Michigan Institutional Review Board. Below I discuss the interview procedure, recruitment process, results, and limitations of this work.

6.2.1 Procedure

Participants first filled out a screening survey regarding basic demographic information. Next, participants were scheduled an online cognitive interview session to evaluate the interactive story. During the cognitive interview, participants were free to express their thoughts and opinions regarding the content, lessons, illustrations, and effectiveness of the interactive story. They were instructed to "think aloud" as they go through each page of the interactive story. The cognitive interviewing technique allows participants to provide insights regarding their interpretation and comprehension of the interactive story [101]. To test if the interactive story was effective, participants were asked questions regarding the lessons and consequences presented in the story. Specifically, they were asked to describe what a password manager is, how auto-filling works, why it it is important to have unique passwords, and the risks of reusing password managers.

6.2.2 Recruitment

I recruited for participants interested in an online session reading an interactive story to evaluate its efficacy in conveying lessons. Participant recruitment was two-

fold: 1) I posted invitations on Facebook, Reddit, and Discord. 2) A recruitment message was sent through the University of Michigan School of Information email lists. Participants were compensated $10 for being a part of the online evaluation study.

6.3 Analysis

The cognitive interview sessions were audio and screen recorded to capture the feedback from participants. A qualitative content analysis of the transcripts of the session was conducted to identify main themes and issues. In this study, I focus on *knowledge acquisition*, which describes the process of how new information is absorbed and stored in memory [102], I tested this by asking participants how well they understood the information they gained from the interactive story. Specifically, I wanted to see if the interactive story was able to convey the convenience aspect, the security aspect, and the password generation and auto-fill features of password managers.

6.4 Limitations

This study has several limitations related to the sample size. While eight participants is a decent number for cognitive interviews [101], I would probably benefit from having a greater sample size to further test the comprehensibility and comparison with the baseline knowledge survey.

6.5 Results of Evaluation Study

In this section, I present the results of the comprehension test from the cognitive interviews. First, I describe the participants' demographic information and password manager experience. Next, I present the results of the comprehensibility test. Lastly,

I present where the interactive story went well and ways it can be improved in future iterations.

6.5.1 Participants

I recruited 8 participants for the online evaluation study. Demographics for the 8 participants are shown in Table 6.1. Only one participant had experience with a third-party password manager, which was LastPass. Other participants use Chrome Password Storage and Apple Keychain. Overall, five (62.5%) participants did not have experience with password managers. Recruiting for participants without password manager experience was imperative in order to fully evaluate if the comprehension from the interactive story was effective. In addition, participants with experience still benefited from reading the interactive story because third-party password managers, such as LastPass, have additional features compared to Chrome Password Storage or Keychain. All but one participants have some college education and the majority were women.

ID	Gender	Age	Educ.	Type of PW Manager Used
P1	M	19	H.S.	No experience
P2	W	40	A.S.	Chrome Password Storage, LastPass
P3	W	23	B.S.	No experience
P4	W	30	M.S.	No experience
P5	W	-	M.S.	No experience
P6	M	25	B.S.	No experience
P7	W	26	M.S.	Chrome Password Storage, Keychain
P8	W	33	M.S.	Chrome Password Storage

Table 6.1: Evaluation Study: Participant Demographics

6.5.2 Comprehension Results

Describing what a password manager is All of the participants were able to articulate what a password manager is, its functionality, and the benefits of using one. More interestingly, all participants followed a pattern in which they described

a password manager. The question was broad in which I asked "In your own words, can you explain what a password manager is?" All participants followed a similar flow similar to how the media gives advice regarding password managers [88, 89]. Namely, they first described the function of master passwords. They then proceeded to highlight password storage and creation. Lastly, they discussed features such as the auto-fill and convenience. The way the participants described password managers may have been partially influenced by the story, since the story followed a similar flow and format. If so, the format of interactive stories may have had an effect on how readers process and understand the information. This shows how the flow of the scenes in an interactive story is just as important as the content.

All participants were confident in stating that password managers would protect them as well as keep their passwords safe. P4 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. P2, who already uses LastPass, said *"I like the guidance and illustrations, because it helps other people understand password mangers. I actually didn't know that my passwords were also encrypted, which is relieving to know!"* while P7 stated *"I don't know much about password managers other than the one I use on Chrome, but the story brought up really good points! I should probably be more careful about how I use mine since I just store the same passwords on the browser."* This shows that the interactive story was effective in increasing their knowledge about password mangers, regardless if they currently do or do not use one. More importantly, the participants brought up their understanding about how password managers encrypt their passwords. Thus, the scene where the characters in the story discuss encryption was effective in conveying this lesson. This is important since previous studies have shown that the lack of knowledge about this encryption lessens the trust that people have around password

managers [14, 45, 82].

Auto-fill Feature All participants knew the surface level of how auto-filling works from previous experience through filling out forms online. P6 mentioned *"If you told me that password managers had an auto-fill feature, that would be the only reason why I would use one."* This quote from P6 illustrates the example of how convenience is still a major factor as to why people would decide to use a password manager, as seen in from the participatory design (Chapter 3) and previous literature [42, 45, 82]. Four of the participants mentioned that they did not know that password managers had an auto-fill feature. This shows that the content emphasizing auto-fill in the story is helpful in raising awareness about the features that users may not be familiar with.

Some participants mentioned that they don't actually know how their passwords are being stored and how the password manager is able to determine which password to use based on the website. P4 mentioned *"I don't actually know how it's being stored in the database. You say it's encrypted but I think it would be nice to see how that works."* A next step in the iteration process of the interactive story can look into explaining the mechanisms of how passwords are stored and how auto-filling works. This can potentially ease some people's uncertainty regarding if auto-filling is a safe feature on password managers.

Unique Passwords and Risks of Reusing Passwords Participants were asked about the password generation feature as well as the risks of reusing passwords. Overall, most of the participants understood the risks of reusing password managers. P6 mentioned *"Basically, if one account is compromised, then potentially all your accounts that have the same password are also compromised"* while P7 said *"By doing that [reusing passwords], you make the hacker's job easy. If one account is hacked, then all your other accounts can be hacked too."* While participants understand the risks of reusing passwords, many also feel guilty for still practicing this behavior. P5

said *"It's actually funny because I still do this! I feel guilty! I should fix my passwords* while P1 says *I have my own pattern but sometimes I still use the same one if I don't care much about the account.* Not surprisingly, this is still a common password behavior [14, 42]. This proves that interactive stories are effective in conveying these risks and having people learn how their own security behaviors.

Misuse of Password Managers For those who have experience with password managers, all the participants do not actually use the full potential of the password managers. When asked about how they use their password managers, all of the participants with experience said that use it solely for password storage. This means that they still reuse the same password across accounts but allow the password manager to save their passwords. I asked about the feature on Chrome Password Storage called "suggested password," which is a password generation feature. The three participants said that they don't use the feature because they fear they won't remember what that password is since it is a jumble of letters and numbers. P2 mentions *"I don't really use the suggested passwords because I wouldn't know what my password manager would be. If I need to enter the password, then I wouldn't know what to do if I don't have my password manager with me."* This shows that even people who currently use a password manager still have incorrect mental models. Thus, the interactive stories still serves a good purpose in educating and correcting mental models regarding password managers.

6.5.3 Content and Design of Interactive Story Results

Password Manager Installation Guidance All of the participants appreciated the password manager installation guidance and felt that it was helpful in understanding the process a bit more. In addition, all the participants felt that it didn't take away from the story and was integrated well. However, some felt that the scenes were text-heavy and felt that it was too long. P4 stated *"I really enjoyed the guidance*

from Lorenzo about how to install a password manager, but maybe you can decrease the text because I ended up focusing on reading the dialogue when the images were more interesting." A future change can look at simplifying the steps by creating a storyboard of the illustration so that readers can visualize the steps in one screen without having to constantly view each step as a separate scene. This can further improve the comprehensability of the password manager installation steps.

Trustworthy Agents I also asked participants about the effectiveness of the support characters in helping the main character install a password manager. 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, which is consistent with previous studies showing how secondary characters can help with explaining security concepts [37]. Interestingly, many participants brought up the conversation surrounding who to trust when given a security advice. At first, Katie, who is Lesley's friend, suggests her to start using a password manager. In addition, Lorenzo, who is Lesley's brother and an IT manager, also suggested the same thing in a different branch. Participants mentioned that while they trust both agents, they were more inclined to trust Lorenzo's advice because of his IT background. This shows that even in stories, the source of advice has a significant influence over the person receiving them. This is consistent with other studies, which shows that people tend to accept security advice from experts [5, 14, 19]. For future iterations of the interactive story, it would be useful to emphasize the agent's expertise and background in order to amplify the advice about adopt a password manager.

Blaming Characters Interestingly, when asked about the scenario that showed how the main character reuses passwords, many participants ended up blaming the main character for the bad practice. P1 says *"Well if only Lesley wasn't so careless with her passwords, then this wouldn't have happened to her"* while P8 argued that

"I don't know if a password manager would have helped Lesley here anyway. She was just careless with her passwords." As discussed earlier, some participants reflected on their own behaviors and felt guilty that they still reuse passwords. However, some participants chose to blame the main character. This scenario was not conveyed well and could use a rework in communicating the poor password behavior better. A potential iteration can look at using statistics to show readers how common certain password behaviors are so that readers can refrain from outright blaming the character and introspectively think about their own password behaviors and see if they should adjust them, allowing them to decide whether or not a password manager is right for them.

The Use of Animations While all participants enjoyed the illustrations, some felt that it was too static with the combination of the dialogue and prose content. P5 said *"I really enjoyed the illustrations, they were helpful. But I think you can probably use animations to make it more lively and easier to follow along. I had to, like, scroll up and down to read the text and look at the images."* P3 said *"I think using animations will help keep my attention a lot longer. It's not like I was bored, but I think using animations can be more effective."* Future iterations of the interactive story can look into embedding the dialogue into the illustration scene as talking bubbles and include small animations to keep the interactive story interesting and alive. This will help with keep the readers' attention, thus, amplifying the effects of the lessons and risks conveyed in the interactive story.

6.6 Outlook: Online Experiment

The results from the online evaluation study showed that the interactive story was successful in increasing the comprehension regarding password managers and security lessons. The goal was to make the interactive study understandable. This evaluation study was a necessary precursor for an online experiment that can be conducted in

the future investigating if it can work better than security text advice or no advice. I outline the experimental design that will be conducted for future work.

The experimental design would look to evaluate the efficacy of an interactive story as compared to regular text security advice. This comparison is important because it will be used to determine if interactive stories can communicate risks, benefits, and uses of password managers compared to how this type of advice is typically given. If this is effective, interactive stories can be used in more interventions to encourage others to use password managers. Overall, the experimental design seeks to answer the following questions:

- R1) How effective are interactive stories in increasing intention and adoption of using password managers compared to traditional text advice?
- R2) Do differences in user characteristics affect the efficacy of interactive stories in being used for security education?
- R3) Can we predict people's intention or adoption of using a password manager based on their current security attitudes and intentions?

Participants will be studied in a between-subjects design and will be randomly assigned to one of two conditions which include 1) interactive story group - participants will be shown the interactive story about password managers, 2) text-advice group - participants will be shown an article about using password managers. To control for confounding effects, the co-variable for previous negative experiences with account compromise will be included.

The experimental design would use existing scales such as:

- Self-Report Measure of End-User Security Attitudes (SA-6) - measures attitudes about adopting security tools
- Security Behavior Intentions Scale (SeBIS), password subscale - measure participants' intentions of particular security behaviors

In addition, I would also include psychometric scales such as:

- Need for Cognition Scale (NFC) [103] - measures how likely an individual is to become involved in a story
- Transportability Scale [104] - measures how much role-taking an individual will partake in based on a mediated character from a story, movie, or game.
- Identification Scale [105] - measures how much role-taking an individual will partake in based on a mediated character from a story, movie, or game.

High scores in these psychometric scales predicts attitude change [103–105]. After 10 days, participants will take a survey about the baseline knowledge of password managers and to provide provide a screenshot of their password manager if they decided to adopt one. This experimental study will solidify the efficacy for using the interactive story for security education, and may be more effective in replace some existing traditional security advice.

CHAPTER VII

Conclusion

7.1 Discussion

In this section, I discuss the overall results from this thesis. First, I discuss the main findings from each chapter that ultimately informed the final design of the interactive story. Next, I discuss the promising approach of interactive stories in being used in security education. Lastly, I discuss implications of practice in utilizing interactive stories.

7.1.0.1 Focus on the convenience aspect of password managers

From the participatory design (Chapter 3), we were informed by users about their negative password experiences. Some of these include the difficulty in remembering and creating passwords as well as adhering to website requirements. When participants were tasked to create a storyboard to encourage others to use password manager, many emphasized on the *convenience aspect* rather than the *security aspect* of using password managers. As supported by the literature, many users indicated that they adopted a password manager due to convenience [42, 83]. By emphasizing the benefit of convenience, users are not suddenly alarmed by the vulnerability of their accounts. In doing so, encourages a smoother transition into password managers rather than being intimidated in getting started. Related to this finding, the participants from

the participatory design session focused on the *inconvenience* consequences if one decides to not use a password manager. This is supported by a previous study from Redmiles et al. emphasizing that realistic examples are more effective than extreme punishments [37]. Future interventions focusing on security practices should look into providing realistic examples that directly benefit people rather than using scare tactics for attitude or behavior change. By providing realistic examples, people can better reflect on their own behaviors and finds ways where they can improve.

7.1.0.2 There are significant differences of the perception and knowledge of password managers from those with experience using password managers compared to those without

As shown in the survey looking at people's general knowledge and misconceptions regarding password managers (Chapter 5), I found significant differences in perception and knowledge of password managers from those with experience using password managers compared to those without. Specifically, we found significant differences between

- Perceived Trust - People without password manager experience do not trust password managers
- Perceived Necessity and Acceptance - People without password manager experience do not think they need to use a password manager
- Perceived Ease of Use - People without password manager experience do not think that password managers are easy to use
- Perceived Cost - People without password manager experience do not think password managers are affordable
- Perceived Risks - People without password manager experience do not think password managers are safe

These differences emphasize the misconceptions and faulty mental models surrounding password managers, which is also supported by previous studies [42, 83]. As a result, these findings informed the final design on the interactive story by using these factors to be addressed in the story, namely, to dispel any misconceptions about password managers. Future security education should look into the general perception or knowledge surrounding a particular tool or practice in order to focus which information should be emphasized and addressed.

7.1.0.3 Interactive stories show promise in being used in security education

Lastly, through an online cognitive interview (Chapter 6), I show that participants were able to comprehend the security risks and consequences of not using a password manager. In addition, participants also saw the potential benefits of using password managers and the features it has that can aid them with their password management practices. However, we also see that people who already use password managers do not use them correctly. Specifically, most still reuse the same password across different websites and only use password managers to store their existing passwords. This shows that there is also potential in interactive stories to *correct* misconceptions and misuse of security tools.

To date, there has not been a published method in creating interactive stories for security education. I took the approach of including users into the design because studies have shown that this is useful in creating effective products or services in the Human-Computer Interaction field [66–68]. By utilizing participatory design, I was able to include users into the design of the interactive story, ultimately creating the core content and narrative of the story. In order to put the interactive story together, I used the Twine tool, which is an open-source platform to create interactive stories [100]. Reflecting on this process, it may require additional work in order to

consistently create security educational materials for interactive stories. I propose that we create a more seamless and effective means in creating interactive stories around security behaviors at scale, in which I discuss in Future Work.

7.2 Implications for Practice

Interactive stories show a promising approach as an educational intervention for security education. Firstly, utilizing interactive stories in education can be effective, especially for children or teenagers. The multimedia aspect of interactive stories can be attractive to this population in conveying security lessons, which is often viewed as boring or intimidating. Depending on the company or organization, this can also be potentially used as a security intervention or training for employees who are not aware about password managers. This work is most effective if an organization is interested in implementing the use of password managers. Indeed, the potential to simulate security consequences in order to convey lessons and risks is large, but helpful to push security education in a positive direction.

7.3 Future Work

The research presented in this thesis suggests a number of future research directions.

7.3.1 Iterations on the current interactive story

Based on the evaluation chapter of this study, the interactive story can go through more iterations to the artwork and content to improve the overall effectiveness. Such iterations include creating a more robust and professional artwork with animations, embedding the dialogue into the artwork, improving the dialogue scenes, and simplifying the installation process scenes.

7.3.2 Utilizing interactive stories for different security or privacy topics

There are opportunities to expand the interactive story in order to be a dependable educational material for security and privacy. Future work can look into using a similar approach of using interactive stories to teach other security or privacy topics such as two-factor authentication or data breaches.

7.3.3 Creating security and privacy interactive story templates

Generally, this thesis provide the process of developing an interactive story using participatory design, learning design principles, conducting a literature review, and using the Twine open-source tool. Another avenue for future work can look at the different venues of heuristics and templates for creating security and privacy focused interactive stories. Creating a tool with specific security consequences and lessons, characters, and artwork can streamline the process in creating interactive stories to be used for security education in the future. In doing so, we are able to effectively simulate security consequences to teach lessons at scale, ultimately improving the nature of security education.

7.4 Summary

Security advice is complex, plentiful, and intimidating to people. I developed and validated a comprehensible and effective interactive story as a method to be used in security education. I did this through a series of user sessions, deploying survey to gather people's general knowledge and misconceptions regarding password managers, conducting a literature review, and using learning science design principles in order to inform the final design of the interactive story.

Taken together, the 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. In doing so, interactive stories have a place in the security education ecosystem in order to educate users on how to behave digitally secure.

APPENDICES

APPENDIX A

Participatory Design Study Materials

Screening Survey Questions

1. What is your email?
    a. Free response

Password managers are tools that assist you in creating and storing passwords across your accounts. Some examples of password managers are 1Password or Chrome Password Storage.

1. Have you ever used a password manager before?
    a. Yes
    b. No
    c. I don't know
2. If you have used a password manager before, which ones have you used?
    a. 1Password
    b. LastPass
    c. Keeper
    d. KeePass
    e. Dashlane
    f. Keychain (on Apple devices)
    g. RoboForm
    h. Firefox Password Manager
    i. Chrome Password Storage
    j. Other: _____

Interactive stories (or Choose-Your-Adventure stories) is a story genre where the reader makes decisions that influences the outcome of a story. Some examples include games such as Telltale's The Walking Dead Series, movies such as Netflix's Black Mirror Bandersnatch episode, or Choose Your Own Adventure stories.

3. Have you engaged with an interactive story before?
    a. Yes [If yes, go to question 4, if no continue to question 5]
    b. No
    c. I don't know
4. Please describe the type of interactive stories you have engaged with and your experiences with them.
    a. Free response
5. What year were you born?
    a. Free text
    b. Prefer not to disclose
6. What is your gender?
    a. Woman
    b. Man
    c. Non-binary
    d. Prefer not to disclose

    e. Prefer to self-describe: _____
7. What is the highest level of school you have completed or the highest degree you have received?
    a. Less than high school degree
    b. High school graduate (high school diploma or equivalent including GED)
    c. Some college but no degree
    d. Associate degree in college (2-year)
    e. Bachelor's degree in college (4-year)
    f. Master's degree
    g. Doctoral degree
    h. Professional degree (JD, MD)
    i. Prefer not to disclose

Participant Presentation Protocol

After each session, participants will be asked to present their storyboard(s).

Questions to ask participants during presentation:

1. Can you briefly walk us through your storyboard?
2. Who are the characters?
3. What are their goals?
4. What decisions will the readers have to make?
5. What are the consequences?
6. What are the different endings?

Appendix 4: Post-Session Survey

1. After this participatory design session, I have a greater understanding of interactive stories
    a. Strongly Agree
    b. Agree
    c. Neither agree nor disagree
    d. Disagree
    e. Strongly disagree
2. After this participatory design session, I have a greater understanding of password managers
    a. Strongly Agree
    b. Agree
    c. Neither agree nor disagree
    d. Disagree
    e. Strongly disagree
3. After creating these storyboards, how likely will you start using a password manager?

    a. Not at all likely
    b. Not very likely
    c. Somewhat likely
    d. Very likely
    e. Extremely likely
    f. I already use a password manager
4. After creating these storyboards, when do you think you will start using a password manager?
    a. Today
    b. Near Future
    c. Never
    d. I already use a password manager
5. What did you like about the workshop session?
    a. Free response
6. What do you think can be improved?
    a. Free response

Participatory Design Session Protocol

Agenda:

I. Introductions and consent form [est. 5 minutes]
II. Goal for this workshop session *[est. 1 minute]*
III. What are interactive stories? *[est. 5 minutes]*
    A. Examples
IV. About password managers *[est. 10 minutes]*
    A. Explanation and Examples
    B. Passwords and Password Manager experiences
    C. What happens/benefits/potential risks of password managers
V. Creating Interactive Stories *[est. 10 minutes]*
    A. Templates
    B. Characters, settings, goals, decisions, climax, endings/consequences
VI. Independent work *[est. 35 minutes]*
VII. Presentations *[est. 10 minutes]*
VIII. Conclusions *[est. 1 minutes]*
IX. Post-Survey *[est. 5 minutes]*

Script:

Introduction

Hello, everyone! Welcome to this design session. In this session, we will create a storyboard about encouraging others to start using a password manager. I just want to point out that you do not need to have previous experience with interactive stories or password managers. I will go over some background materials with you.

This is for my thesis project, in which I will convert your storyboards into online interactive stories to test the effectiveness it has to be used for security training materials through an experimental study design. So again, thank you for your time.

I have a consent form for you here. Please read it over and feel free to ask me any questions before we start.

[Participants read and sign consent form. Answer any questions they have]

[Present participatory design session materials (see Appendix 6)]

1. **Goal**
    a. The goal for today's workshop session is to create a storyboard for a Choose-Your-Own-Adventure story that encourages others to use a password manager. Don't worry! I will go over what a password manager is, and we'll go over how to create a Choose-Your-Own-Adventure story together. There will be templates and materials for you to use.
2. **Background about interactive stories**
    a. So, what are interactive stories? Interactive stories (or Choose-Your-Own-Adventure stories) is a story genre that allows the reader to make decisions in the story that influences the plot or ending. I'll go over some examples with you to help solidify that definition.
    b. One example is an interactive movie.
    c. Anyone familiar with this show? Can you explain what it is?
        i. This one is called Bandersnatch which is an episode from the Black Mirror Series available on Netflix. It gives the viewers the autonomy to shift how the movie will play out based on the decisions they make.
        ii. Here is an example of interactive games. [Show Youtube video: https://youtu.be/CC8TqVEGXsY?t=1516]
    d. This is an example of a minimal graphics but text-based interactive game on iOS. As you can see, you have small snippets of narrative followed by some decisions or actions for you to take.
    e. Another way of viewing Choose-Your-Own-Adventure stories is that it "branches out." Rather than having a linear process, you can imagine it as a stem in which each decision creates a different narrative or outcome.
    f. Here is an example of a text-based browser game that we can both look at together.

    So do you sort of get how interactive stories are? Since we will be creating something similar about password managers, I'll go over what password managers are and the potential benefits and drawbacks of using them.

3. **What are password managers?**

a. Password managers are tools that assist you in creating unique passwords across your accounts as well as storing those passwords in one safe location. These are some examples of password managers, such as 1Password, LastPass, and RoboForm.
b. We can visualize password managers as a vault where all your passwords are stored in. You only need one key, one one password to unlock all your passwords.
c. This is what 1Password looks like where you can create your accounts and store your passwords on each of them.
d. Also, one thing we tend to miss is that whenever you browser asks to save that password, it is also a type of password manager. However, the difference is that it doesn't create unique passwords for you, but rather, just stores those passwords.
e. In addition, if you use a Mac, we have a program called Keychain where it usually stores your login information and even wifi passwords. But those can only be accessed if you enter your computer or laptop's password.
f. So, I can show you how password managers work. For example, I can try to log into my Canvas account. So I use 1Password. If I go to the login page, I can see that I would have to enter in my username and my password. But instead, I can go to my 1Password vault, enter my master password, and I would be able to unlock the vault and autofill my account details. I can do this for all logins and I would essentially only need to remember one password.
g. So, before we talk about the pros and cons of password managers, I would like to hear your experiences with passwords in general. Anything negative? Positive? Write them down on sticky notes!
h. Next, I know some of you here have used a password manager before. Can you let us know why you started using password managers? What are your experiences with password managers in general?
i. So with that said, what do you think are the benefits of using password managers? Let's write these down and post them up.
    i. People use password managers for various reasons, but some reasons are for convenience, where people can fill out their password information easily across all of their devices. It helps create strong passwords, so instead of trying to remember unique and complex passwords for many accounts, they only need to remember one master password. And lastly, it keeps your passwords safe. The passwords are encrypted and stored safely in a vault where only you have access to.
j. Next, what are the potential risks of using a password manager?
    i. There are definitely pros and cons in using one, but password managers are better than keeping your password files in an Excel sheet or, reusing the same password across your accounts.
    ii. Without password managers, we tend to re-use passwords or use easy-to-guess passwords, which increases our chances to be hacked

across multiple accounts. If one password is leaked, hacked, or guessed, all accounts with the same password will be affected. However, with password managers, we can create unique passwords for each account, minimizing the risk of other accounts being hacked. Remembering complex and unique passwords for all our accounts is difficult for humans to do so password managers mitigates this risk. Think of password managers as a vault of all your passwords where you need to only remember one password to enter that vault.

iii. However, one trade-off with using password managers is if someone gets a hold of your master password, they would have all your passwords. However, password managers are really great in their security in which your passwords are encrypted into a vault file inside the vault. And that file is only encrypted/decrypted on your devices. So if a password manager company got 100% compromised in a data breach, your master password will never be released to the attacker.
In addition, password managers require two-factor authentication, so the only way an attacker can get a hold of your password is if they also physically have your device.
Without password managers, if an attacker already has your email address password and log in to your email, they can simply reset your passwords with your stolen email.

iv. In short, password managers mitigate some high risks such as data breaches, while making some lower risks worse, where if you DO reveal your master password to someone else using your device, then your password files can be compromised. For most people, this is a positive trade-off as long as you keep your master password to yourself.

4. Okay, so we covered interactive stories and just covered password managers. We can start creating interactive stories! The prompt will be “Password managers saves the day!” So I’m essentially looking to have at least 2 minimum endings, one that covers what happens if you DON’T use a password manager? And one ending covering what happens if you DO use a password manager? And any type of ending you would want to create. Creating interactive stories can be a bit daunting at first so I’ll go step by step and provide examples first before diving in.

5. I’ll go step by step in how to create interactive stories. I’ll go over creating characters, choosing a setting, writing the narrative, making decisions, and creating multiple endings and consequences
    a. I also have templates for you to use. The first one is a chart which looks like this. So on top you have places to write your characters and setting. Here, you would write the narrative of the story. Then you would write the decisions. Based on those decisions, you can continue the narrative. And so on and so on. However,

this can feel restricting and limiting for some people. It had limited decision points and it might not fit your needs.

b. So you are free to get a paper sheet and either illustrate your story or create your own diagram or flowchart using sticky notes. I'll leave it up to you.

6. **Creating Interactive Stories**
    a. So for now, you don't have to do anything. We'll go over this again. Right now, I'll just be showing examples.
    b. So first, we create a character. What I find helpful is creating user scenarios to sort of flesh out the characters. However, this isn't required. Just having a name of a person is enough. Here, we have Fred and Sally.
    c. Next, we choose a setting. This is helpful in visualizing how the story will take place. For this example, everything will take place in Fred's home.
    d. Next is creating character goals. In order for the story to move forward, your character(s) should have a goal they are trying to accompish in the story. In this example, Fred wants to start using online banking. So his goal is to set up his online banking account.
    e. Decisions. This is the fun part. We have to create decisions for our characters but also for our readers. In this example, we have the decision of either writing the password on a sticky note, or download a password manager. Let's say we ended up choosing to download a password manager. It's also helpful to create a sense of urgency to replicate how we may behave in real life. So here, we have start using a password manager or pick up the kids from school.
    f. So this brings us to the climax, or the most exciting part of the story. Usually the decision that would lead up to the ending. Here, Fred decides to pick up the kids and end up forgetting to use the password manager. Fred decides to just write his password on a sticky note instead.
    g. This brings us to the end! Or endings! Plural! And our characters experience the consequences of their actions. Here we have 3 endings, one neutral, one bad, and one good.
    h. So those are very simple examples. You can be as elaborate as you want to be. You can even start the story of having Fred decide what to eat for breakfast. I'll leave that up to you.
    i. So now, it's your turn! We'll share our characters and settings to one another but I'll leave you to creating the narrative, decisions, and endings to yourself. In the end, everyone will have a chance to share their story.
7. **Participatory session starts**
8. **[Participants present storyboard]** 10 minutes
    a. See Appendix 3 for participant presentation protocol
9. **[Conclusion and Post Survey]** 5 Minutes
    a. Thank you for participating! I really appreciate your time and work on this session. Before you leave, please complete this post-session survey. Feel free to reach out to me if you have any questions. Thank you!
    b. See Appendix 4 for Post Session Survey

Workshop Design Session

Let's create an interactive story
about encouraging users to use password managers!

Goal for today

Create a storyboard for an interactive story that encourages others to use a password manager.

What are interactive stories?

An interactive story (or Choose-Your-Adventure story) is a story genre lets the reader make decisions to influence the outcome of the story.

Interactive Movies:

Interactive Games:

Examples:

What are interactive stories?

"Branches out"

Activity

Create a storyboard for an interactive story (Choose-Your-Own-Adventure story) that encourages others to use a password manager.

What are password managers?

Password managers are tools that assist you in creating and storing passwords for your accounts in one location.

onelogin

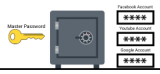
1Password

dashlane

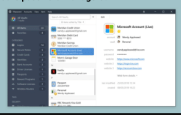
LastPass

RoboForm

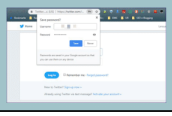
What are password managers?



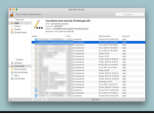
What are password managers?



What are password managers?



What are password managers?



Password Managers: Demo

Passwords: Your Experiences

What are your experiences with passwords in general?

Anything annoying? Negative? Positive?

Let's write these down!

Passwords Managers: Your Experiences

Why did you start using a password manager?

What are your experiences with password managers in general?

What are the benefits of using password managers?

What are the potential risks of using a password manager?

onelogin

1Password

dashlane

LastPass

RoboForm

Activity

Create a storyboard for an interactive story (Choose-Your-Own-Adventure story) that encourages others to use a password manager.

Prompt: Password Managers saves the day!

Two Main Endings

What happens if you DON'T use a password manager?

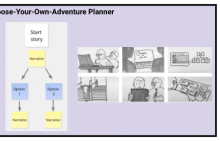
What happens if you DO use a password manager?

Creating an Interactive Story

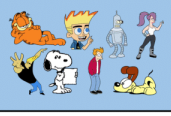
- Character(s)
- Setting(s)
- Goals
- Narrative
- Decisions
- Endings and Consequences
  - What happens if you DON'T use a password manager?
  - What happens if you DO use a password manager?

Choose-Your-Own-Adventure Planner

Choose-Your-Own-Adventure Planner



Step 1: Creating our Characters: User Scenarios



Examples

Fred

Step 2: Choose your setting

Example

Step 3: Character(s)' Goals

Example

Step 4: Decisions

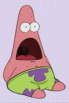
Example:

~~Start using a password sticky manager~~

OR

~~Back up all passwords~~ Back up all passwords in password manager?

Step 5: Climax: Password managers saves the day! (or not)



Example

Forgets about password manager and decides to write password on sticky note instead.

Step 6: Endings (plural!) and Consequences

The Ends

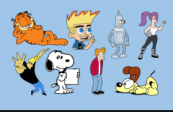
Example

Neutral ending
His daughter comes over and helps Fred set up his password manager

Bad ending
Robber gets into his house, sees sticky of passwords and is able to log into his bank account

Good ending
Fred enjoys the convenience of using a password manager that he ended up burning his sticky note of passwords.

Step 1: Creating our Characters: User Scenarios



Step 2: Choose your setting

Step 3: Character(s)' Goals

Step 4: **Narrative**

Step 5: **Decisions**

Step 6: **Climax**: Password managers saves the day! (or not)

Step 7: **Endings and Consequences**

Presentations: Walk us through your storyboards

1. Who are the characters?
2. What are their goals?
3. What decisions will the readers have to make?
4. What are the consequences?
5. What are the different endings?

Thank you!

APPENDIX B

Baseline Knowledge of Password Managers Study Materials

Baseline About Password Managers Survey

1. Have you ever used a password manager before?
    a. Yes
    b. No [go to matrix]
    c. I don't know
2. When did you start using a password manager?
    a. Free response
3. What password manager(s) have you used?
    a. 1Password
    b. LastPass
    c. Keeper
    d. KeePass
    e. Dashlane
    f. Keychain (on Apple devices)
    g. RoboForm
    h. Firefox Password Manager
    i. Chrome Password Storage
    j. Other: _____
4. Why did you start using a password manager?
    a. Free response

[Matrix]
True/False
Password

Note: You do not need to have password manager experience to take this survey.

Please answer the following questions about password managers the best you can.
You will not be penalized for wrong answers.

<u>Perceived Security</u>

1. It is more secure storing your passwords digitally (i.e. in spreadsheet) than than using a password manager
2. It is more secure to use a password manager than storing your passwords physically (i.e. in notebooks)
3. I would feel more comfortable writing my passwords in a word document than a password manager

<u>Perceived Trust</u>

4. I trust password managers to keep my data safe
5. I trust myself better in managing my passwords rather than using a password manager

<u>Perceived Necessity and Acceptance</u>

6. I prefer to manage my own passwords

7. I prefer to use a password manager to protect my passwords
8. My passwords are safe without a password manager

Perceived Ease of use

9. Password managers are difficult to set up
10. Password managers are easy to use
11. Password managers are convenient
12. I worry that accessing my accounts may be more difficult with a password manager
13. Setting up a password manager would take an excessive effort on my part

Perceived Cost

14. Password managers are expensive
15. The cost to use a password manager is reasonable

Perceived Risks

16. If someone hacks my password manager, all my passwords will be exposed
17. Password managers are vulnerable to hackers

Perceived Features

18. Password managers allow me to auto-fill my login credentials
19. Password managers generate unique passwords for me
20. Password managers automatically change my passwords for me
21. Password managers work across all devices (mobile, laptop, desktop)
22. Password managers can only store login information (username, email, passwords)
23. Password managers allow me to share my passwords to friends and family
24. Password managers allow two-factor authentication
25. Password managers can detect weak passwords
26. Password managers can detect reused passwords
27. Password managers can detect unsecured websites
28. Password managers have an antivirus built in
29. Password managers alert you if you have been hacked
30. Password managers allow you to store files (pictures, PDFs)
31. Password managers allow me to store my financial information (such as credit cards, and bank information)
32. Password managers only work if you are connected to the internet

Demographics Section

1. How old are you?
    a. Free text
    b. Prefer not to disclose
2. What is your gender?
    a. Man
    b. Woman
    c. Non-binary
    d. Prefer to self-describe:_____
    e. Prefer not to answer

3. What is the highest level of education you have completed or the highest degree you have received?
    a. Less than high school
    b. High School Graduate
    c. Some College
    d. Bachelor's Degree
    e. Associate's Degree
    f. Master's Degree
    g. Doctoral Degree
    h. Professional Degree (e.g. M.D., J.D.)
    i. Prefer not to answer
4. What is your annual household income?
    a. Less than $25,000
    b. $25,000 to $34,999
    c. $35,000 to $49,000
    d. $50,000 to $74,000
    e. $75,000 to $99,000
    f. $100,000 to $124,000
    g. $125,000 to $149,000
    h. $150,000 or more
    i. Prefer not to answer
5. Have you ever worked in a "high tech" job such as computer programming, IT, cybersecurity, or computer networking?
    a. Yes
    b. No
    a.

APPENDIX C

Evaluation Study Materials

Screening Survey

1. What is your email?
    a. Free response
2. Have you ever used a password manager before?
    a. Yes
    b. No
    c. I don’t know
3. If you have used a password manager before, which ones have you used?
    a. 1Password
    b. LastPass
    c. Keeper
    d. KeePass
    e. Dashlane
    f. Keychain (on Apple devices)
    g. RoboForm
    h. Firefox Password Manager
    i. Chrome Password Storage
    j. Other: _____
4. What year were you born?
    a. Free text
    b. Prefer not to disclose
5. What is your gender?
    a. Woman
    b. Man
    c. Non-binary
    d. Prefer not to disclose
    e. Prefer to self-describe: _____
6. What is the highest level of school you have completed or the highest degree you have received?
    a. Less than high school degree
    b. High school graduate (high school diploma or equivalent including GED)
    c. Some college but no degree
    d. Associate degree in college (2-year)
    e. Bachelor's degree in college (4-year)
    f. Master's degree
    g. Doctoral degree
    h. Professional degree (JD, MD)
    i. Prefer not to disclose
7. What is your educational background?
    a. List of majors list

Demographic Survey

1. How old are you?
    a. Free text
    b. Prefer not to disclose
2. What is your gender?
    a. Man
    b. Woman
    c. Non-binary
    d. Prefer to self-describe:_____
    e. Prefer not to answer
3. What is the highest level of education you have completed or the highest degree you have received?
    a. Less than high school
    b. High School Graduate
    c. Some College
    d. Bachelor's Degree
    e. Associate's Degree
    f. Master's Degree
    g. Doctoral Degree
    h. Professional Degree (e.g. M.D., J.D.)
    i. Prefer not to answer
4. What is your annual household income?
    a. Less than $25,000
    b. $25,000 to $34,999
    c. $35,000 to $49,000
    d. $50,000 to $74,000
    e. $75,000 to $99,000
    f. $100,000 to $124,000
    g. $125,000 to $149,000
    h. $150,000 or more
    i. Prefer not to answer
5. Have you ever worked in a "high tech" job such as computer programming, IT, cybersecurity, or computer networking?
    a. Yes
    b. No

Cognitive Interview Protocol

Introduction

Hi! Thank you for being here today! Today, I'll be showing you an interactive story or Choose-Your-Own-Adventure story about password managers. I just want to point out that you do not need to have previous experience with interactive stories or password managers.

I will ask you to interact with the story and while you do so tell me what you are thinking, what you're seeing, what decisions you're making and why, and your opinions about the story in general.

I may ask you some questions while you go through the story as well. Afterwards, I'll just have you fill out a few questionnaires.

There are no right or wrong answers, I just want to hear your thoughts and opinions. Keep in mind, this is not about testing you but rather about testing and improving this interactive story so I'd love to hear about any thoughts you have including when you're confused, when something is unclear or when you like something

Lastly, I would like to audio and screen record the session so I don't have to take notes or miss anything. Would that be okay? Okay, great! Please read and sign this consent form...

Do you have any questions after reading the consent form? Alright, if it is ok with you I will now start the recording.

[start screen and audio recording]

Okay, now I will show you the interactive story. Again, please share your thoughts, impressions and decisions. I'm interested in any feedback or suggestions you may have.

[have participant interact with the story]

Questions if participant is not saying much

1. Why would you choose this option?
2. How would you behave in this situation?
3. How does this make you feel?
4. What do you think about the illustration on this page?

[after the participant is finished with the interactive story, **have them take the baseline password manager survey**]

Thank you! Now, I have a few questions that I want to ask you regarding the story.

So the ultimate goal of the interactive story is to see if it effectively communicates the benefits of password managers and the potential risks if you don't use one.
With this said,

1. What did you think went well or could be improved with the scenario highlighting the risk of reusing the same password which caused the main character financial risks?
    a. We communicated it this way, how would you communicate it instead?
2. What do you think went well or could be improved about highlighting the benefits of using a password manager by auto-filling the login fields?
    a. Can you explain to me how the auto-filling works?
    b. We communicated it this way, how would you communicate it instead?
3. What do you think went well or could be improved about highlighting the benefits of using a password manager in creating unique passwords?
    a. Can you explain to me why it's important to create unique passwords?
    b. We communicated it this way, how would you communicate it instead?
4. In your own words, tell me how a password manager works.
    a. What do you think went well or could be improved in the story to better explain how a password manager works?
5. If you were interested in using a password manager, how would you search for one?
    a. What do you think went well or could be improved in the story to better explain how to search or get started in using a password manager?
6. Have you seen any educational materials about security or privacy before?
    a. Can you describe the contents of the material?
    b. Did you follow the advice? Why or why not?
    c. How did this advice help you?
        i. If no:
            1. What sort of educational material would you like to see to understand security and privacy lessons?
7. Anything else you would like to add regarding this interview, the interactive story or anything else?

Thank you! Now, I just have an exit survey for you to take. The survey would ask about different personality questions, so please answer them the best you can.

APPENDIX D

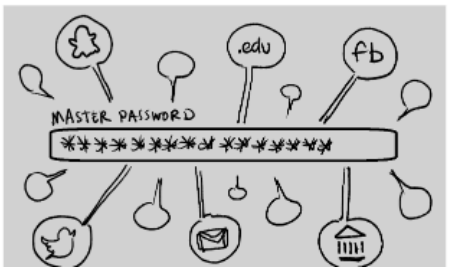
Final Sketches of Interactive Story

Scene 01:
Introduction

Scene 02:
Finish eating pancakes

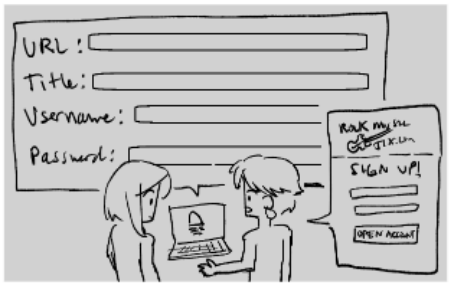
Scene 03:
Log in

Scene 04:
Search for a password manager



Scene 05:
Help Lesley install password manager

Scene 06:
Download password manager to other devices



Scene 07:
Change and import passwords

Scene 08:
Create new account

Scene 09:
Log into rockmusictickets.com

Scene 10:
2 weeks later

Scene 11:
If you used password manager

Scene 12:
Purchase discounted tickets

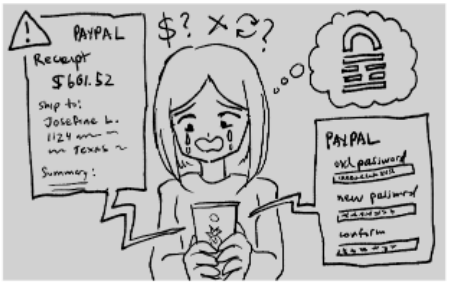
Scene 13:
Use different password

Scene 14:
Purchase tickets 1

Scene 15:
Purchase tickets 2

Scene 16:
A few days after the concert

Scene 17:
Katie attempts to enter same passwor on Paypal



Scene 18:
Katie ordered some clothes

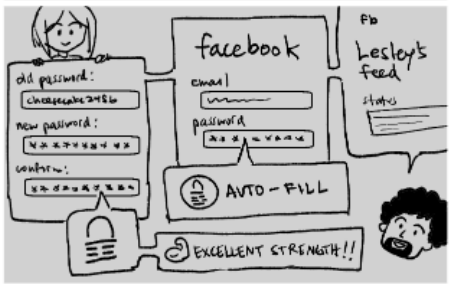
Scene 19:
Lesley regrets not using a password manager

Scene 20:
Lesley calls her brother Lorenzo

Scene 21:
Help Lesley install a password manager 2

Scene 22:
Download password manager to other devices 2

Scene 23:
Change and import passwords 2



Scene 24:
Change Facebook password

Scene 25:
The End

References

[1] U.S. Census Bureau. Annual estimates of the resident population by single year of age and sex for the united states, 2018. https://www.census.gov/data/tables/time-series/demo/popest/2010s-national-detail.htmls, Last accessed on 2020-04-03.

[2] U.S. Census Bureau. Educational attainment of the population 18 years and over, by age, sex, race, and hispanic origin, 2018. https://www.census.gov/data/tables/2018/demo/education-attainment/cps-detailed-tables.html, Last accessed on 2020-04-03.

[3] U.S. Census Bureau. Population by age and sex, 2018. https://www.census.gov/library/publications/2019/demo/p60-266.html, Last accessed on 2020-04-03.

[4] 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.

[5] 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.

[6] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How i learned to be secure: A census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 666–677, New York, NY, USA, 2016. ACM.

[7] Brett Shelton. Designing and creating interactive fiction for learning. 01 2005.

[8] Cormac Herley. no thanks for the externalities: The rational rejection of security advice by users. 01 2009.

[9] Bruce Schneier. Digital security in a networked world, 2000.

[10] Ross J. Anderson. Why cryptosystems fail. *Commun. ACM*, 37(11):32–40, November 1994.

[11] Lorrie Faith Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UPSEC'08, USA, 2008. USENIX Association.

[12] US-Cyber Emergency Response Team. Cybersecurity tips, 2020. `https://www.us-cert.gov/ncas/tips`, Last accessed on 2020-03-28.

[13] 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, Ottawa, July 2015. USENIX Association.

[14] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 11:1–11:16, New York, NY, USA, 2010. ACM.

[15] Elissa Redmiles, Miraida Morales, Lisa Maszkiewicz, Rock Stevens, Liu Everest, Dhruv Kuchalt, and Michelle Mazurek. First steps toward measuring the readability of security advice. 2017.

[16] Soumya Sen, Carlee Joe-Wong, Sangtae Ha, and Mung Chiang. A survey of smart data pricing: Past proposals, current plans, and future trends, 2012.

[17] Batya Friedman, Helen Nissenbaum, David Hurley, Daniel C. Howe, and Edward Felten. Users' conceptions of risks and harms on the web: A comparative study. December 2002.

[18] 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.

[19] Rick Wash and Emilee Rader. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 309–325, Ottawa, July 2015. USENIX Association.

[20] 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.

[21] Emilee Rader and Rick Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 12 2015.

[22] 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.

[23] 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.

[24] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, page 739–749, New York, NY, USA, 2014. Association for Computing Machinery.

[25] Mary Ellen Zurko. User-centered security: stepping up to the grand challenge. volume 2005, pages 14 pp.–, 01 2006.

[26] Nalin Asanka Gamagedara Arachchilage and Steve Love. A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3):706 – 714, 2013.

[27] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching johnny not to fall for phish. *ACM Trans. Internet Technol.*, 10(2):7:1–7:31, June 2010.

[28] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. volume 229, pages 88–99, 01 2007.

[29] Sukamol Srikwan and Markus Jakobsson. Using cartoons to teach internet security. *Cryptologia*, 32(2):137–154, April 2008.

[30] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. Stop clicking on "update later": Persuading users they need up-to-date antivirus protection. In Anna Spagnolli, Luca Chittaro, and Luciano Gamberini, editors, *Persuasive Technology*, pages 302–322, Cham, 2014. Springer International Publishing.

[31] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human–Computer Interaction*, 32(3):215–257, 2016.

[32] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, CCS '13, pages 915–928, New York, NY, USA, 2013. ACM.

[33] Jungwoo Ryoo, Angsana Techatassanasoontorn, Dongwon Lee, and Jeremy Lothian. Game-based infosec education using opensim.

[34] Google. Be internet awesome, 2017. `https://beinternetawesome.withgoogle.com/en_us`, Last accessed on 2019-04-22.

[35] Paul A. Aleixo and Krystina Sumner. Memory for biopsychology material presented in comic book format. *Journal of Graphic Novels and Comics*, 8(1):79–88, 2017.

[36] Rick Wash and Chis Fennell. Emotional impact: How stories affect password behavior. 2018.

[37] Candice Schumann Rock Stevens Peter Sutor Michelle L. Mazurek Elissa M. Redmiles, Angelisa Plane. Can edutainment change software updating behavior?, 2017.

[38] Sandra H. Berry David E. Kanouse Rebecca L. Collins, Marc N. Elliott and Sarah B. Hunter. Entertainment television as a healthy sex educator: The impact of condom-efficacy information in an episode of friends. 2003.

[39] S.T. Murphy M.G. Kennedy and V. Beck. Entertainment education and multicultural audiences: an action and research agenda. 2004.

[40] Kashima Y. Clark A. Peters, K. Talking about others: Emotionality and the dissemination of social information. 2009.

[41] D. Humphries. Best practices for workplace passwords, 2015.

[42] 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.

[43] Ambarish Karole, Nitesh Saxena, and Nicolas Christin. A comparative usability evaluation of traditional password managers. In *Proceedings of the 13th International Conference on Information Security and Cryptology*, ICISC'10, page 233–251, Berlin, Heidelberg, 2010. Springer-Verlag.

[44] Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*, USENIX-SS'06, USA, 2006. USENIX Association.

[45] 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.

[46] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Sven Bugiel, and Michael Backes. Studying the impact of managers on password strength and reuse. *CoRR*, abs/1712.08940, 2017.

[47] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? *CoRR*, abs/1901.02672, 2019.

[48] Clark N. Quinn. *Engaging Learn Design e-Learn Games*. Pfeiffer, 2005.

[49] Tami Wyatt, Xueping Li, Yu Huang, and Rachel Farmer. Developing an interactive story for children with asthma. *Computers, Informatics, Nursing (Accepted)*, 01 2013.

[50] 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.

[51] J. P. Gee. *What Video Games Have to Teach Us About Learning and Literacy.* Palgrave Macmillan, 2003.

[52] Alexander Repenning and Clayton Lewis. Playing a game: The ecology of designing, building and testing games as educational activities. In Piet Kommers and Griff Richards, editors, *Proceedings of EdMedia + Innovate Learning 2005*, pages 4901–4905, Montreal, Canada, June 2005. Association for the Advancement of Computing in Education (AACE).

[53] John Anderson, Albert Corbett, Kenneth Koedinger, and Ray Pelletier. Cognitive tutors: Lessons learned. *Journal of the Learning Sciences*, 4:167–207, 04 1995.

[54] Iris Stuart. The impact of immediate feedback on student performance: An exploratory study in singapore. *Global Perspectives on Accounting Education*, 1, 03 2012.

[55] Albert T. Corbett and John R. Anderson. Locus of feedback control in computer-based tutoring: Impact on learning rate, achievement and attitudes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '01, page 245–252, New York, NY, USA, 2001. Association for Computing Machinery.

[56] R.E. Mayer. Using multimedia for e-learning. *Journal of Computer Assisted Learning*, 33(5):403–423, 2017.

[57] R. C. Clark. *Developing Technical Training: A Structured Approach for the Development of Classroom and Computer-Based Instructional Materials.* Addison Wesley Publishing Company, 1989.

[58] J. R. Anderson. *Rules of the Mind.* Lawrence Erlbaum Associates, Inc., 1993.

[59] Bethany Rittle-Johnson and Kenneth R. Koedinger. Comparing instructional strategies for integrating conceptual and procedural knowledge. 2002.

[60] Richard Mayer and Richard Anderson. The instructive animation: Helping students build connections between words and pictures in multimedia learning. *Journal of Educational Psychology*, 84:444–452, 12 1992.

[61] Richard E. Mayer. *Segmenting Principle.* Cambridge University Press, 2009.

[62] Mayer R. E. Clack, R. C. *E-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning.* John Wiley Sons, Inc., 2002.

[63] R. E. Mayer. *Multimedia Learning.* Cambridge University Press, 2001.

[64] Committee on Developments in the Science of Learning and National Research Council. *How People Learn: Bridging Research and Practice.* National Academies Press, 2000.

[65] H. P. Bahrick. *Maintenance of knowledge: Questions about memory we forgot to ask.* J. Exper. Psych, 1979.

[66] 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.

[67] 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.

[68] Stacey Guy, Alexandria Ratzki-Leewing, and Femida Gwadry-Sridhar. Moving beyond the stigma: Systematic review of video games and their potential to combat obesity. *International journal of hypertension*, 2011:179124, 03 2011.

[69] Matthew Hong, Udaya Lakshmi, Thomas Olson, and Lauren Wilcox. Visual odls: Co-designing patient-generated observations of daily living to support data-driven conversations in pediatric care. pages 1–13, 04 2018.

[70] Jennifer Sheridan, Nick Bryan-Kinns, Stuart Reeves, Joe Marshall, and Giles Lane. Graffito: Crowd-based performative interaction at festivals. pages 1129–1134, 01 2011.

[71] Robyn Taylor, Guy Schofield, John Shearer, Jayne Wallace, Peter Wright, Pierre Boulanger, and Patrick Olivier. Designing from within: humanaquarium. pages 1855–1864, 05 2011.

[72] John Carroll and Mary Beth Rosson. Participatory design in community informatics. *Design Studies*, 28:243–261, 05 2007.

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

[74] Holtzblatt K. Beyer, H. *Contextual design*. Interactions, 1999.

[75] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering stronger password requirements: User attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, New York, NY, USA, 2010. Association for Computing Machinery.

[76] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, page 657–666, New York, NY, USA, 2007. Association for Computing Machinery.

[77] 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, Ottawa, July 2015. USENIX Association.

[78] Blase Ur Miranda Wei, Maximilian Golla. The password doesn ' t fall far : How service influences password choice. 2018.

[79] John Campbell, Dale Kleeman, and Wanli Ma. Password composition policy: Does enforcement lead to better password choices? *ACIS 2006 Proceedings - 17th Australasian Conference on Information Systems*, 01 2006.

[80] Philip Inglesant and Angela Sasse. The true cost of unusable password policies. volume 1, pages 383–392, 01 2010.

[81] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, page 2595–2604, New York, NY, USA, 2011. Association for Computing Machinery.

[82] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? 01 2016.

[83] 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.

[84] Google Chrome Help. Generate a password google chrome help, 2020.

[85] Nora Alkaldi and Karen Renaud. Encouraging password manager adoption by meeting adopter self-determination needs. 01 2019.

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

[87] J. N. K. Rao and A. J. Scott. *On Chi-Squared Tests for Multiway Contingency Tables with Cell Proportions Estimated from Survey Data*. Ann. Statist., Volume 12, Number 1 (1984), 46-60., 1984.

[88] Everplans. The four most popular password managers, 2020. `https://www.everplans.com/articles/the-four-most-popular-password-managers`, Last accessed on 2020-04-03.

[89] PCMag. The best password managers for 2020, 2020. `https://www.pcmag.com/picks/the-best-password-managers`, Last accessed on 2020-04-03.

[90]

[91] 1Password. 1password pricing plan, 2020. `https://1password.com/sign-up/`, Last accessed on 2020-04-05.

[92] LastPass. Lastpass pricing plan, 2020. `https://www.lastpass.com/pricing`, Last accessed on 2020-04-05.

[93] DashLane. Dashlane pricing plan, 2020. `https://www.dashlane.com/plans`, Last accessed on 2020-04-05.

[94] C. Luevanos, J. Elizarraras, K. Hirschi, and J. Yeh. Analysis on the security and use of password managers. In *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pages 17–24, 2017.

[95] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. The emperor's new password manager: Security analysis of web-based password managers. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 465–479, San Diego, CA, August 2014. USENIX Association.

[96] Kasper B. Rasmussen Paolo Gasti. *On the Security of Password Manager Database Formats*. European Symposium on Research in Computer Security, 2012.

[97] Sean Oesch and Scott Ruoti. That was then, this is now: A security evaluation of password generation, storage, and autofill in thirteen password managers, 08 2019.

[98] Norton. Norton privacy manager, 2020. https://us.norton.com/norton-privacy-manager?inid=nortoncom_nav_norton-privacy-manager_products-services:overview, Last accessed on 2020-04-03.

[99] Kaspersky. Kaspersky: Total security, 2020. https://usa.kaspersky.com/total-security, Last accessed on 2020-04-03.

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

[101] 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.

[102] Merlin C. Wittrock. *Knowledge Acquisition and Education*. The Journal of Mind and Behavior, 2000.

[103] Gabriel Lins de Holanda Coelho, Paul H. P. Hanel, and Lukas J. Wolf. The very efficient assessment of need for cognition: Developing a six-item version. *Assessment*, 0(0):1073191118793208, 0. PMID: 30095000.

[104] Markus Appel, Timo Gnambs, Tobias Richter, and Melanie Green. The transportation scale-short form (ts-sf). *Media Psychology*, 18:243–266, 02 2015.

[105] Jonathan Cohen. Defining identification: A theoretical look at the identification of audiences with media characters. *Mass Communication and Society*, 4, 11 2009.