Replication: A Study on How Users (Don't) Use Password Managers

Pithayuth Charnsethikul
University of Southern California
Information Sciences Institute
charnset@usc.edu

Anushka Fattepurkar
University of Southern California
fattepur@usc.edu

Dipsy Desai
University of Southern California
Information Sciences Institute
deepakde@usc.edu

Gale Lucas
University of Southern California
Institute for Creative Technologies
lucas@ict.usc.edu

Jelena Mirkovic
University of Southern California
Information Sciences Institute
mirkovic@isi.edu

***Abstract*—We replicated the study by Mayer et al. [1] on password habits and password manager (PM) usage at a large private US university. We conducted an online survey (n=437) and found high awareness (96%) and usage (94%) of PMs, but limited use of password generation (26%) and substantial password reuse, with participants reusing more than half of their passwords. These findings are consistent with the original study. However, we found that participants were unlikely to adopt a free third-party PM offered by the university, contrary to the original findings. Extending the original study, we found that awareness of the free PM was low: only 35% knew about it, and its adoption was even lower, at just 15%. We also found that faculty had the strongest password habits, while students had the weakest. Based on our findings, we provide recommendations for increasing the use of password generation features, broadening adoption of an institution-provided PM, and guiding future replication efforts.**

I. Introduction

For decades, passwords have been the most widely adopted form of authentication, as they are intuitive and easy to use [2]. With the ever-growing number of accounts, users face increasing challenges in managing passwords. Prior work shows that the median number of password-protected accounts per user increased from 25 in 2006 [3] to 80 in 2018 [4]. Ideally, each password should be strong and unique across accounts. In practice, users often prioritize convenience, relying on weak but memorable passwords [3], [5] and reusing passwords across services [1], [3], [6], [7]. Research suggests that this behavior stems from users underestimating the risks posed by weak passwords [8], [9] and password reuse [4], [10].

Password managers (PMs) are designed to help users securely manage their passwords. They can help create and store many unique, strong passwords, thus eliminating the risk of weak or reused passwords. Although PM adoption was initially low – 18% in 2016 [11] – it has increased in recent years, reaching 77% in 2021 [1]. While PMs can help users generate strong and unique passwords, users primarily rely on PMs for convenience features such as auto-filling, storing, and synchronizing passwords across devices [12]. Users make far less use of security-oriented features like password generation, which were designed to address the challenges of creating and managing strong, unique passwords [13], [14].

Prior work shows that institution-wide studies, such as those conducted at universities, provide an effective way to capture insights across diverse user groups, that can help understand PM adoption, usage patterns, and the reasons behind them at scale [1], [15], [16], [17], [18]. We were especially intrigued by Mayer et al. [1], who conducted a study at the George Washington University (GWU) to quantify password habits and PM usage at a university. This study was one of the first large-scale measurement that quantified adoption of PMs at university settings. Mayer et al. produced several important findings. For example, most participants used PMs, with third-party PMs being the least used. Consistent with Pearman et al. [13], ease of use and transparency drove adoption of built-in PMs, while security primarily motivated the use of third-party PMs. Many users reused passwords, but third-party PM users tended to reuse them less. Based on the observation that use of third-party PMs drove better security habits, Mayer et al. measured participants' likelihood of adopting a third-party PM if the university offered it for free, as GWU was considering purchasing a license (though they did not). They found that users were likely to adopt this free third-party PM.

In this paper, we replicated Mayer et al.'s study [1] four years later at the University of Southern California (USC), which has twice the student population of GWU. USC provides students, staff and faculty with free 1Password subscriptions. This allows us to verify whether the hypothesis by Mayer et al. – that university participants are likely to adopt a free third-party PM – holds true in practice. Specifically, we conducted an online survey (n=437) to examine USC participants' password practices and their use of PMs including

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23032
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

whether they adopted the free PM provided by the university.

Replicating the study at another university is valuable for several reasons. First, institutional context matters: universities differ in size, student demographics, IT environment, and security practices. This variance allows us to examine whether the original findings generalize to different institutional settings. Second, the replication was conducted at a different point in time, enabling us to evaluate the robustness of Mayer et al.'s findings and to identify which results are sensitive to temporal changes. Third, our study introduces a meaningful intervention where participants have access to a third-party PM for free. This allows us to assess whether removing cost and access barriers affects PM adoption and usage patterns.

We aim to answer the following research questions:

RQ1: Are university participants aware of PMs? (**Awareness**)

RQ2: How do university participants manage their passwords, and what role do PMs play? (**Password Strategies**)

RQ3: What are university participants' experiences with using PMs? (**Password Manager Users**)

RQ4: How do university participants manage their university account passwords? (**University Password Strategies**)

RQ5: Do university participants adopt a free PM offered by the university, and why? (**Free-PM adoption**)

We summarize our findings. **RQ1:** Most users are now aware of PMs. Only 4% of participants reported learning about them for the first time during the study, consistent with 9% at GWU. **RQ2:** Each user reuses more than half of their passwords: 40% of passwords are unique per user (median), consistent with findings at GWU (77% of GWU participants reported reusing passwords). In addition, the use of password generation remains low: 26% of participants regularly use PMs to generate passwords, consistent with 20% at GWU, though 58% of USC participants use PMs to generate passwords at least occasionally. Extending beyond GWU findings, we found that faculty have the strongest password habits, while students have the weakest: faculty have a significantly higher number of unique passwords and use PMs to generate more passwords than staff and students. **RQ3:** Most users at USC use PMs: 94% of participants reported using them, consistent with 77% at GWU. 76% of PM users at USC, in fact, use multiple types of PMs, while GWU did not report this figure. Browser-based PMs remain the most commonly used, while third-party PMs are still the least used, consistent with findings at GWU. However, our results show that 45% of participants use third-party PMs – a substantial increase from 18% at GWU. **RQ4:** Most users perceive their university accounts as more secure than other accounts: 94% of participants rated their university passwords as at least as secure as their other passwords, and 59% rated them as more secure, consistent with findings at GWU (83% and 36% respectively). **RQ5:** Users were unlikely to adopt the free third-party PM offered by the university: 48% of PM users and only 26% of non-PM users reported being likely to adopt it. This contrasts with findings at GWU, where participants were more likely to adopt the free PM (71% and 56%, respectively). More importantly, we found that awareness of the free PM is low: only 35% of participants knew about it, and usage is even lower, with only 15% actually using it. After learning about the free PM in the study, only 24% of participants expressed interest in adopting it.

Based on our findings, we provide the following recommendations. First, to increase the use of password generation features, generated passwords should better align with users' preferences for memorability, as suggested by our results. While some third-party PMs already offer options for generating more memorable passwords, this functionality needs to be more widely available in the PMs that users most commonly rely on, such as browser- and OS-based PMs. Second, to increase adoption of an institution-provided third-party PM, institutions should move beyond passive promotion and instead provide timely, contextual nudges that clearly communicate the added value of the free PM. They should also address the perceived effort of PM transition [19] and concerns over long-term access, as our results show that these are key barriers to adoption. Third, we highlight directions for future replication, emphasizing the need to study a broader range of institutional contexts and geographic regions, since both our replication and the original study focus only on US universities. In addition, we recommend follow-up qualitative studies to better understand users' underlying motivations and concerns that cannot be fully captured through quantitative analysis alone.

II. Background and Related Work

Password Managers (PMs) are software tools that help users manage their account passwords by securely storing them, auto-filling them at login time, making them available across different devices, and generating new strong passwords. There are three types of PMs as described in [1]: (1) **System-provided PMs**, which are built into the operating system (OS), such as Apple Keychain in iOS or Google Password Manager in Android. These PMs can be synchronized across devices running the same or compatible OS, for example, between iOS and macOS, or across Android devices; (2) **Browser PMs**, which are built into web browsers such as Chrome, Firefox, and Brave. These PMs allow users to synchronize passwords across devices by logging into the same browser account and enabling a sync option on each device; and (3) **Third-party PMs**, which are standalone applications such as 1Password, Dashlane, and LastPass. These PMs typically require a subscription and offer a wider range of features than system-provided or browser-based PMs. These features include more flexible organization options (e.g., multiple vaults for separating types of passwords), secure storage for non-password data and advanced cross-platform support.

A. Password Security

Passwords have been the most widely used and broadly accepted form of authentication for decades, largely because they are intuitive and straightforward [2]. For security reasons, passwords should be strong and unique for each service, yet previous research shows that these practices are difficult for users to implement. Florêncio et al. reported that users tend

to use weak passwords when they are not required to create strong ones [3]. Stobert et al. extended this finding by showing that users do choose to create strong passwords, but they reserve this effort for accounts they consider important [5]. However, users often misunderstand what constitutes a strong password. Ur et al. found that users tend to underestimate how vulnerable weak passwords can be [8], [9]. For example, they might believe that simply adding numbers to a password greatly improves its security, when in fact it does little, or underestimate how easily common phrases such as "iloveyou" or common keyboard patterns like "1qaz2wsx3edc" can be cracked by attackers, or assume that passwords that are hard to spell are inherently more secure. Hanamsagar et al. extended this finding by showing that users also tend to underestimate the number of account passwords they have, lose track of them, and misunderstand the extent of threats from password reuse [4] and how sophisticated and effective password-guessing attacks have become [4], [20], [21].

Due to these frequent user misconceptions, many systems now enforce password-creation policies (PCP) and incorporate password meters or nudges to help users create stronger passwords [22], [23], [24], [25]. There has been substantial research on PCP, examining both their security and usability [24], [26], [27], [28], [29], [30], [31]. Intuitively, stronger policies are often assumed to reduce usability. However, Komanduri et al. demonstrated that this is not always the case [32]. For example, a policy requiring only a longer password (16 characters) produced significantly stronger passwords than a policy requiring a shorter password length but with multiple character cases. This finding was later supported by Shay et al. [33], [34]. Woods et al. also suggested that unique passwords are more memorable than modified or reused passwords [35]. Similarly, Kim et al. found that both memorability and security increased majorly for verbal passwords under stronger PCP [36].

Advances in password cracking make it increasingly important to strengthen PCP [37], [38], [39], especially given today's powerful computing resources. However, a major challenge for users is that stronger policies often require them to invest more effort in creating secure passwords. Abdrabou et al. reported that users' pupils dilated more when creating stronger passwords, suggesting increased cognitive load [40]. To minimize cognitive load, many users generate a small number of strong passwords and reuse them across multiple sites [6], exposing themselves to password-reuse attacks. Early studies estimated that 43-51% of users reused passwords across multiple sites [7], and this number increased to 77% by 2022 [1]. Florêncio et al. and Wash et al. found that users typically reuse each password on 2-4 sites [3], [6]. With the growing number of accounts per user – from a median of 25 in 2006 [3] to 80 in 2018 [4], managing account passwords – each ideally requiring a strong, unique password – becomes increasingly challenging for users over time.

B. Password Managers

Password managers (PMs) are designed to help ease users' cognitive burden when managing their passwords.

Adoption challenges. PMs have advanced substantially over the past decade [41], [42]. However, research shows that adoption was low initially, largely due to limited understanding of these tools [43] and concerns about their security [44], [45], [46], [47]. Alkaldi et al. found that many users were unsure what PMs are, how to use them effectively, and whether they could be trusted [11]. Fagan et al. further showed that PM users adopted these tools primarily for their convenience and usefulness, whereas non-users avoided them mainly due to security concerns and were more suspicious of the tools than PM users [48]. Consistently, Klivan et al. found that users indeed viewed PMs as tools for convenience rather than security [12]. While trust in PMs improves over time [49], some users still do not fully trust PMs, especially older users [50]. This leads users to avoid storing important passwords in a PM [12].

Adoption of various types of PM. Lyastani et al. and Pearman et al. found that third-party PMs are primarily adopted by security-oriented users, whereas system-provided and browser-based PM users are often motivated more by convenience and may be more prone to weak passwords and reuse [13], [14]. Some users now even adopt multiple types of PMs simultaneously, using one as a backup for another [51]. Ponticello et al. also found that blind and low-vision users now adopt PMs primarily for usability and accessibility reasons [52].

C. Institutional Adoption of Security Technologies

Institution-wide studies at a university provide an effective way to measure adoption of security technologies across a large user population. Universities are especially appealing for studying security practices because they include a diverse population with varying IT backgrounds – from students who may be less concerned about online security and privacy to faculty and staff who typically undergo security training – while still allowing users to make their own IT choices. Unlike other institutions such as businesses or hospitals, which have stricter policies and compliance rules, universities allow researchers to observe how people naturally use security tools across a variety of digital contexts and everyday activities. Shay et al. reported that although university users were annoyed by stricter password policies, they still felt these policies improved their security [15]. Similarly, Colnago et al. found that users generally viewed Duo, a 2FA platform, as annoying yet easy to use, while still believing it enhanced account security [16]. Dutson et al. later confirmed these findings at a different university and further showed that students and faculty held more negative perceptions of Duo than staff [53], consistent with Arnold et al., who reported that students were displeased with 2FA because it added extra login steps, particularly during time-sensitive tasks such as quizzes and tests [54]. Colnago et al. also highlighted that ease of use and perceived value play major roles in users' decisions to adopt 2FA [16]. Nisenoff et al. showed that users prevalently reused their passwords. Through guessing attacks, they were

able to identify 32% of university passwords that were reused across accounts exposed in online data breaches [10]. When updating passwords, Ariana et al. and Colnago et al. observed substantial increases in university help desk tickets, 3–4× and 5×, respectively due to users forgetting new passwords or encountering difficulties with the update process [16], [18]. Mazurek et al. found that users from science and technology schools created stronger passwords than those from the business school, and stronger passwords were associated with higher rates of failed login attempts [17]. Becker et al. supported this, showing that users with passwords of strength over 300 days (calculated by Shannon entropy) were 4× more likely to forget them compared to those with passwords of 100-day strength, suggesting that users with stronger passwords are more likely to forget and reset them [55].

D. Our Replication Focus

Mayer et al. [1] studied adoption of password managers among George Washington University's faculty, staff and students in 2021. They found that 77% of users relied on PMs, but only 18% used third-party PMs. Mayer et al. based their survey on the interview questions from Pearman et al. [13]. Both studies consistently found that the adoption of built-in PMs, such as those in browsers or operating systems, is primarily driven by convenience, whereas adoption of third-party PMs is motivated by security. The low usage of third-party PMs may also be explained by their poor usability [56]. Mayer et al. further reported that 77% of users reused passwords, consistent with [15]. One main finding of Mayer et al.'s study was that institutional users would be likely to adopt a third-party PM if offered by their institution for free.

Our work sought to replicate Mayer et al.'s study at USC. Unlike GWU, USC provides a third-party PM, 1Password, for free to all students, staff and faculty. This creates a natural experiment that can validate or refute Mayer et al.'s conclusions about users' willingness to adopt a third-party PM offered for free by the university. Our study mostly replicates Mayer et al.'s methodology, and extends it with additional questions that dive deeper into users' reasons for PM adoption We elaborate this in detail in Section III-A.

Our study at USC represents the second large-scale quantitative measurement of PM usage at a university, after the study at GWU [1]. We confirm many of the findings from the original study and other prior work, including: an upward trend in PM awareness and usage [1], [11]; many users now relying on multiple PMs [51]; persistently high rates of password reuse [1], [3], [6], [7], [19]; and low use of PMs to generate strong passwords [1], [13], [14]. We contribute the following novel findings: (1) Contrary to Meyer et al.'s findings, users at USC were unlikely to adopt a free, third-party PM; (2) We measured additionally user awareness of the free third-party PM offer at USC, and its usage, and find that both were low; (3) We found that users reused on average more than half of their passwords; and (4) We found that students had the weakest password habits, while faculty had the strongest.

III. Methodology

We used an online survey to measure USC participants' password management practices and experiences with PMs. The survey was adapted from the original work [1], with some questions modified and other questions added to capture additional insights that were not explored in the original study (Section III-A). We used Qualtrics [57] to host the survey and distributed it through several recruitment channels to reach USC participants (Section III-B).

Before launching the study, we piloted the survey with 10 lab members to gather feedback, particularly on the new questions added. We revised the survey accordingly before distributing it to USC participants. The study was conducted over the course of one month, from September to October 2025. In total, we collected 619 responses and removed low-quality ones (Section III-C), resulting in 437 responses used for data analysis (Section III-D). Study participants were anonymous. They had an option to submit their email into a raffle for a $10 gift card. We discuss ethical considerations in Section III-E and the study's limitations in Section III-F.

A. Questionnaire

The survey consists of ten parts, covering various aspects of password management and experiences with PMs. The full questionnaire can be found in Appendix VII-C.

1. Informed Consent: Participants were first provided with an overview of the study, the requirements for participation (i.e., being affiliated with USC), the estimated completion time which is between 15 and 20 minutes, and the raffle.

2. Password Management Strategies: We provided participants with a list of different password management strategies (e.g., memorizing, using browser PMs, writing passwords on paper, etc.) and asked them to use sliders to indicate the percentage of their passwords stored with each strategy. The total percentage can exceed 100%, as users may employ multiple strategies to store one password. The original study used multiple-answer checkboxes for this question. Our modified format allowed us to measure how much participants relied on each password storage. This modification maintains conceptual equivalence with the original measure while improving measurement resolution and clarity, and still allows mapping back to the original binary format. We then asked whether participants used a given password strategy, such as a browser PM, to make their passwords available across devices, using multiple-choice questions as was done in the original study.

3. University Account Password Management: We asked participants multiple-choice questions about their strategies for managing their USC account passwords. In the original study, some of these questions were free text. For ease of processing, we converted these questions into multiple-choice format, using the major themes identified in the original study as options. We added the option "Other" to each question, to allow for free-text responses. This modification operationalizes previously established qualitative findings into standardized measures, consistent with the approach used by Mayer et

al. [1] in deriving survey questions from Pearman et al. [13]. It enhances reliability and comparability across participants while directly testing whether the original thematic structure generalizes to a new sample. The inclusion of an "other" option allows participants to share new or unexpected ideas, while still keeping the survey questions consistent for all participants. Additionally, USC university requires all its account users to create passphrases, not passwords. We added 5-point Likert scale questions to measure participants' satisfaction with USC passphrase requirements.

4. General PM: Similar to [1], we asked participants where they first learned about PMs. We then provided 5-point Likert scale questions to measure user agreement with statements that PMs exhibit or create the following eight characteristics: *Security*, *Tranquility*, *Fun*, *Ease of Use*, *Difficulty*, *Annoyance*, *Transparency*, and *Trust* – questions that [1] derived from [16]. We asked participants again in this section if they use any PM, as an attention check. We discuss this in Section III-C.

5. PM Users: Participants who indicated any PM usage in Part 2 were directed to this survey section. We asked PM users about their experiences with PMs, such as their reasons for using them, the products they use, their satisfaction levels, and what they liked and dislike about PMs. These questions were derived from the original study with some modifications. For example, we converted some free-text questions into multiple-choice ones using themes identified in the original study and adding the "Other" option. We also rephrased certain multiple-choice questions that originally allowed a single response to allow multiple selections. We made this modification because some original questions did not fully reflect participants' experiences when more than one answer could apply. For example, participants may use multiple PM products or have multiple reasons for liking PMs, which would not be captured by the single-choice questions used in the original study. We added questions to gain deeper insight into how users relied on PMs for password generation.

6. Non-PM Users: Participants who did not use any PM were directed to this survey section. We asked non-PM users about their main reasons for not using PMs. In the original study, this question was asked as a free-text response. While we retained this free-text question, we also added a 5-point Likert scale for each reason identified in the original study's responses.

7. Free PM Adoption: We asked participants how likely they were to use a free PM if offered by their institution using a 5-point Likert scale, similar to the original study.[1] USC offers a free third-party PM to their users, unlike GWU. To measure user awareness of this offer, we asked them if they knew that USC offers 1Password subscription for free. In a separate question we asked users if they used 1Password or not. We added 5-point Likert scale questions to better understand participants' reasons for choosing to use or not use the free PM provided by USC, a topic that was not explored in depth in the original work.

[1]The original study used a 7-point scale. We mapped the 7-point responses to our 5-point scale using linear rescaling (Appendix VII-A).

8. IT Skills: We used the same set of questions from the original work, which were derived from the Web Skill Measure [58] and the SA-6 Security Attitude Measure [59], to assess participants' overall technical background. Both sets of questions were in the form of a 5-point Likert scale matrix.

9. Demographics: We asked participants about their demographics, including gender, age, ethnicity, and role at USC.

10. Raffle: We asked participants if they wanted to enter a $10 raffle, where one winner is selected for every ten participants.

B. Recruitment and Participant Demographics

We conducted our study with a university population at USC. Our survey was distributed to the USC community through several channels for exactly one month, from September to October 2025. During the first two weeks of recruitment, we advertised our survey via institutional Slack channels, each with thousands of members (one with more than 15,000 members), and posted 100 paper flyers around the campus. This approach had a low yield of under 100 valid responses. We then changed our recruitment strategy to distribute the survey via personalized emails, using Mail Merge option in MS Word coupled with Outlook. We compiled a list of 7,445 email addresses of USC employees, using public Web pages of different academic departments. Out of 7,445 contacts, we received 335 valid responses, resulting in a response rate of 5% (compared to GWU's 14% response rate using central email distribution system for recruitment). To collect student responses, we recruited student participants using the psychology department's subject pool. This pool consists of freshman and sophomore students enrolled in a class that requires survey participation for course credit.

Table I in Appendix VII-B summarizes the demographics of our participants. After removing low-quality responses (Section III-C), our USC sample includes 437 participants, which is greater than the original GWU sample of 277. A power analysis indicated that the total sample size (714) was sufficient to provide high power (>95%) to detect a medium effect (Cohen's w = .30) in a chi-square test of independence (df = 1 and α = .05), suggesting the adequacy of the sample size. Both USC and GWU skew toward younger participants (46% and 42% aged 18–35, respectively). Our sample includes a higher proportion of participants aged 18-25 (32%) compared to GWU (22%), which can be attributed to our intentional recruitment of freshman and sophomore students through the psychology department's subject pool. Our sample is more balanced in terms of gender between male (45%) and female (49%) than GWU, whose sample was predominantly female (65%). With regard to ethnicity, white participants still make up the largest proportion in both USC (42%) and GWU (61%). At USC, we have 23% Asian, 15% Hispanic and 3% Black participants, compared to GWU's 6% Hispanic, 11% Black and no separately reported Asian participants (presumably included under 14% of "Other"). With regard to participant's role in the institution, both studies have similar proportions of student participants (38% for USC and 33% for GWU), but different faculty and staff ratios (USC

study has 44% faculty and 19% staff, while GWU study has 21% faculty and 43% staff). For IT skills, USC participants have a slightly higher average Web Skill score (3.53) than GWU participants (3.35). With regard to the security attitude (SA-6), average SA-6 scores were similar between USC (3.36) and GWU (3.33). [2] This similarity suggests that both USC and GWU participants are comparable in terms of their IT skills.

C. Data Quality

We ensured data quality by removing incomplete responses and those that failed the attention check. Specifically, participants were asked twice if they used PMs – in Part 2 and Part 4 of the survey. We removed participants whose responses to these two questions were not consistent. Out of 619 responses, we excluded 151 incomplete responses and 31 failed attention checks, leaving 437 for data analysis.

D. Data Analysis

We report descriptive statistics as percentages, since the sample sizes in our study and the original work are different. To statistically compare these descriptive results, we used a chi-square test of independence with the count of users in a given group (e.g., PM users) as a dependent variable and the institution (USC vs GWU) as the independent variable.

We ran the same logistic regressions and the same pre-processing steps as Mayer et al. to validate the original findings on factors that associate with user awareness (Section IV-A) and usage of PMs (Section IV-C). Further details on which specific variables were selected for each logistic regression analysis can be found in Section IV-A and Section IV-C, and our exact approach to coding the variables for logistical regression is provided in Appendix VII-D.

We also compared responses between faculty, staff, and student populations, which were not explored in depth in the original work. For continuous dependent variables such as the percentage of unique passwords (Figure 4) and the percentage of random passwords generated by PMs (Figure 7), we used a one-way between-subjects ANOVA to test whether participant role is significantly associated with these variables, followed by planned contrasts comparing (Student vs. Staff), (Student vs. Faculty) and (Staff vs. Faculty) to determine which specific pairs differed significantly. For categorical dependent variables such as whether participants were aware of the free PM (Figure 12) and whether they used the free PM (Figure 13), we used a chi-square test of independence. If the chi-square test was significant, we performed post-hoc pairwise comparisons using separate chi-square tests for each pair of groups, with Bonferroni-corrected significance thresholds ($\alpha = .05/3 = .017$) to account for multiple comparisons [60].

E. Ethical Considerations

Our study was approved by our Institutional Review Board (IRB) as exempt. Participation in our study was anonymous. Optionally, participants could choose to provide their email address for the $10 raffle. These emails were stored separately from survey responses, and were deleted after the raffle.

F. Limitations

As a replication study, our work shares inherent limitations with the original study. It faces common challenges of online surveys, such as self-selection bias, reliance on self-reported data, and potential misinterpretation of questions by participants. Individuals with greater familiarity with passwords and PMs, or stronger opinions on the topic, are more likely to participate in the study than those who are less interested, making our results on some questions, such as awareness, a likely upper bound. Additionally, to ensure a fair comparison with the original study, it was important for our replication's participant distribution to closely match that of the original study. While the overall distribution between student (38%) and non-student participants (63%) in our study closely aligns with the original work (33% students and 64% non-students), the breakdown within the non-student group differs (Table I, 44% faculty / 19% staff in ours vs 21% faculty / 43% staff in the original). Matching participant population distribution perfectly was challenging due to practical constraints such as voluntary participation, limited access to population data, and differences in response rates across subgroups. However, these differences in population distributions provided an opportunity to examine whether the original findings generalize to a different population. Our study also addresses some previous limitations of the original work, particularly regarding participant diversity, as our sample is more balanced in terms of gender and more diverse in terms of ethnicity (more non-white participants). Both our study at USC and the original study at GWU occured at US educational institutions, which means our findings may not generalize to other types of institutions or other countries. We modified some questions from free-text to multiple-choice formats, which simplified the measurement but limited richer insights.

IV. Results

In this section, we present our findings, organized in order of the research question (RQs).

A. RQ1: Awareness

Figure 14 in Appendix VII-E shows how participants first learned about PMs, and compares our findings with Mayer et al. At USC, 4% of participants were unaware of PMs before the study, compared to 9% at GWU. The majority of participants in both universities did not recall how they first learned about PMs. A *chi*-square test shows that USC participants were significantly more aware of PMs than GWU participants ($\chi^2 = 5.53, p = .02$). We ran the same logistic regression as the original study to determine which factors (SA-6 score, Web Skill score, gender, age) were associated with participants' awareness of PMs. Our results show that both web skills and age were significantly associated with participants' awareness of PMs ($OR_{\text{web skill}} = 2.43$, $p < .01$;

[2] We had to correct this measure from the original paper (Appendix VII-B).

$OR_{\text{age}} = 1.06$, $p = .03$). For each one-point increase in the web skill score, participants were $2.43\times$ more likely to be aware of PMs, and for every one-year increase in age, they were $1.06\times$ more likely to be aware of PMs. These results align with the original findings about web skill, but the original study did not find that age correlated with user awareness.

B. RQ2: Password Strategies

Figure 1 illustrates participants' use of different password management strategies at USC and at GWU. Since we measured password management strategy usage with sliders, any positive response for a given strategy meant that a given participant used that strategy. In terms of the most commonly used strategies, USC participants reported remembering passwords (98%), using any PM (94%), and using a browser PM (77%) as their primary methods for managing passwords, consistent with GWU participants. We further found that, for every strategy, the percentage at USC was significantly higher than at GWU ($22.32 \leq \chi^2 \leq 288.67$, $p < .001$), except for paper or physical media. This may suggest an increasing trend in PM usage over the past years or a significant difference between our participant populations. Another difference between our and Mayer et al.'s findings lies in reported use of forget-and-reset strategy (75% in our study, 10% in Mayer et al.'s study, $\chi^2 = 288.67, p < .001$). Such a large difference is unlikely between two very similar participant populations. Instead, we believe that the difference stems from differences in survey design. At GWU, participants were asked to select all password strategies they could recall at the moment. We prompted participants to consider each strategy individually, and reflect on whether they actually use it by indicating how many of their passwords are managed with that strategy. We hypothesize that this led to more complete reporting. Due to the low number of responses for non-PM users – only 6% – we report their results in Appendix VII-E.

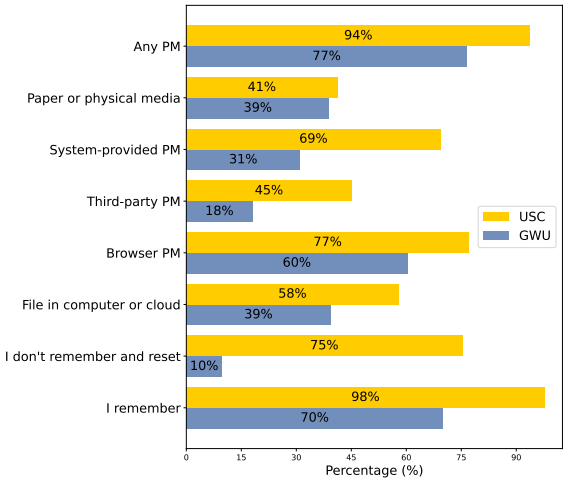

Fig. 1. Participants' use of different password management strategies.

Figure 2 shows the distribution of percentages of passwords that USC participants reported managing with each strategy – a dimension not explored in Mayer et al. [1]. Participants remembered a median of 50% of their passwords, while the remaining passwords were managed using browser PMs (40%), system-provided PMs (21%), or saved on a computer or in the cloud (5%). Despite these strategies, 10% of passwords had to be reset. This finding suggests that as the number of passwords increases, users rely on multiple management strategies, and may still fall back on password resets. This highlights the ongoing challenge of password management.

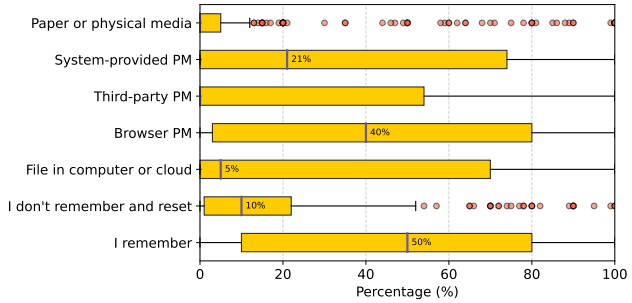

Fig. 2. Box plot of the percentages of passwords USC participants store with each password management strategy.

Figure 3 shows how users made their passwords available across devices at USC vs GWU. Our results are consistent with the original study. Most participants who used PMs also relied on its features to access passwords across devices. The order of common strategies matches at both institutions, with PM features being the most common (63-75% at USC), sync tools such as Google Drive or Dropbox next (43%), and manually copying password files being the least (24%). This consistent finding highlights the growing number of passwords and devices users manage, and emphasizes the importance of features that make passwords accessible across devices.

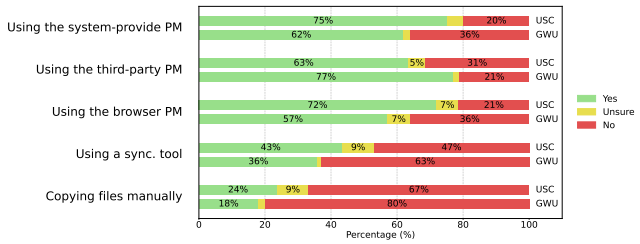

Fig. 3. Whether participants rely on their password management strategies to make their passwords available across devices.

The original study further investigated whether participants reused passwords and found that over 77% of users do so. In our study, we expanded the scope of this question to measure the fraction of each participant's passwords that were unique. Figure 4 illustrates the overall distribution of the proportion of unique passwords among USC participants, broken down by role (faculty, staff, and students). Participants had unique passwords for a median of 40% of their accounts, indicating that more than half of their passwords were reused. A one-way between-subjects ANOVA revealed a significant effect

of participant role on the proportion of unique passwords ($F(2, 434) = 32.92, p < .001$). Planned contrasts analysis further showed that students used significantly fewer unique passwords than staff ($t = -3.44, p < .001$) and faculty ($t = -8.50, p < .001$), and that faculty had significantly more unique passwords than staff ($t = 2.68, p = .008$). Since students are typically younger than staff and faculty, we hypothesized that age might be associated with the fraction of unique passwords participants have. A bivariate Pearson correlation supported this hypothesis, showing that age was significantly and positively correlated with the fraction of unique passwords ($r(411) = .39, p < .001$). This indicates that older participants tended to have a larger fraction of passwords that are unique. However, age was also significantly and negatively correlated with the fraction of passwords participants could remember ($r(411) = -.45, p < .001$), suggesting that older participants remembered fewer passwords. This decline in memory could be explained by password uniqueness, as the fraction of passwords remembered was significantly and negatively correlated with the fraction of unique passwords ($r(437) = -.39, p < .001$), meaning that participants who used more unique passwords tended to rely less on memory for password management. Thus, faculty remembered the smallest fraction of their passwords, followed by staff and students, respectively. We further explain this analysis in Appendix VII-E).

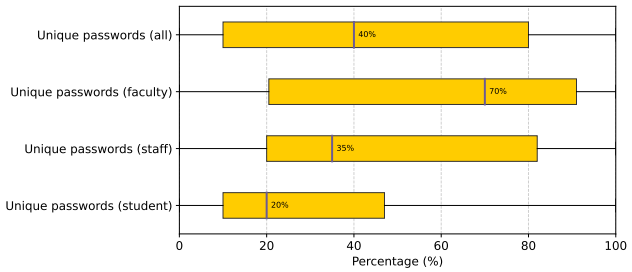

Fig. 4. Box plot of the percentages of unique passwords across all, faculty, staff, and student participants at USC.

C. RQ3: Password Manager Users

Figure 1 shows that 94% of USC participants used PMs, compared to 77% of GWU participants ($\chi^2 = 43.61, p < .001$). Since our study was conducted four years after the original work, it is possible that PM usage naturally increased over time. Of the 94% of PM users (410/437), 76% used multiple PM types (311/410), consistent with Oesch et al.'s finding that many users now employ multiple PM types, often using one as a backup for another [51]. In terms of PM types, USC participants most commonly used browser PMs (77%), followed by system-provided PMs (69%), with third-party PMs being the least (45%), consistent with the order observed at GWU. In Appendix VII-E, Figure 19 shows the PM products used by participants. In our study, USC participants could select all PM products they use, whereas in the original study, participants selected only the PM they used most. Consequently, unlike GWU, the percentages for USC PM usage do not sum to 100%. The most popular PM products at both universities were consistent, with Chrome and Apple Keychain being the most commonly used. Overall, participants from both universities were satisfied with PMs (Figure 20), with 87% of USC and 94% of GWU participants indicating satisfaction at or above "slightly satisfied" with PMs.

With regard to reasons for PM usage (Figure 21 in Appendix VII-E), our findings align with GWU: users used PMs mainly for managing passwords across devices (76%), autofilling passwords (80%), remembering them (77%), and secure storage (60%). We then ran the same logistic regression as the original study to determine which factors (SA-6 score, Web Skill score, the eight aspects of PM usability, participant role and university account security – Section III-A Part 4, 8, and 9, plus Appendix VII-D) were associated with PM use. We found that ease of use of PMs was significantly associated with PM use ($OR_{\text{ease of use}} = 3.49$, $p = .02$), meaning that participants were $3.49\times$ more likely to use PMs when they perceived that PMs were easy to use. This is consistent with the original study: a participant was $14.53\times$ more likely to use PMs if they perceived them as easy to use ($p < .001$). In addition, the original study found that participants were $1.15\times$ more likely to use PMs if they understood how PMs work ($p = .047$), while our analysis did not find significant association between these variables in our population. This difference may be due to passage of time, which increased awareness of PMs and their design. Thus, the effect of ease of use on PM use is smaller, though it remains significant, while transparency, which previously barely passed the significance threshold, is now no longer a significant predictor.

Next, we examined whether participants used PMs to generate their passwords. Figure 5 shows that 26% of our USC participants use PMs to generate passwords, which is consistent with 20% reported at GWU. Additionally, our study used a 5-point Likert scale to measure how frequently participants used PMs to generate their passwords (Figure 6). We found that 58% of our participants have used PMs to generate their passwords at least occasionally (≥Sometimes), and 26% have used them regularly (≥Most of the time), matching the exact use percentage in Figure 5. This suggests that the original study may have underestimated PM use for password generation, because it asked only about most common approach participants employed for password generation, while we allowed for multiple responses to cover all strategies.

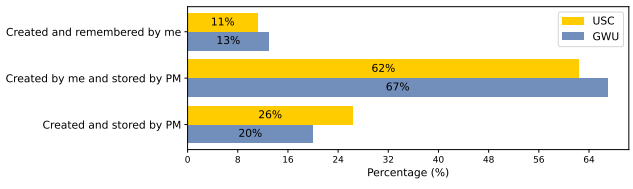

Fig. 5. How PM users create and store their passwords.

We further explored why participants used PMs to generate their passwords (Figure 22 in Appendix VII-E). We found

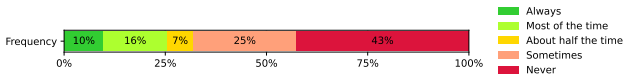

Fig. 6. Frequency of using PM to generate passwords.

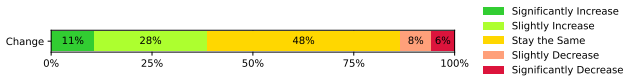

Fig. 8. Change in the use of PMs to generate random passwords over time.

that 30% reported no specific reason for using this feature, while 34% used it primarily when prompted to change their passwords. Importantly, participants were unlikely to use PMs to generate passwords for high-security accounts (15%) or frequently used accounts (5%). This suggests that users still preferred to memorize passwords for accounts they considered important or used often, rather than adopting stronger, randomly generated passwords. Figure 7 specifically shows that participants had random passwords generated by PMs for a median of only 10% of their accounts, reemphasizing that users prefered passwords they can remember for the majority of their accounts. Across different roles, we observed that faculty participants had the highest usage of PMs for password generation, consistent with Figure 4, where faculty participants also had the highest fraction of unique passwords. A one-way between-subjects ANOVA revealed a significant effect of participant role on the proportion of passwords generated by PMs ($F(2, 353) = 17.41, p < .001$)[3]. Planned contrasts analysis further showed that faculty had significantly higher portion of passwords generated by PMs than staff ($t = 3.04, p = .003$) and students ($t = 5.84, p < .001$). This suggests that faculty have more unique passwords because they rely more on PM-generated passwords than staff and students. We also asked participants how they expected their use of PMs for generating random passwords to change over time. Figure 8 shows that nearly half of participants (48%) expected their use of PMs for password generation to stay the same, while 39% believed they would use them more. We exect that the overall use of PMs for password generation will continue to increase over time, as users create more password-protected accounts.

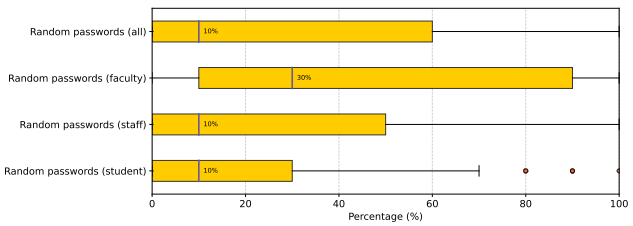

Fig. 7. Box plot of the percentages of random passwords generated by PMs across all, faculty, staff, and student participants at USC.

We asked participants what they liked about PMs and what concerns they had about them (Appendix VII-E). Unlike the original work, which only asked participants to choose the main aspect they liked or were concerned about, we allowed for multiple answers. Figure 23 shows that 83% of participants liked the PM feature that auto-fills their passwords, 78% liked that they did not have to memorize passwords, and 63% liked the ability to synchronize passwords across devices. On the other hand, Figure 24 shows that 41% of participants had security concerns about PMs, 30–37% were concerned about PMs not working correctly in different situations, and 35% were concerned about losing the master password. These rankings of the most liked and most concerning aspects of PMs are consistent with the original study's findings.

D. RQ4: University Password Strategies

Similar to the original study, we asked participants to rate the security of their university account passwords compared to their other passwords (Figure 25 in Appendix VII-E). 94% of USC participants reported that their university account passwords were at least as secure as their other passwords, significantly higher than 83% at GWU ($\chi^2 = 21.25, p < .001$). Moreover, 59% of USC participants rated their university passwords as more secure than their other passwords, compared to 36% at GWU ($\chi^2 = 35.18, p < .001$). These results suggest that participants perceive their university accounts as important, reflected in their use of more secure passwords.

Additionally, we asked participants to rate their satisfaction with the USC passphrase requirements (Figure 9). Participants were most dissatisfied (≤Somewhat dissatisfied) with the requirement to make their passwords 16-64 characters in length (45%). Participants were generally satisfied (64–90%) with requirements of not reusing previous passwords, updating the password annually, and not including their username in the password. To better understand how participants managed their USC university passphrase, we asked how they created it for the first time (Figure 26) and the strategies they used to update their passphrase annually (Figure 27) in Appendix VII-E. We offered several plausible answers to each question and allowed users to select all that applied. Consistent with the original work, which measured these using free text, two of the main strategies participants employed when creating their university account password/passphrase were using memorable phrases (50%) and reusing passwords (42%) with strategic modifications. 40% reported creating brand-new passphrase using their own secret patterns. Participants also showed signs of security awareness, with only 13–14% using personal information in their passphrase or reusing exact passwords from other accounts, and 15% using PMs to generate random passphrases. For passphrase updates, the most commonly used strategies were replacing or rotating characters (49%) and adding different endings to a current passphrase (38%). Specifically, 12% used a counter and 9% included a date in their passphrase, which they could update when a passphrase change was required. 18% used PMs to update

[3]Out of 410 PM users, we received 356 responses, giving the total degree of freedom of 355. Ideally, all PM users would have answered this question, but because we forgot to mark it as required, some responses were missing.

new passphrases, and 13% selected new passphrases from a list of passphrases they frequently used. These results indicate that users favored memorable passwords for their university accounts. This aligns with our explanation in Section IV-C, where we discussed that users prefered memorable passwords over random ones generated by PMs for frequently used accounts. University accounts fall into this category, which explains the strong preference for memorable passwords.

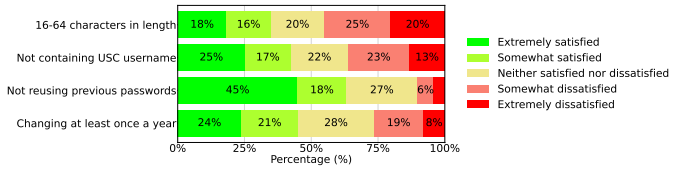

Fig. 9. Satisfaction with USC passphrase requirements.

E. RQ5: Free PM Adoption

Given that USC offered a free 1Password subscription to its community, we examined not only participants' likelihood to adopt the free PM, but also their actual usage and perceptions. This extends the original study, which only asked about the likelihood of adoption. Figure 10 shows that 48% of PM users at USC were likely (≥Somewhat likely) to adopt the free PM, which is significantly lower than the 71% of PM users at GWU in the original study ($\chi^2 = 28.90, p < .001$). Similarly, In Figure 11, 26% of non-PM users at USC were likely to adopt the free PM, which is significantly lower than the 56% of non-PM users at GWU ($\chi^2 = 5.52, p = .019$). At USC, PM users were significantly more likely to adopt the free PM than non-PM users ($\chi^2 = 4.04, p = .045$). A similar pattern was also observed at GWU ($\chi^2 = 4.65, p = .031$).

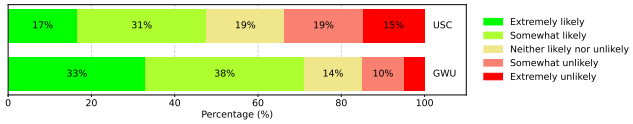

Fig. 10. Likelihood of PM users adopting a university-provided free PM.

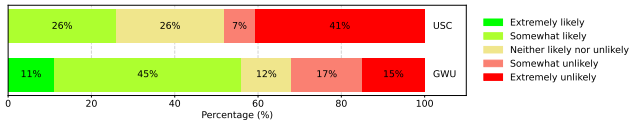

Fig. 11. Likelihood of non-PM users adopting a university-provided free PM.

To further examine actual usage, we first asked participants whether they were aware that USC offered a free 1Password subscription, followed by whether they used this free PM. Figure 12 shows that only 35% of USC participants were aware of the free 1Password subscription. In particular, fewer students (22%) were aware of the free PM compared to faculty (41%) and staff (47%). A *chi*-square test showed that participant role was significantly associated with participants' awareness of the free PM ($\chi^2 = 19.38, p < .001$). Post-hoc *chi*-square tests further revealed that students were significantly less aware of the free PM than faculty ($\chi^2 = 12.90, p < .001$) and staff ($\chi^2 = 14.24, p < .001$). Correspondingly, actual free PM usage was even lower than awareness. Figure 13 shows that only 15% of USC participants actually used the free PM. A *chi*-square test shows no significant differences among participant roles ($\chi^2 = 4.14, p = .126$), suggesting that the low usage of the free PM is consistent regardless of whether participants are employees or students.

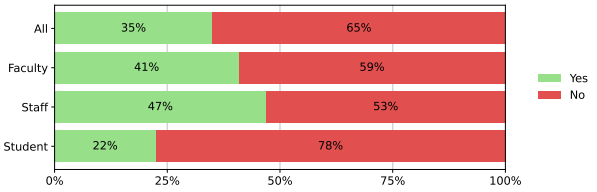

Fig. 12. Do participants know that USC offers the free PM (1Password)?

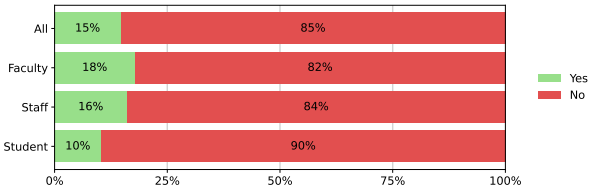

Fig. 13. Do USC participants use the free PM (1Password)?

To better understand why participants did not use the free PM, we provided a set of potential reasons and asked them, on a 5-point Likert scale, how strongly they agreed with each reason (Figure 28 in Appendix VII-E). We found that the main reasons participants chose not to use the free PM were satisfaction with their current password management (74% of participants agreed – indicated "Strongly agree" or "Somewhat agree") and concern around losing access to the free PM once they were no longer affiliated with USC (67% agreed). Additionally, 51% of participants felt that switching their password management methods would be difficult and troublesome. This unwillingness to adopt the free PM is also supported by the fact that only 24% of those who are currently not using the free PM reported that they would actually want to use it, and just 28% thought it would be a good idea if the free PM were set up by default with their university account. We also asked participants who used the free PM (1Password) about their experience, using a 5-point Likert scale (Figure 29 in Appendix VII-E). 87% were satisfied with 1Password, and 84% would recommend it to others who have never used it. Only 31% found 1Password challenging to learn at first. These results suggest that users generally had a positive experience with 1Password. Overall, our results indicate that low awareness of the free PM offering and satisfaction with the current password management strategies are the main reasons for low adoption of the free PM at USC.

V. Discussion

We discuss the implications of our findings in this section and offer recommendations and directions for future research.

A. Main Implications

Awareness. Our results support prior findings that show an increased awareness of PMs. In 2016, Alkaldi et al. reported that only 50% of their participants correctly understood what a PM were [11]. Mayer et al. reported that 91% of university participants were aware of PMs in 2021 [1], and our study found 96% awareness at USC in 2025. This reflects a substantial rise of PM awareness over the past decade, which also appears to drive higher PM usage.

Password Strategies. Our results support prior findings showing that PM usage continues to increase: Alkaldi et al. (2016) find PM usage among 18% of participants [11], Mayer et al. (2021) among 77% [1], and we (2025) find it among 94% of participants. We extend previous findings that 43–77% of users reuse passwords [1], [7] by showing that only 40% of each user's account passwords are unique, meaning that more than half are reused. In our study, age and participant role at USC were significantly correlated with the fraction of their passwords that were unique, with older users and faculty having a higher fraction of unique passwords. We hypothesize that this pattern may be specific to our university sample, where older users, mostly faculty, are more security-aware than younger users, who are primarily undergraduates, and therefore tend to reuse passwords. This aligns with Theofanos et al. [61], who found that adults manage significantly more passwords than children, as younger users exhibit misconceptions about passwords and poorer security practices (e.g., sharing passwords, reusing them, and using personal information).

PM Users. Our results further extend prior findings. We not only show the upward trend in PM usage, but also find that, among the 94% of PM users, 76% actually used multiple types of PMs, supporting Oesch et al.'s finding that many users now employ multiple PM types, often using one as a backup for another [51]. Browser PMs remain the most commonly used among users [1], [19] and convenience remains a key factor driving PM adoption [1], [12], [13], [19], [48]. Previous studies reported low usage of third-party PMs [13], [14], which may be due to their reported poor usability [56]. Our results show that 45% of USC participants used third-party PMs. This proportion may be partly explained by the fact that USC provides free third-party PM subscriptions. However, only 15% of our participants adopted the free PM, meaning that the remaining 30% used their own personal subscription to third-party PMs. This 30% is still substantially higher than the 18% reported by Mayer et al. [1], suggesting continued growth in third-party PM adoption. Additionally, previous studies have reported low adoption of PMs' password-generation features [1], [13], [14]. Our results show a similar pattern: only 26% of participants used the feature regularly, although 58% have used it at least occasionally. Responses to our additional questions revealed that the main reason for this low use of PMs for password generation is users' desire for memorable passwords, especially for accounts that are important and used frequently. This preference is understandable given previous findings of usability issues with PMs' password generation, including websites rejecting generated passwords due to composition policies [44], [45] and the difficulty of entering or recalling generated passwords when PMs are unavailable [51]. We provide recommendations for increasing use of PMs for password generation in Section V-B.

University Password Strategies. Our results support prior findings. Specifically, 59% of participants perceived their university account passphrase as more secure than their other passwords, a substantial increase compared to the 36% reported by Mayer et al. at GWU [1]. This difference may be interpreted in two ways. First, users may increasingly view their university accounts as important, leading more of them to create stronger-than-usual passwords. Second, the higher proportion at USC may be due to its password-creation policies (PCPs), which differ from those at GWU. USC uses PCPs that require a minimum length of 16 characters and has no character composition requirement, whereas GWU requires a minimum of 8 characters with at least one uppercase letter, one lowercase letter, one number, and one special character [62]. Both prohibit the reuse of previous passwords and the inclusion of the username in the password. Prior work has shown that PCPs requiring only longer passwords produce significantly stronger passwords than those with more complex composition rules and shorter length requirements, while also offering better usability [32], [33], [34]. In other words, USC's PCPs likely help users create passphrases that are stronger, as reflected in the higher proportion of participants who believe that their university passphrase is stronger than their other passwords. Additionally, both USC and GWU users primarily relied on personal strategies such as using memorable phrases or reusing existing passwords to create their university passwords. At USC, users typically updated passwords by replacing characters or modifying password endings. Zhang et al. [21] documented these same behaviors 15 years ago, and we find that they remain prevalent.

Free PM adoption. Our results refute the hypothesis offered in Mayer et al. [1] that users would likely adopt a third-party PM if offered for free. We find that our participants had low awareness of the free PM (35%), and even lower adoption (15%). Even after being made aware of the free PM during the study, only 24% of participants who were not currently using it expressed interest in adoption. Even among staff (16%) and faculty (18%), adoption of the free PM remained relatively low. The most common reasons for this lack of adoption were satisfaction with current password management strategies and the expectation that switching to a new PM may not be worth the effort. Munyendo et al. found that, despite most PMs offering features to transfer credentials in bulk, users still relied largely on manual efforts when switching between PMs, such as copying and pasting credentials, and received limited guidance during the process [19]. This result emphasizes that switching from one PM to another is a challenging process.

B. Recommendations and Future Research

Based on our findings, we offer the following recommendations to increase use of PMs.

Increasing Use of Password Generation. Our results show that password memorability is highly important to users. As a result, increasing the use of password generation largely depends on whether the generated passwords are practical to use – that is, both secure and memorable. PMs that are most used by users, such as browser-based and OS-based PMs, generate strong random passwords by default but offer little or no support for generating more memorable passwords. Although a few third-party PMs, such as 1Password and LastPass, have provided memorable password generation, it is understandable that many users may remain unaware of this alternative. Increasing the use of password generation thus requires more than simply offering the feature. First, memorable password generation should be made available in widely deployed PMs, not only in third-party tools that are more commonly used by tech-savvy users. Second, this feature must be carefully studied to ensure a balance between memorability and security, as improving memorability may weaken passwords and research in this area is currently limited [63]. Additional user studies are needed to better understand what makes passwords memorable, alongside technical security research to evaluate whether such passwords remain sufficiently strong. Together, these efforts are necessary to identify an appropriate middle ground. Third, the feature must be easy to access and intuitive to use. Users must not only be aware that memorable password generation exists, but also be able to select and use it with minimal effort. Prior research about security and privacy tools on social media suggests that even when users are aware of available protections, effective use is often hindered by poor usability and by tools being hard to find within the interface [64]. Therefore, making the feature easy to find and use is essential for increasing adoption.

Broadening Adoption of Free, Third-Party PMs. Although USC has promoted the free PM through multiple channels, such as emails, Slack messages, and required security training for employees, our results suggest that both awareness and adoption remain low. We found that the main reasons behind this low adoption are users' satisfaction with their current password management practices, the perceived difficulty of switching, and the concern of losing access to the free PM if they leave the university. To increase adoption, institutions should first focus on improving user awareness of the free PM offering. Promotion efforts should move beyond passive campaigns and instead provide timely and meaningful nudges – for example, recommending the PM during account creation, password resets, or after security incidents – when users are more likely to pay attention and recognize its value. Promoting the free PM at these moments also helps highlight the added benefits of a subscription-based, third-party PM offered at no cost. For example, when users reset a compromised password or respond to a security alert, institutions can emphasize features that are often unavailable in browser- or OS-based PMs, such as memorable password generation. Once users are aware of the PM and motivated to try it, institutions must ensure that they feel confident that adoption will be easy and low-effort. Institutions should therefore emphasize the simplicity of migrating from existing password management solutions. This can be supported through seamless onboarding at key moments, such as when users first join the institution, by providing guided password import workflows from browser-based and commonly used PMs, along with concise, step-by-step instructions that minimize user effort. Third, concerns about losing access after leaving the institution should be addressed early by clearly communicating exit options as part of promoting the free PM. Informing users upfront that their password vaults can be seamlessly transferred to personal accounts can help reduce fears of losing access. These concerns can be further mitigated by offering clear exit options at the time of departure, such as providing explicit, step-by-step instructions for transferring password vaults to personal accounts as part of the offboarding process.

Future Replication. Both our replication and the original study focus exclusively on universities as institutional settings, and only on universities in the US. Other types of institutions, such as businesses, hospitals, or government organizations, may employ different security training, practices, and policies. Similarly, institutions in other countries may operate under different cultural expectations or regulatory frameworks. Replicating this work across a broader range of institutional contexts and geographic regions would therefore help assess the generalizability of these findings. In addition, both studies rely primarily on quantitative data. While this approach is effective for identifying broad trends, future research would benefit from incorporating qualitative methods, such as interviews or open-ended survey questions, to gain deeper insight into users' motivations, concerns, and decision-making around password management in institutional settings. For example, in Figure 24 in Appendix VII-E, users identify security as their primary concern with PMs. Qualitative follow-up could help clarify what specific security issues users are referring to, such as concerns about the strength of generated passwords, password storage mechanisms, or other aspects of PM design.

VI. Conclusion

We replicated Mayer et al.'s study [1] measuring password habits and password manager (PM) usage at our large private university. We found results consistent with the original study, including prevalent awareness and use of PMs, low usage of PMs for password generation, and widespread password reuse – with the extent of reuse being a novel finding. We also found a contradictory result: users were unlikely to adopt a free third-party PM offered by the institution. Additionally, their awareness and actual usage of the free PM were relatively low. Finally, our results highlight opportunities for improvement in terms of increasing password-generation usage and broadening adoption of the free third-party PM offered by the institution, for which we provide recommendations.

REFERENCES

[1] P. Mayer, C. W. Munyendo, M. L. Mazurek, and A. J. Aviv, "Why users (don't) use password managers at a large educational institution," in *USENIX Security*, 2022.

[2] C. Herley and P. Van Oorschot, "A research agenda acknowledging the persistence of passwords," *IEEE S&P*, 2012.

[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in *WWW*, 2007.

[4] A. Hanamsagar, S. S. Woo, C. Kanich, and J. Mirkovic, "Leveraging semantic transformation to investigate password habits and their causes," in *CHI*, 2018.

[5] E. Stobert and R. Biddle, "The password life cycle," *ACM Transactions on Privacy and Security (TOPS)*, 2018.

[6] R. Wash, E. Rader, R. Berman, and Z. Wellmer, "Understanding password choices: How frequently entered passwords are re-used across websites," in *SOUPS*, 2016.

[7] A. Das, J. Bonneau, M. C. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *NDSS*, 2014.

[8] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, ""i added '!' at the end to make it secure": Observing password creation in the lab," in *SOUPS*, 2015.

[9] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, "Do users' perceptions of password security match reality?" in *CHI*, 2016.

[10] A. Nisenoff, M. Golla, M. Wei, J. Hainline, H. Szymanek, A. Braun, A. Hildebrandt, B. Christensen, D. Langenberg, and B. Ur, "A Two-Decade retrospective analysis of a university's vulnerability to attacks exploiting reused passwords," in *USENIX Security*, 2023.

[11] N. Alkaldi and K. Renaud, "Why do people adopt, or reject, smartphone password managers?" in *EuroUSEC*, 2016.

[12] S. Klivan, S. Höltervennhoff, N. Huaman, Y. Acar, and S. Fahl, ""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 *SOUPS*, 2023.

[13] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, "Why people (don't) use password managers effectively," in *SOUPS*, 2019.

[14] S. G. Lyastani, M. Schilling, S. Fahl, M. Backes, and S. Bugiel, "Better managed than memorized? studying the impact of managers on password strength and reuse," in *USENIX Security*, 2018.

[15] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: user attitudes and behaviors," in *SOUPS*, 2010.

[16] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin, ""it's not actually that horrible": Exploring adoption of two-factor authentication at a university," in *CHI*, 2018.

[17] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur, "Measuring password guessability for an entire university," in *CCS*, 2013.

[18] M. Ariana, H. Grant, S. Stefan, and V. Geoffrey M., "An empirical analysis of enterprise-wide mandatory password updates," in *ACSAC*, 2023.

[19] C. W. Munyendo, P. Mayer, and A. J. Aviv, ""i just stopped using one and started using the other": Motivations, techniques, and challenges when switching password managers," in *CCS*, 2023.

[20] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, and R. Shay, "Measuring Real-World accuracies and biases in modeling password guessability," in *USENIX Security*, 2015.

[21] Y. Zhang, F. Monrose, and M. K. Reiter, "The security of modern password expiration: an algorithmic framework and empirical analysis," in *CCS*, 2010.

[22] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "How does your password measure up? the effect of strength meters on password creation," in *USENIX Security*, 2012.

[23] J. Amador, Y. Ma, S. Hasama, E. Lumba, G. Lee, and E. Birrell, "Prospects for improving password selection," in *SOUPS*, 2023.

[24] K. Lee, S. Sjöberg, and A. Narayanan, "Password policies of most top websites fail to follow best practices," in *SOUPS*, 2022.

[25] R. Shay, L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, M. L. Mazurek, W. Melicher, S. M. Segreti, and B. Ur, "A spoonful of sugar? the impact of guidance and feedback on password-creation behavior," in *CHI*, 2015.

[26] S. Alroomi and F. Li, "Measuring website password creation policies at scale," in *CCS*, 2023.

[27] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *CHI*, 2010.

[28] D. Florêncio and C. Herley, "Where do security policies come from?" in *SOUP*, 2010.

[29] P. Mayer, J. Kirchner, and M. Volkamer, "A second look at password composition policies in the wild: Comparing samples from 2010 and 2016," in *SOUPS*, 2017.

[30] S. Sahin, S. A. Roomi, T. Poteat, and F. Li, "Investigating the password policy practices of website administrators," in *IEEE S&P*, 2023.

[31] A. Gautam, S. Lalani, and S. Ruoti, "Improving password generation through the design of a password composition policy description language," in *SOUPS*, 2022.

[32] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password-composition policies," in *CHI*, 2011.

[33] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Can long passwords be secure and usable?" in *CHI*, 2014.

[34] ——, "Designing password policies for strength and usability," *ACM Transactions on Information and System Security (TISSEC)*, 2016.

[35] N. Woods and M. Siponen, "Questioning a security assumption: Are unique passwords harder to remember than reused or modified passwords?" *Computers & Security*, 2025.

[36] E. Kim, K. Lee, D. Kim, and H. Kim, "Open sesame! on the security and memorability of verbal passwords," in *IEEE S&P*, 2025.

[37] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *IEEE S&P*, 2012.

[38] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *CCS*, 2010.

[39] D. L. Wheeler, "zxcvbn: Low-Budget password strength estimation," in *USENIX Security*, 2016.

[40] Y. Abdrabou, Y. Abdelrahman, M. Khamis, and F. Alt, "Think harder! investigating the effect of password strength on cognitive load during password creation," in *CHI EA*, 2021.

[41] D. McCarney, D. Barrera, J. Clark, S. Chiasson, and P. C. van Oorschot, "Tapas: design, implementation, and usability evaluation of a password manager," in *ACSAC*, 2012.

[42] E. Stobert and R. Biddle, "A password manager that doesn't remember passwords," in *Proceedings of the 2014 New Security Paradigms Workshop (NSPW)*, 2014.

[43] S. Chiasson, P. van Oorschot, and R. Biddle, "A usability study and critique of two password managers," in *USENIX Security*, 2006.

[44] N. Huaman, S. Klivan, M. Oltrogge, Y. Acar, and S. Fahl, "They would do better if they worked together: The case of interaction problems between password managers and websites," in *IEEE S&P*, 2021.

[45] S. Oesch and S. Ruoti, "That was then, this is now: A security evaluation of password generation, storage, and autofill in Browser-Based password managers," in *USENIX Security*, 2020.

[46] Z. Li, W. He, D. Akhawe, and D. Song, "The Emperor's new password manager: Security analysis of web-based password managers," in *USENIX Security*, 2014.

[47] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, "Password managers: Attacks and defenses," in *USENIX Security*, 2014.

[48] M. Fagan, Y. Albayram, M. M. Khan, and R. Buck, "An investigation into users' considerations towards using password managers," *Human-centric Computing and Information Sciences*, 2017.

[49] P. A. Cabarcos and P. Mayer, "'the more accounts i use, the less i have to think': a longitudinal study on the usability of password managers for novice users," in *SOUPS*, 2025.

[50] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, "Why older adults (don't) use password managers," in *USENIX Security*, 2021.

[51] S. Oesch, S. Ruoti, J. Simmons, and A. Gautam, ""it basically started using me:" an observational study of password manager usage," in *CHI*, 2022.

[52] A. Ponticello, F. Sharevski, S. Anell, and K. Krombholz, "How blind and low-vision users manage their passwords," in *CCS*, 2025.

[53] J. Dutson, D. Allen, D. Eggett, and K. Seamons, "Don't punish all of us: Measuring user attitudes about two-factor authentication," in *EuroS&PW*, 2019.

[54] D. Arnold, B. Blackmon, B. Gibson, A. G. Moncivais, G. B. Powell, M. Skeen, M. K. Thorson, and N. B. Wade, "The emotional impact of multi-factor authentication for university students," in *CHI EA*, 2022.
[55] I. Becker, S. Parkin, and M. A. Sasse, "The rewards and costs of stronger passwords in a university: Linking password lifetime to strength," in *USENIX Security*, 2018.
[56] S. Seiler-Hwang, P. Arias-Cabarcos, A. Marín, F. Almenares, D. Díaz-Sánchez, and C. Becker, ""i don't see why i would ever want to use it": Analyzing the usability of popular smartphone password managers," in *CCS*, 2019.
[57] Qualtrics, "Understand every customer. act when it counts," December 2025. [Online]. Available: https://www.qualtrics.com/
[58] E. Hargittai and Y. P. Hsieh, "Succinct survey measures of web-use skills," *Social Science Computer Review*, 2012.
[59] C. Faklaris, L. Dabbish, and J. I. Hong, "A self-report measure of end-user security attitudes (sa-6)," in *SOUPS*, 2019.
[60] R. A. Armstrong, "When to use the bonferroni correction," April 2014. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/24697967/
[61] M. Theofanos, Y.-Y. Choong, and O. Murphy, "'passwords keep me safe' – understanding what children think about passwords," in *USENIX Security*, 2021.
[62] GWU, "Reset your password," December 2025. [Online]. Available: https://it.gwu.edu/reset-your-password
[63] M. Clark, G. L. Snow, and K. Seamons, "Choose from a list: A user study of random password memorability," in *CHI*, 2025.
[64] P. Charnsethikul, A. Zunquti, G. Lucas, and J. Mirkovic, "Navigating social media privacy: Awareness, preferences, and discoverability," in *PETS*, 2025.

VII. Appendix

A. Linear Rescaling

We convert a 7-point scale to a 5-point scale by keeping the endpoints and the midpoint the same ($1 \rightarrow 1$, $4 \rightarrow 3$, $7 \rightarrow 5$) and grouping the remaining values to the nearest scale points (2 and $3 \rightarrow 2$, 5 and $6 \rightarrow 4$).

B. Demographics

We have noticed a discrepancy in the original paper. Specifically, we derived the SA-6 question for our survey from the original paper's appendix, which presented the question in a 5-point Likert scale. However, based on the original work's artifact (https://github.com/gwusec/2022-USENIX-Password-Managers/), this question was actually measured on a 7-point Likert scale. As a result, we cannot directly compare the average SA-6 score reported in the original paper (4.47) with our SA-6 score, as they are on different scales. To fix this, we applied the linear rescaling above (Appendix VII-A) to convert the original SA-6 scores to a 5-point scale before averaging them. After rescaling (Table I), the average SA-6 scores are similar between USC (3.36) and GWU (3.33). The similarity in both SA-6 and Web Skill scores suggests that USC and GWU participants are comparable in terms of their IT skills.

TABLE I
Demographics of the USC participant sample (n=437) and the GWU participant sample (n=277).

	Num. (%)	
	USC	**GWU**
Gender		
Male	198 (45%)	86 (31%)
Female	216 (49%)	181 (65%)
Non-binary	9 (2%)	2 (1%)
Prefer not to say	14 (3%)	8 (3%)
Age		
18-25	142 (32%)	62 (22%)
26-35	62 (14%)	53 (19%)
36-45	78 (18%)	42 (15%)
46-55	61 (14%)	43 (16%)
56-65	40 (9%)	26 (9%)
65+	27 (6%)	6 (2%)
Prefer not to say	26 (6%)	45 (16%)
Ethnicity		
African American or Black	14 (3%)	30 (11%)
Asian or Pacific Islander	102 (23%)	-
Hispanic or Latino	65 (15%)	16 (6%)
White or Caucasian	185 (42%)	168 (61%)
Middle Eastern or North African	20 (5%)	-
Native American or Indigenous	1 (0%)	-
Mixed race	17 (4%)	-
Other	5 (1%)	40 (14%)
Prefer not to say	28 (6%)	23 (8%)
Position		
Faculty/Leadership	191 (44%)	58 (21%)
Staff	81 (19%)	118 (43%)
Student	165 (38%)	91 (33%)
Prefer not to say	0 (0%)	10 (4%)
SA-6 mean (sd)	3.36 (0.91)	3.33 (0.83)*
Web Skill mean (sd)	3.53 (0.96)	3.35 (0.92)

C. Survey Questionnaire

1) Informed Consent: We are conducting a research study to understand USC users' password management strategies and experiences with password managers. We are seeking your participation in this study. Your participation is voluntary, and we will address your questions or concerns at any point before or during the study.

You are be eligible to participate in this study if you meet the following criteria: (a) You are over 18 years old.

If you decide to participate in this study, you will be asked to do the following activities: (a) Complete an online survey.

Before submitting the survey, you will be asked if you want to enter the $10 raffle where we give out a $10 gift card to one winner out of every 10 participants. If you decide to enter the raffle, please provide your email address at the end of the survey. We only use emails for distributing the gift cards and will delete them immediately after the raffle is completed.

Even though the survey is about passwords, we assure you that we do not ask for your exact passwords.

Our research group will publish the results in conference and journal publications. Participants will not be identified in the results. We will take reasonable measures to protect the security of all your personal information. All data will be de-identified prior to any publication or presentations. We may share de-identified data with other researchers in the future.

2) Password Management Strategies:

1. Use the slider to indicate the percentage of your passwords stored

with each management technique. (a) % of passwords I remember. (b) % of passwords I don't remember and don't store but rely on reset when I need to access the service. (c) % of passwords I store in a file on my computer or in a file in a cloud. (d) % of passwords I store in browser (e.g., passwords saved in Chrome). (e) % of passwords I store in a third-party password manager (e.g., 1Password or LastPass). (f) % of passwords I store in a system-provided password manager (e.g., Apple's Keychain). (g) % of passwords I write down on paper or other physical media.

Percentages can add up to more than 100 (e.g., if you remember some passwords but also save them in password manager).

2. Use a slider to estimate the percentage of your account passwords that are unique and not reused on other accounts.

Q2.3–Q2.6 are shown to participants based on the password strategies they reported in Q2.1.

3. You indicated that you store your passwords as digital file(s). Answer the following questions [Yes/No/Unsure]:
   - I manually copy this file to multiple devices.
   - I use a synchronization tool, like Dropbox or Google Drive.
4. You indicated that you save your passwords in a browser. Answer the following questions [Yes/No/Unsure]:
   - Do you use your browser's features to make your passwords available on browsers installed on multiple devices?
5. You indicated that you save your passwords in a third-party PM. Answer the following questions [Yes/No/Unsure]:
   - Do you use your third-party password manager to make your passwords available on multiple devices?
6. You indicated that you save your passwords in a system-provided PM. Answer the following questions [Yes/No/Unsure]:
   - Do you use your system-provided password manager to make your passwords available on multiple devices?

3) University Account Password Management:

1. How satisfied are you with each USC password requirement? [Extremely dissatisfied / Somewhat dissatisfied / Neither satisfied nor dissatisfied / Somewhat satisfied / Extremely satisfied] (a) Your password must be between 16 and 64 characters in length. (b) Your password must not contain your USC username. (c) Your password must not reuse previous passwords. (d) You need to change your password at least once every.
2. What strategies do you use to create your USC account password? [Select all that apply] ☐ I reuse the exact same password from my different account. ☐ I reuse a password with some strategies (e.g., adding a unique text). ☐ I create a completely new password but follow my personal pattern or formula. ☐ I generate a new random password using tools such as browser or password manager. ☐ I use a memorable phrase with some modifications (e.g., letters, numbers, special characters). ☐ I use personal information or dates. ☐ Other.
3. What strategies do you use to update your USC account password? [Select all that apply] ☐ I have a list of regularly used passwords and select a different one from that list. ☐ I replace or rotate characters (e.g., letters, numbers, special characters). ☐ I add different ending to my current password. ☐ I generate a new random password using tools such as browser or password manager. ☐ I update the counter in my current password (e.g., password1, password2, password3, etc.). ☐ I update the date in my current password (e.g., password2022, password2023, password2024, etc.). ☐ Other.
4. Please indicate how secure your USC account password is compared to your other account passwords. [Much less secure / Somewhat less secure / About equally secure / Somewhat more secure / Much more secure / Unsure]
5. Please explain why you chose that level of security for your USC account password. [Select all that apply] ☐ I have important information in my USC account, such as class enrollment and personal details. ☐ I try to make all my passwords (including the USC one) as secure as possible. ☐ I try to make my password memorable. ☐ I rely on two-factor authentication, so I'm less concerned about my password. ☐ I apply the same password creation strategy for my USC account as I do for other accounts. ☐ I haven't given it much thought and just use whatever is easiest at the moment. ☐ Other.

4) General Password Manager:

1. Where did you first hear about password managers? ☐ Work ☐ Media (Internet, TV, radio, etc) ☐ Other people (friends, family, etc, but not at work) ☐ School class ☐ Email from USC ☐ I don't know (don't remember, not sure) ☐ I first heard about it in this study ☐ Other
2. Do you use password manager(s)? [Select all that apply] ☐ I save my passwords in the browser (for example in Chrome) ☐ I use a third-party manager (for example, 1Password or Lastpass) ☐ I use a system-provided password manager (e.g. Apple's Keychain) ☐ I do not use a password manager
3. Please indicate your agreement with the following statements. [Strongly disagree / Somewhat disagree / Neither agree nor disagree / Somewhat agree / Strongly agree] (a) Using a password manager makes accounts less likely to be compromised. (b) Using a password manager means I do not have to worry as much about the safety of my accounts. (c) Password managers are fun to use. (d) Password managers are easy to use. (e) Password managers are difficult to use. (f) Password managers are annoying to use. (g) Password managers can be trusted. (h) I know how password managers work.

5) Password Manager Users:

1. What are your reasons for using a password manager? [Select all that apply] ☐ To conveniently manage passwords across devices. ☐ To autofill passwords for faster logins. ☐ To remember passwords. ☐ To generate passwords. ☐ To securely store passwords. ☐ To help generate stronger passwords. ☐ Other.
2. Which password managers do you use? [Select all that apply] ☐ LastPass ☐ 1Password ☐ Dashlane ☐ KeePass ☐ EnPass ☐ Kaspersky ☐ Password Manager ☐ Apple Passwords & Keychain ☐ Firefox ☐ Chrome ☐ Google Password Manager on Android ☐ Other
3. How satisfied are you overall with your experience using a password manager? [Extremely satisfied / Moderately satisfied / Slightly satisfied / Neither / Slightly dissatisfied / Moderately dissatisfied / Extremely dissatisfied]
4. Please select in the following the statement which describes you the most. When creating or resetting a password for an important account. ☐ I let the password manager create and store the password. ☐ I create the password myself, and the password manager stores it for me. ☐ I create the password myself and recall it without storing it in the password manager.
5. Rate how often you use your password manager to generate passwords for you. [Never / Sometimes / About half the time / Most of the time / Always]
6. Did you have a specific strategy when changing your existing account passwords to randomly generated ones? ☐ I only change passwords for accounts with high security (e.g., banking, email). ☐ I only change passwords for accounts I used frequently. ☐ I only change passwords when their accounts required a password change. ☐ I didn't have a specific strategy. ☐ Other.

7. Use a slider to estimate the percentage of your account passwords that are randomly generated by password managers.
8. Over time does the percentage of your accounts with random passwords increase, stay them same or decrease? [Significantly decrease / Slightly decrease / Stay the same / Slightly increase / Significantly increase]
9. What do you like about using a password manager? [Select all that apply] ☐ Not having to type my passwords (autofill). ☐ Generate strong passwords. ☐ Not having to memorize passwords. ☐ Synchronizing passwords for access across multiple devices. ☐ Having unique passwords. ☐ Using the desktop client. ☐ Viewing my passwords. ☐ Other.
10. What do you dislike about using a password manager? [Select all that apply] ☐ I have security concerns about how passwords are stored. ☐ I have concerns that someone could steal my master password. ☐ Entering passwords on an incompatible device where the password manager cannot be installed. ☐ Entering passwords when PM is not installed. ☐ Saves passwords that I do not want to save. ☐ Cannot view passwords. ☐ Generates passwords with unacceptable symbols. ☐ Does not work correctly on some websites. ☐ Other.

6) Non-Password-Manager Users:

1. Please indicate your agreement with the following statements. [Strongly disagree / Somewhat disagree / Neither agree nor disagree / Somewhat agree / Strongly agree] (a) I prefer to memorize my passwords. (b) I don't have that many unique passwords. (c) I'm concerned about security risks (e.g., if my computer or password manager is hacked). (d) I don't trust the company behind a password manager. (e) I prefer to write passwords down and store them on paper. (f) I don't know how to use a password manager. (g) I know how to use one but it is hard to use and inconvenient.
2. Have you used a password manager in the past? [Yes/No]
3. Could you imagine using a password manager again? ☐ Yes, I would reconsider using one. ☐ No, I would not use one again.
4. After learning about password managers from this survey, could you imagine adopting a password manager in the future? ☐ Yes, I would consider adopting. ☐ No, I wouldn't.

7) Free Password Manager Adoption:

1. If you were a member of an organization (company, university, etc.) which offered a password manager to all its members for free, how likely are you to adopt this password manager? [Extremely unlikely / Somewhat unlikely / Neither / Somewhat likely / Extremely likely]
2. Do you know that USC offered a password manager (1Password) to faculty, staff and students for free? [Yes/No]
3. Are you currently using 1Password? [Yes/No]

If Q7.5 is Yes.

4. Please indicate your agreement with the following statements. [Strongly disagree / Somewhat disagree / Neither agree nor disagree / Somewhat agree / Strongly agree] (a) I am satisfied with my experience using 1Password. (b) It was challenging to learn how to use 1Password at first. (c) I would recommend 1Password to USC people who have never used it.

If Q7.5 is No.

5. Please indicate your agreement with the following statements. [Strongly disagree / Somewhat disagree / Neither agree nor disagree / Somewhat agree / Strongly agree] (a) I want to adopt 1Password offered by USC. (b) I think it will be difficult to switch to 1Password. (c) I prefer 1Password to be set up with my USC account by default. (d) I am happy with my current approach to password management. (e) I'm afraid I will lose access to 1Password once I'm no longer at USC.

8) IT Skills:

1. Please indicate your agreement with the following statements. [Strongly disagree / Somewhat disagree / Neither agree nor disagree / Somewhat agree / Strongly agree] (a) I seek out opportunities to learn about security measures that are relevant to me. (b) I am extremely motivated to take all steps needed to keep my online data and accounts safe. (c) Generally, I diligently follow a routine about security practices. (d) I often am interested in articles about security threats. (e) I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe. (f) I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.
2. How familiar are you with the following computer and Internet-related concepts? [No understanding / Low understanding / Medium understanding / High understanding / Full understanding] (a) Advanced search (b) PDF (c) Spyware (d) Wiki (e) Cache (f) Phishing

9) Demographics:

1. What is your gender? ☐ Male ☐ Female ☐ Non-binary ☐ Prefer not to say
2. What is your age? [Numeric entry] ☐ Prefer not to disclose
3. What is your ethnicity? ☐ African American or Black ☐ Asian or Pacific Islander ☐ Hispanic or Latino ☐ White or Caucasian ☐ Middle Eastern or North African ☐ Native American or Indigenous ☐ Mixed race ☐ Prefer not to say ☐ Other
4. What is your position at USC? ☐ Faculty or Leadership ☐ Staff ☐ Student ☐ None

10) Raffle:

1. Are you willing to be contacted via email for follow-up studies and/or have your email entered into a raffle for a $10 gift card? (If so, you will be asked for your email address on the next page.) [Select all that apply] ☐ I am willing to be contacted via email for follow-up studies. ☐ I want my email to be entered into the $10 gift card raffle. ☐ None of the above

If participants are willing to be contacted or want to enter the raffle.

2. Please enter your email address. [free text]

D. Data Preprocessing

We followed the exact preprocessing steps used in the original work [1]. We mapped the responses from the 5-point Likert scale to ordinal numbers ($1 \rightarrow 5$). For the SA-6 score and the Web Skill score in Section III-A (Part 8), each composed of a set of 5-point Likert responses, we converted each response to its corresponding ordinal value and then averaged them. For each PM usability aspect in Section III-A (Part 4), we mapped its response to a binary scale: *Agree* (Likert values 4 and above) and *Disagree* (Likert values $1-3$), with *Agree* coded to 1. Similarly, we mapped each participant's university account security (Figure 25) to 1 for *More secure* ($\geq$Somewhat more secure) and to 0 for the rest or *Less secure*. We coded gender to binary with *Women* as 1 and *Men* as 0. We did not include the non-binary gender (Table I) because it accounted for only 2% of responses – the same reason as in the original study (1%). We coded participant role as 1 for *Student* and 0 for *Non-Student* (staff and faculty).

E. Additional Results

At USC, Figure 15 shows non-PM users' perceptions of why they do not use PMs. A majority reported preferring to memorize passwords rather than use PMs (78%), while 48% indicated that they did not have many passwords. Security concerns were also common:

60% expressed concerns about the security of PMs, and 71% reported not trusting the companies behind them. Additionally, 22% of non-PM users reported having used PMs in the past, and 83% of them indicated they would reconsider using PMs again in the future. On the other hand, 78% of non-PM users who had never used PMs before, 67% of them reported that they still would not consider using PMs.

Figures 16, 17, and 18 show the distributions of percentages of passwords that USC faculty, staff, and student participants reported storing using each password management strategy, respectively. A one-way between-subjects ANOVA revealed a significant effect of participant role on the proportion of passwords participants could remember ($F(2, 434) = 50.38, p < .001$). Planned contrasts further showed that faculty remembered significantly fewer passwords than staff ($t = -3.66, p < .001$) and students ($t = -10.53, p < .001$), while students remembered significantly more passwords than staff ($t = 3.79, p < .001$).

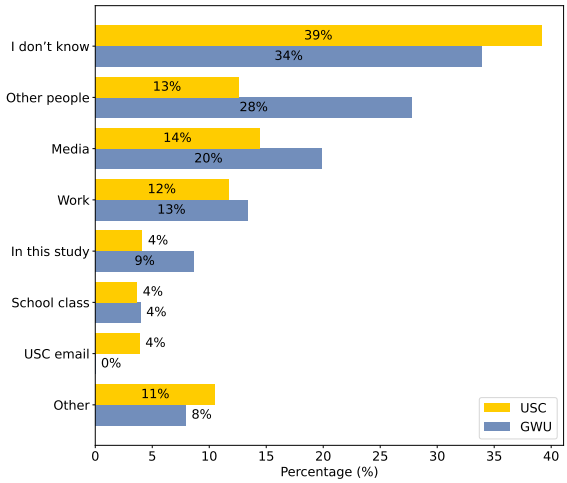

Fig. 14. Where participants first heard about PMs. In the original work, participants could select multiple options, thus the percentages do not sum to 100%, whereas in our study, participants selected only one option.

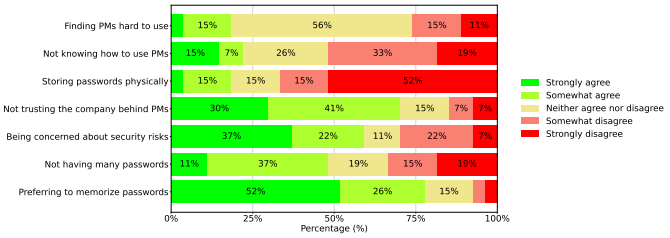

Fig. 15. Perception on PMs from non-PM users at USC.

ACKNOWLEDGMENT

Research was supported by the Army Research Office (ARO) and accomplished under Cooperative Agreement Number W911NF-20-2-0053. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Army Research Office.

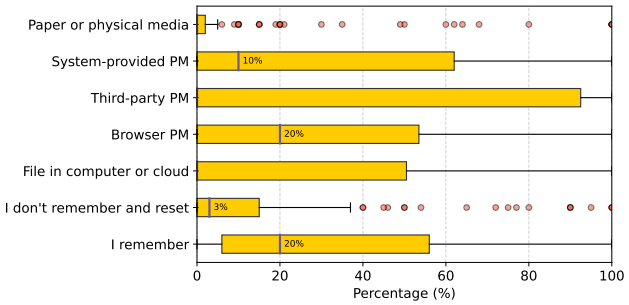

Fig. 16. Box plot of the percentages of passwords USC faculty participants store with each password management strategy.

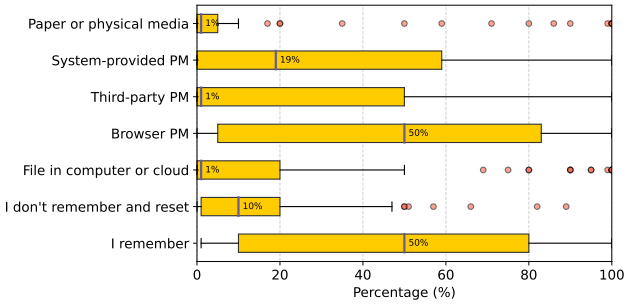

Fig. 17. Box plot of the percentages of passwords USC staff participants store with each password management strategy.

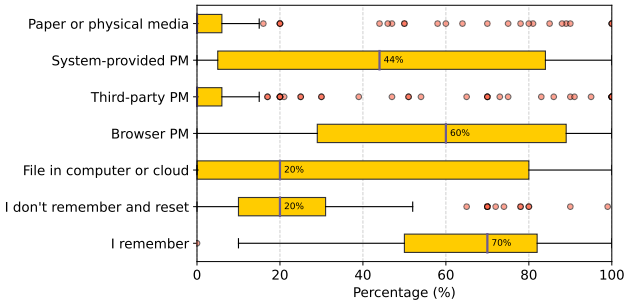

Fig. 18. Box plot of the percentages of passwords USC student participants store with each password management strategy.

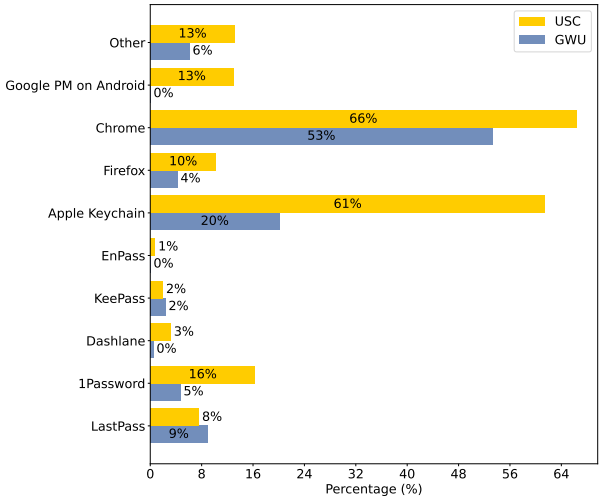

Fig. 19. PM products used by participants. USC participants could select all PM products they use, so percentages do not sum to 100%.

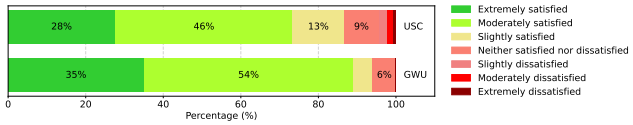

Fig. 20. Satisfaction with PMs.

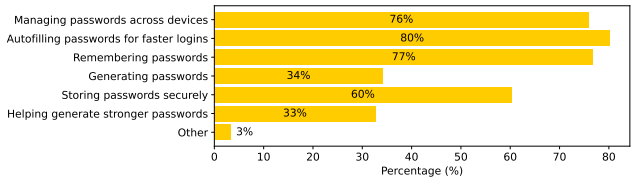

Fig. 21. Reasons participants use PMs.

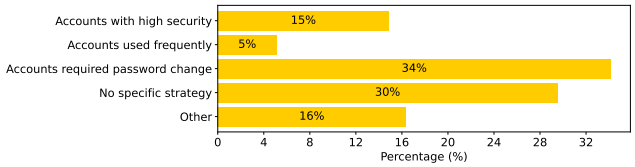

Fig. 22. The main reason PM users use PMs to generate passwords.

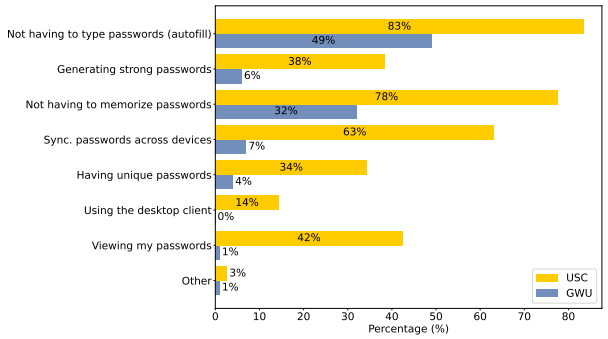

Fig. 23. Aspects of PMs that participants like.

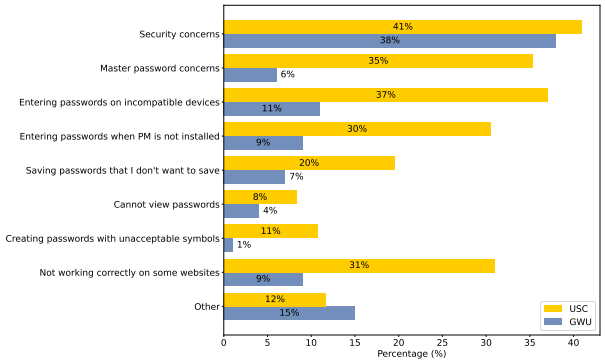

Fig. 24. Aspects of PMs that participants are concerned about.

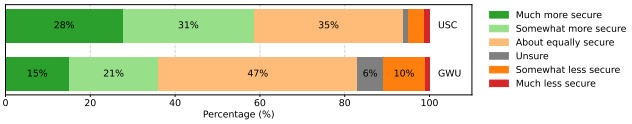

Fig. 25. University account password security compared to other passwords.

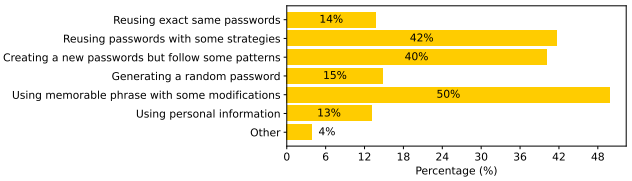

Fig. 26. Different password creation strategies.

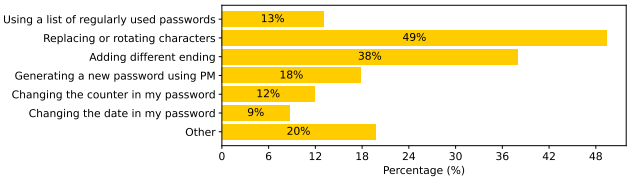

Fig. 27. Different password update strategies.

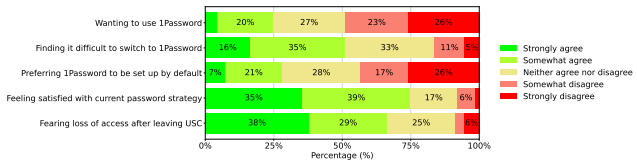

Fig. 28. Perceptions of participants who don't use the free PM (1Password).

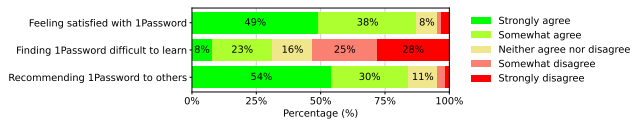

Fig. 29. Perceptions of participants who use the free PM (1Password).