Investigating Factors and Interventions in the Low Adoption of Password Managers

Randall Weber, Naif Alkaltham

12/15/23

Department of Cyber Security

College of Computing and Information Sciences

Rochester Institute of Technology

rjw9659@rit.edu, nma4209@g.rit.edu

Abstract

In today's digital world, almost everyone has faced the challenge of creating and remembering different passwords for various websites and online services. Although it might seem like a simple task, it is more complicated than it appears. When we try to create strong and unique passwords for every website or application, it becomes challenging to remember them all. As a result, many people often use simpler, easy-to-recall passwords or even reuse the same password across multiple accounts, this can be risky. To overcome this problem, cybersecurity professionals recommend the use of a Password Manager (PM) which stores and generates secure passwords for a user. However, overall adoption rates of PMs are quite low despite their associated benefits, with the largest hurdle to adoption being attributed to user mistrust. This study investigates the factor behind low PM adoption via a survey-based user study. By performing an analysis of the responses from the participants, the study was able to uncover several key factors behind user wariness in PMs. Using the information derived from the user responses, several interventions have been identified that can be incorporated into PM design to bolster user trust and confidence. Based on these discoveries, we believe the findings of this study will not only help shed light on the specific factors that influence PM trustability but also allow future PMs to be designed with improved trustability and usability.

Introduction

For most people, password management is a tricky and frustratingly common hassle. Almost every website and online service requires its own unique and secure password for authentication, not to mention any device used to access these services. Many users struggle with the task of password generation, and creating and remembering a wide array of unique passwords across multiple services can become incredibly challenging Zhang et al, (2019). As a result, users tend to create easier, less secure passwords that are less burdensome to recall. Even worse behavior than poor password generation can also occur due to the difficulties of password management.. In some cases, users re-use the same password across multiple logins to save themselves the trouble of memorizing multiple complex passwords Zhang et al., (2019). Re-used passwords pose a significant cyber security risk, as one lost password can cascade into many security breaches. A compromised password on a personal login could even lead to a security breach at the individual's place of work, education, or more if the same login is used in multiple locations.

One proposed solution to the problem of password memorization and generation is a technology called Password Managers (PM)s. PMs are a service that can securely encrypt and store a user's passwords like a kind of digital vault. Instead of memorizing many complex passwords for multiple logins, the user need only remember a singular password, which will provide access to their password ‘vault.' Some password managers even offer the ability to generate new passwords based on secure guidelines, removing the burden of password creation from the user. Password managers take many forms: they can be based on the users’ local device or even exist as a browser add-on with a company storing the users’ passwords on a remote server.

Trust has long been identified as a key issue in PM adoption, with historically low adoption rates due to low user trust of the technology. While attempting to explore methods of increasing adoption rates for PMs, many papers have noted that increased usability features can in fact be detrimental when trying to get users to trust PMs. As there is a limited amount of research to identify when usability features begin to inhibit the trustability of a PM, the primary research objective of this study was to understand what factors have contributed to the low adoption rates and mistrust of password managers. By combining our user study with an extensive review of the literature surrounding PM adoption and trustability, we hope to provide an increased understanding of the user trust relationship with PMs which can in turn be used to suggest interventions for PM designs with the aim of increasing overall adoption rates and usability.

Background

Passwords have been the cornerstone of computing security for almost as long as computers have been available to consumers, with alphanumeric passwords being the most common authentication method. As observed by Alkaldi et al. (2019), many users find the practice of creating memorizing alphanumeric passwords incredibly cumbersome due to memorization demands, thus often opting to either choose short and weak passwords that are easy to remember to ease memory load. These coping mechanisms and behaviors can lead to predictable passwords, making it easy for hackers and other malicious actors to access users' accounts, violate their privacy, and steal their data. Password Managers are designed to address this problem by providing users with a mechanism to store all their passwords in a single place and avoid the burden of excessive memorization. Password managers allow users to use a singular strong password to access a secure vault of all the user's other passwords. Password managers frequently possess secure password generation and autofill features to provide further assistance to users. Autofill allows the PM to automatically input the user's login credentials when prompted, eliminating the need for users to memorize many complex passwords. By combining autofill and with password generation features, which create unique passwords for the user in accordance with strong password guidelines, PMs allows users to maintain many strong passwords for their separate accounts without having to worry about rote memorization.

PMs store their encrypted password vaults using two distinct methods. The first method is storing the vault on the user's own device. In this case the password manager generally takes the form of a separate application that needs to be open while performing logins. This method allows the user to retain local control of the password database but can also open the user to risk if the device storing the passwords is compromised. The second method relies on a third party for storage for the password vault. This method is the most popular form of PM and is represented by managers like Google's password manager and other browser based PMs. This method relies on especially strong trust in the PM company to maintain the security of the user's password vault.

Related Work

The intention to use password managers has received considerable attention from cybersecurity scholars seeking to establish the factors influencing adoption intentions because password manager adoption rates have been historically low despite endorsement by reputable cybersecurity professionals and organizations. One of the factors highlighted as the possible causes of this low adoption and mistrust is a lack of awareness regarding these tools Alkaldi & Renaud, (2022). Some researchers have also cited poor usability as a limiting factor in the adoption of password managers Seiler-Hwang et al., (2019). However, several researchers have disputed this assertion, arguing that the issue is more complex and goes beyond usability concerns Zhang et al., 2019; Schechter, (2019). The possibility of cost being a limiting factor has also been disputed on the grounds that there are numerous password management apps that are readily available for free Alkaldi & Renaud, (2022).

Many attempts have been made to address the problem of effective password generation and memorization. Since the issue of 'weak' passwords is so widespread and ubiquitous, it has become imperative for security researchers to discover new tools and techniques to solve the problem. Tools like graphical passwords have been experimented with to create a simpler alternative to traditional passwords, but all of these tools have come with their own security and usability trade-offs. For instance, while a graphical password may be easier to remember, it is much easier to shoulder surf compared to a traditional text-based password (Tari et al., 2006).

While previous studies of security usability, like the one by (Fahl et al. 2012), have indicated that more usable and user-friendly systems are more likely to inspire trust in the user, the opposite appears to be true for Password Managers. The trust relationship between users and password managers is further complicated by worries of password manager companies being breached by malicious actors or the risk of having all of one's passwords in a single centralized location. For instance, a study conducted by (Zhang et al. 2019) suggested that users are unwilling to hand over control of their passwords to a password manager due to fear of the susceptibilities associated with such tools, especially web-based ones. They identified the auto-fill functionalities in some of the password managers as one of the factors that could be contributing to the existing mistrust. Zhang and colleagues' findings suggest that the usability and user-friendliness associated with password managers have not managed to inspire trust among the users. Based on these observations, this paper seeks to bridge the gap

(Alkaldi et al. 2019) investigated the influence of meeting users' self-determination needs on the intention to adopt smartphone password managers. Their study was based on the self-determination theory (SDT), which posits that humans are motivated to engage in a specific activity by three psychological needs: autonomy, competence, and relatedness (Alkaldi et al., 2019). After running a longitudinal experiment testing the influence of satisfying the participants' self-determination needs on the intention to install a password manager, they reported that meeting the three needs proposed by the STD encouraged smartphone password manager adoption. Alkaldi and colleagues' study was limited by the fact that the relatedness aspect was tested by asking participants to recruit others, increasing the possibility of sampling bias. Furthermore, the study had no mechanisms of establishing whether the participants retained the password managers after installing them. This limitation implies the need to investigate the factors influencing long-term adoption.

User trust in Storage Methods/Centralization: Earlier iterations of password managers struggled with gaining user trust in a centralized password storage system. Even as far back as a PM study by (Halderman et al, 2005), when little research had been made about user trust of PMs, the authors were cognizant of the fact that many users feared the centralization of a password manager. The model used by Halderman et al's study features many critical components of modern password managers, like a single strong password for login to the 'vault' and autofill of encrypted passwords as well. When attempting to authenticate to a site, the author's system, Password Multiplier, is opened and prompts for a master password to access the system. After the master password is provided, either a new password is generated by Password Multiplier and used to autofill the site login or a previously created password is auto-filled instead. The weakness of this paper, like many other Password Manager designs, is that it does not include a study or detailed analysis of user confidence in the system. The authors acknowledge that users may be hesitant to trust centralized control of their passwords but do not delve further into that specific question.

(Guan et al. 2018) identifies several potential reasons for user trust in Password Managers. The two primary reasons cited by the paper are fears of software vulnerability and a feeling of vulnerability with all of their passwords being centralized in one location. This feedback especially on the centralization of passwords echoes user concerns mentioned in previous studies. The researchers propose VaultIME, a novel concept for a mobile device-based PM that, instead of completely filling the users' password for them, would detect if the user inputted a 'near-enough' password and autocorrect to the correct password stored in a password manager. The main weakness of this paper is the lack of user studies. The authors of the paper make sure to test for any potential security flaws with VaultIME rigorously and are very successful in that regard, but they do not answer the question of whether the design is easier to trust for users.

(Amft et al. 2023) argues that password manager usage might be deterred by mixing passwords. In other words, users don’t want to store their gaming password alongside their banking password if both use the same security authentication. Additionally, built-in PMs for browsers saw a much higher adoption rate than 3rd party PMs due to users desire for convenience. An important finding of this paper is that password managers are primarily valued as a convenience tool for users with their autofill features rather than a security tool for storing passwords in a secure location.

User Trust via Convenience/usability: (Halderman et al. 2005) sought to create a desirable password manager by combining security and convenience. The implementation of Halderman et al.’s design is very similar to many modern password managers and features a singular strong login to access a 'vault' of hashed passwords, which the program auto-fills into prompted login fields. The main shortcoming of this paper is there is little mention of any usability studies to evaluate the proposed design. As the authors’ feedback is the only available analysis of the tool's functionality, it is difficult to ascertain how usable it was to the average individual. The lack of a study also makes it difficult to judge if users would have difficulty trusting the tool and if the supposed convenience of the tool improved user trust in the password manager itself or if that convenience had the opposite effect of lowering confidence in the manager.

(Alodhyani et al. 2020) presents the findings of a study conducted to investigate the factors contributing to the low adoption of password managers. The study performed a heuristic evaluation to determine the challenges associated with password managers' user interfaces and functions and usability tests using interviews and online questionnaires. The authors suggest that trust and transparency issues are the primary contributing factors to the low adoption of PMs, with usability playing an insignificant role in overall adoption rates. However, some issues related to the user interface and functions of password managers were raised, including design complexity and use of computer jargon.

(Chaudhary et al 2019) explores further research into the usability of password managers. On the other hand, (Zibaei et al. 2023) advocates an alternative method of using nudges to boost usability and trust in password managers based on safari’s password manager. The authors advocate an alternative method of using nudges to boost usability and trust in password managers based on safari’s password manager. The authors analyze the fact that safari’s password manager has a higher adoption than most other password managers. The paper dissects many of the factors that the researchers believe increase adoption like using different language to inform the user a password has been created/saved ex: “Safari has created a strong password for this website”. The paper indicates that autofill capabilities and a default nudge to prompt the user to create/save their password to manager are the most effective methods for increasing adoption.

Study Design

Based on the literature review, the main idea the study sought to understand was what factors have contributed to the low adoption rates and mistrust of password managers. By understanding this question the study can help answer the question of what interventions can increase user trust/adoption in password managers and guide users to follow cybersecurity best practices? An overwhelming theme of the reviewed literature is that many researchers are aware of the fact that users without a security background (and, in some cases, even users who have a security background) have a difficult time trusting password managers as a technology. (Alkaldi et al. 2019), indicate that traditional methods of improving user confidence in software, like better usability and more readable UI’s, can have a counterproductive effect by lowering user confidence in the password manager. To this end, the project builds upon the previous studies' findings to investigate why users are hesitant to trust password managers and recommend the strategies that can be used to boost users’ trust in these tools.

The study was not seeking to test a new security/privacy-related task, product or idea at this time. It sought to shed light on the reasons behind the low adoption rate of password managers and analyze novel strategies that can be used to improve its overall usage. To delve into this topic, the study relied on a critical review of the available literature and a survey to gain further insight into users' thoughts and feelings about password managers. Participants were recruited via email and word of mouth, with the only required prerequisite for volunteers being that they must have some experience creating and authenticating with passwords. Experience with password managers was ideal but not necessary. We wanted feedback from users who have decided against using password managers or have not made use of them for one reason or another. The low barrier for entry helped to get a wider percentage of the population and acquire data from a diverse array of demographics. This technique's relevance to the present study is enhanced by the fact that it eliminates sampling biases like the one reported by (Alkaldi and Renaud 2022), which involved asking participants to recruit others. It also improves results generalizability because the views obtained are not from a specific group or platform. Utilizing feedback from a diverse array of demographics helped to generate new ideas concerning the factors influencing users' adoption or trust in password managers.

The distribution of online survey questionnaires was a great success with a total of 40 unique responses. The target population was mainly individuals from non-technical and non-security backgrounds. Based on the data collected from the survey, it appears this objective was achieved. Only 12.5% of participants self-reported some experience with cybersecurity. The main vector for spreading the survey was distributing emails and word of mouth. Volunteers were provided with an informed consent form that explained relevant information regarding the research purpose, requirements for participation, procedure, risks and benefits, and confidentiality of any personal details shared.

Both closed and open-ended questions were used in the survey questionnaires to avoid limiting the participants' responses and encourage them to give as much information as possible. These questions' responses helped to gauge the users perception as to usability and trustworthiness of password managers. The feedback received from participants helped in devising strategies that can be used to improve users' trust and acceptability of password managers. Since some of the data obtained is qualitative, a thematic analysis was employed to find themes from the patterns of responses. These themes informed discussions about factors influencing password managers' adoption and the strategies needed to boost their usage and users' trust/acceptance. The quantitative data obtained was used to draw charts for statistical analysis and presentation.

Study Results

Respondents demographics profile

The demographic characteristics assessed in the present study included age and technical backgrounds of the participants. As indicated in the chart below (Figure 1), the majority of those who responded to the questionnaires were between 55 and 64 years old (35.7%), followed by those aged 65 years and above (32.5%). Young adults (18 to 24 years) were the third-largest age group, comprising 15% of the respondents. Adults and middle-aged persons accounted for the remaining percentage (15%).

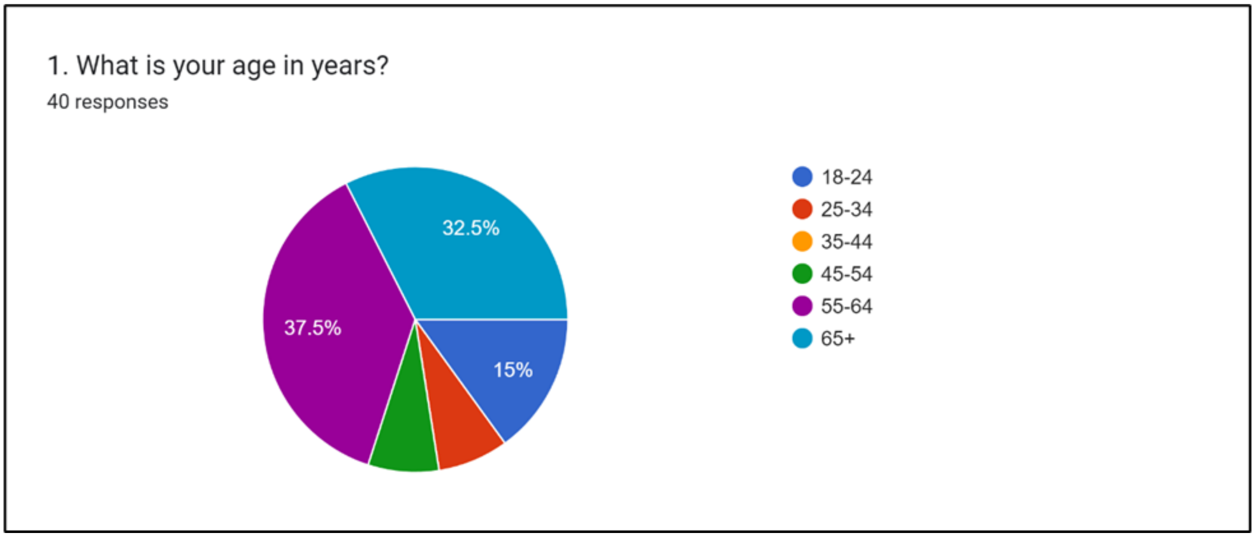


Figure 1: A chart showing respondents' age profile

Regarding the respondents' technical backgrounds, results indicated that most of participants had little to no background in cybersecurity, suggesting they were from non-technical/non-security backgrounds (see Figure 2 below).

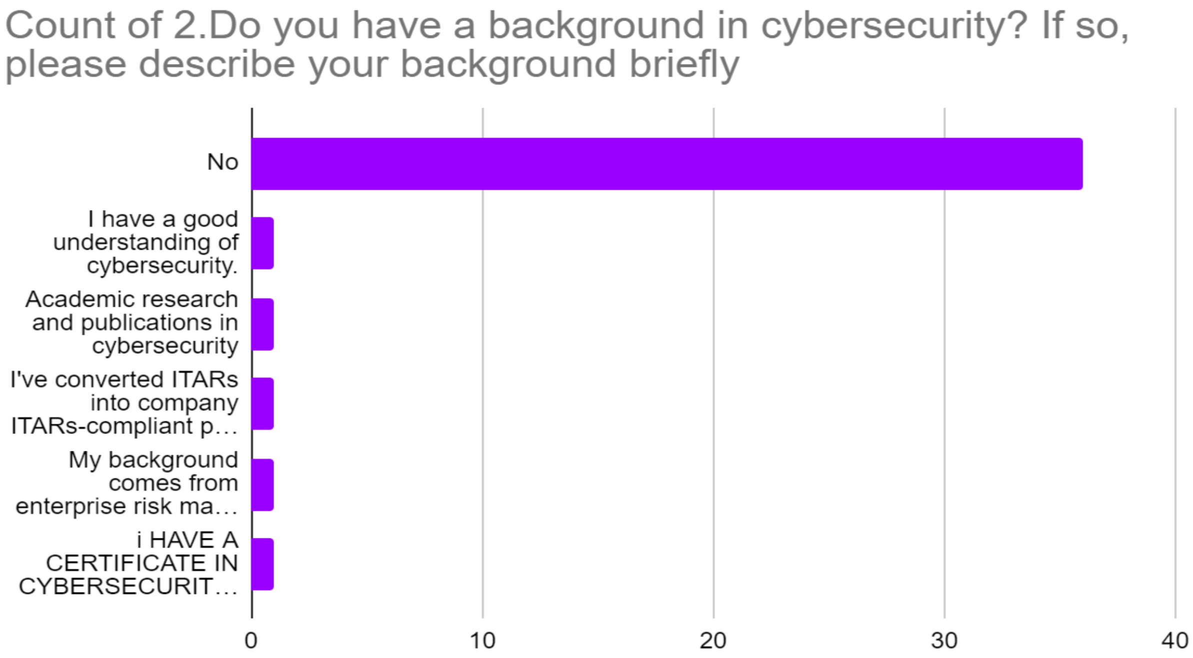
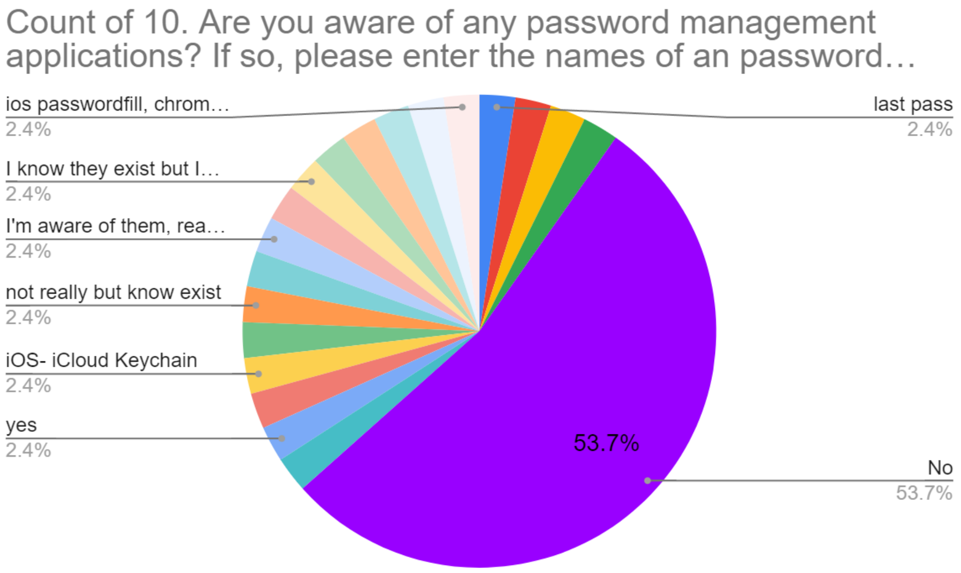


Figure 2: Respondents technical background

Findings for Hypothesis: What factors have contributed to the low adoption rates and mistrust of password managers?

The study identified several critical factors contributing to the low adoption rates and mistrust of password managers. These include concerns over software vulnerabilities, centralized password storage, and the perceived complexity of password manager interfaces. Additionally, a lack of awareness about these tools and their benefits played a significant role in their underutilization.



Findings for Hypothesis: What interventions can increase user trust/adoption in password managers and make users follow best cybersecurity practices?

Finding: The study identified several key interventions crucial for enhancing trust and adoption of password managers. These include addressing software vulnerabilities, providing options for both centralized and local password storage, and simplifying the user interface of password manager tools. Additionally, increasing awareness and understanding of the benefits and functionalities of these tools emerged as a significant factor in their underutilization.

Discussion

Discussion of the results on the factors contributing to the low adoption rates and mistrust of password managers.

One of the primary objectives of the present study was to explore the factors contributing to the low adoption rates and mistrust of password managers. The responses obtained from the participants suggested that concerns over software vulnerabilities, centralized password storage, and the perceived complexity of password manager interfaces are the primary reasons users do not use or trust password managers. It also emerged that a lack of awareness about these tools and their benefits has played a significant role in their underutilization and users' mistrust towards them. In other words, many people do not know password managers or have no idea how they are used and their benefits. This finding indicates that if awareness campaigns are conducted to educate internet users about the meaning and importance of password managers, the adoption rate can improve.

Awareness campaigns could also go a long way toward addressing the security and privacy concerns of storing passwords in a centralized place. Many participants in this study expressed their fears that centralizing all their passwords can expose them to security and privacy risks due to possible data breaches. To this end, helping them understand how password managers can help them manage their password security could be critical in enhancing their confidence. Previous studies have also cited a lack of awareness as one of the factors contributing to the existing mistrust in password managers. For instance, (Alkaldi and Renaud, 2022) established that a lack of awareness regarding these tools has contributed to their low adoption and mistrust. (Zhang et al. 2019) examined the reasons for not using password managers effectively and found that users are afraid of storing their passwords in a single centralized location due to the possibility of unauthorized or malicious actors exploiting the susceptibilities of these tools.

Discussion of the results on the interventions that can increase user trust/confidence in password managers and make users follow best cybersecurity practices.

The other objective of this study was to propose interventions that can increase user trust/confidence in password managers and make users follow best cybersecurity practices. Based on the participants' responses, it emerged that trust and adoption of password managers can be enhanced using several interventions. They include addressing software vulnerabilities, providing options for both centralized and local password storage, and simplifying the user interface of password managers. Additionally, increasing awareness and understanding of the benefits and functionalities of these tools emerged as a significant factor in boosting users' trust/confidence in password managers and making them follow best cybersecurity practices. This finding is supported by several past studies, including Alkaldi et al. (2019), Alkaldi and Renaud (2022), and Seiler-Hwang et al. (2019).

Implications and recommendations

This study has significant theoretical and practical implications. Its theoretical contributions include expanding the available knowledge regarding the factors contributing to the mistrust and low adoption of password managers. The presented findings can also provide the basis for future researchers to examine the matter comprehensively. Practical implications include creating awareness about password managers, their benefits, and their impacts on the security and usability of computer systems. The findings presented can be used by developers of password management tools to improve their usability and make the necessary adjustments to improve acceptability. To this end, it is recommended that significant awareness campaigns be conducted to enhance users' knowledge of the meaning of password managers and their benefits. Such knowledge will go a long way to mitigating some of the users' concerns regarding these tools. It is also recommended that such tools be as user-friendly and secure as possible to increase satisfaction and trust.

Limitations

Most of the constraints observed so far are related to the data collection process. For instance, time constraints have posed the most significant challenge because a balance has to be struck between this project and other classes. This challenge also forced us to limit the scope to a manageable sample size, which could limit results' generalizability. It is worth noting that the study targeted respondents with no technical or security background, meaning that the views of those with background in cybersecurity could not be captured. Furthermore, the self-selected sampling technique employed to find participants increased the risk of having respondents who do not meet the desired criteria. Another limitation worth highlighting is the possibility of some users giving inaccurate information regarding their password management behaviors. Gender information was also not collected during the survey process, and further reading has indicated that gender may also play a role in password manager selection/trust (Yan, J., & McCabe, D.).

Future work

The next steps to extend the work of this project would be to design a fully functioning prototype based on the design suggestions laid out in this paper. Ideally a user study would be conducted after the prototype has been completed and with a detailed analysis to evaluate the trustability, security, and ease of use of the prototype compared to other popular password managers. Additionally to further enhance the data used to design a mockup, limited user interviews which were beyond the scope of this project, would allow a much deeper understanding of the user's trust relationship with PMs and could provide much more extensive insights that a simple questionnaire could provide as well. Further research also needs to be carried out to assess the viability of advertising done by PM companies. Other studies have also recognized insufficient advertisement of PMs to consumers and our data indicated a majority of participants had no knowledge of PMs provides strong evidence to that point.

References

1. Alkaldi, N., & Renaud, K. (2022). MIGRANT: Modeling smartphone password manager adoption using migration theory. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *53*(2), 63–95.Accessed on 10/10/23
2. Alkaldi, N., Renaud, K., & Mackenzie, L. (2019). Encouraging password manager adoption by meeting adopter self-determination needs. Accessed on 10/30/23
3. Alodhyani, F., Theodorakopoulos, G., & Reinecke, P. (2020). Password managers—it's all about trust and transparency. *Future Internet*, *12*(11), 189. Accessed on 11/13/23
4. Amft, S., Höltervennhoff, S., Huaman, N., Acar, Y., & Fahl, S. (2023). "Would you give the same priority to the bank and a game? I do {not!}" exploring credential management strategies and obstacles during password manager setup. In *Nineteenth Symposium on Usable Privacy and Security* (pp. 171-190). Accessed on 11/13/23
5. Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., & Berki, E. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features. *Computer Science Review*, *33*, 69-90. Accessed on 11/20/23
6. Fahl, S., Harbach, M., Muders, T., Smith, M., & Sander, U. (2012, July). Helping Johnny 2.0 to encrypt his Facebook conversations. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1-17). Accessed on 11/12/23
7. Guan, L., Farhang, S., Pu, Y., Guo, P., Grossklags, J., & Liu, P. (2018). VaultIME: Regaining user control for password managers through auto-correction. In *Security and privacy in communication networks: 13th International Conference, Securecomm 2017, Proceedings 13* (pp. 673-686). Accessed on 11/23/23
8. Halderman, J. A., Waters, B., & Felten, E. W. (2005, May). A convenient method for securely managing passwords. In *Proceedings of the 14th International Conference on World Wide Web* (pp. 471-479). Accessed on 11/25/23

9. Schechter, S. (2019). *Before you use a password manager*. Medium. https://stuartschechter.medium.com/before-you-use-a-password-manager-9f5949ccf168. Accessed on 11/25/23

10. Seiler-Hwang, S., Arias-Cabarcos, P., Marín, A., Almenares, F., Díaz-Sánchez, D., & Becker, C. (2019). “I don't see why I would ever want to use it." analyzing the usability of popular smartphone password managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1937-1953). Accessed on 11/27/23

11. Silver, D., Jana, S., Boneh, D., Chen, E., & Jackson, C. (2014). Password managers: Attacks and defenses. In *23rd USENIX Security Symposium* (pp. 449–464). Accessed on 11/27/23

12. Tari, F., Ozok, A. A., & Holden, S. H. (2006, July). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *In Second Symposium on Usable Privacy and Security* (pp. 56–66). Accessed on 11/27/23

13. Zhang, S., Pearman, S., Bauer, L., & Christin, N. (2019, August). Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security.* Accessed on 11/27/23

14. Zibaei, S., Salehi-Abari, A., & Thorpe, J. (2023). Dissecting nudges in password managers: simple defaults are powerful. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)* (pp. 211-225). Accessed on 11/27/23

15. Yan, J., & McCabe, D. (2022). Gender bias in password managers. *arXiv preprint arXiv:2206.14136*. Accessed on 11/27/23

Appendix:

Study Questions:

1. What is your age in years?

2.Do you have a background in cybersecurity? If so, please describe your background briefly

3. On scale of 1-5 (5 being the highest) how much does the following statement apply to you: "I have difficulty keeping track of all my passwords"

4. Have any of the online services you use required you to create a password?

5. Approximately how many unique passwords do you have for online services?

6. What strategies do you typically apply to recall your passwords?

7. On a scale of 1 to 5, how confident are you in your current password management strategy?

8. Do you use a browser based auto fill like on Chrome or Firefox? If so which one?

9. How frequently do you enter passwords without the assistance of an auto-fill service

10. Are you aware of any password management applications? If so, please enter the names of an password managers you have heard of.

11. Have you ever used a password manager? If so, which one(s)?

12. If you answered the previous question, which password manager(s) did you use? Additionally please describe your experience.

13. If you answered N/A to question 11, why have you not considered using a password manager?

14. Have you ever forgotten your password for an online service?

15. What are your main concerns regarding the use of password managers? (Select all that apply)

16. Assuming all proper security measures are taken, Would you be more likely to trust a password manager that stores your information in the cloud/external location or on your personal device?

17. What is your reasoning for preferring an external or local based solution to password storage?

18. If a password manager could assure you of its security and privacy, would you consider using it?

19. How often do you change your passwords for online services?

20. Have you ever had an account compromised by a stolen password?

21. If you answered Yes to question 20, were you using a password manager at the time?