Why Users (Don't) Use Password Managers at a Large Educational Institution

Peter Mayer
peter.mayer@kit.edu
Karlsruhe Institute of Technology

Collins W. Munyendo
cmunyendo@gwu.edu
The George Washington University

Michelle L. Mazurek
mmazurek@umd.edu
University of Maryland, College Park

Adam J. Aviv
aaviv@gwu.edu
The George Washington University

Abstract

We quantitatively investigated the current state of Password Manager (PM) usage and general password habits at a large, private university in the United States. Building on prior qualitative findings from SOUPS 2019, we survey n=277 faculty, staff, and students, finding that 77% of our participants already use PMs, but users of third-party PMs, as opposed to browser-based PMs, were significantly less likely to reuse their passwords across accounts. The largest factor encouraging PM adoption is perceived ease-of-use, indicating that communication and institutional campaigns should focus more on usability factors. Additionally, our work indicates the need for design improvements for browser-based PMs to encourage less password reuse as they are more widely adopted.

1 Introduction

Password management remains a weak link in the security ecosystem. Prior work shows that users tend to select weak and ineffective passwords that are easily guessed [28, 48] and reused across accounts [17]. This has led to the wide recommendation of Password Managers (PMs) that can store, recall, and generate unique passwords for each account [25]. It is often assumed that users are hesitant or uninterested in using PMs due to perceived increased management requirements [44], added complications [9], fear of losing access to the passwords [42], misplaced beliefs that current password generation habits are sufficient [44], or that PMs offer no improvements over current password habits [15].

To evaluate the penetration of PMs and the factors that affect adoption, we developed an online survey (n=277) distributed to a random sample of faculty, staff, and students at a large private university in the US. The survey included a series of closed-item responses on various password management habits and motivations for using PMs (or not) derived from the qualitative themes identified by Pearman et al. [42]. Our study therefore offers one of the first large-scale quantitative measurements of PM usage within an organization.

We were also motivated in assessing the role of institutions and organizations in encouraging PM usage and good password management habits, generally. While such studies have existed in the space of password selection [5, 35] and two-factor-authentication [11, 14], encouraging PM usage at the organizational level has not been previously explored. We were particularly interested in assessing the potential benefits and impact of a university investing in a large, campus-wide deployment of a third-party PM via a site-license for all students, faculty, and staff. The institution in which this study was conducted is considering purchasing such a license.

We find that awareness and use of PMs is much broader than previously reported: 77% of our participants used a PM. Predominately, these were browser built-in PMs (60%), matching previous findings [30] and therefore likely to generalize beyond our sample. In contrast, only 18% of our PM users used a third-party PM (some used multiple). Generally, the vast majority of respondents reuse passwords across accounts (77%), but those who use third-party PMs are much less likely to do so, suggesting that third-party PMs promote better password habits as compared to built-in, browser-based PMs, confirming prior work [30, 42].

We also find that perceived ease-of-use overall plays a key role: when considering users of all types of PMs, an overwhelming majority point to ease-of-use, rather than security benefits, as their motivation for using a PM. Participants were 14.5× more likely to use a PM if they found it "easy to use." However, when considering only third-party PM users, security plays an important role, where participants were 12.8× more likely to use a third-party PM. PM adoption campaigns should thus focus on demonstrating how PMs can improve the user experience and easily be used in normal web-browsing habits rather than exclusively focus on the security benefits.

We also find that third-party PM users are significantly more likely to use the PM to generate passwords than participants using browser built-in PMs, and the majority of participants (66%) would also adopt a PM if it was offered to them for free by their organization. This suggests an opportunity for institutions to foster secure password management habits by

investing in third-party PMs, with the benefits likely cascading. Additionally, more work is required to improve the design of browser built-in PMs as these are the most commonly used PMs, but not used to their full potential by generating unique, random passwords per account.

2 Background on Password Managers

Password Managers (PMs) are a software security tool designed to help users improve their password security while decreasing the burden of remembering passwords. Generally PMs are classified into three types:

1. **Operating System built-in PMs**: These PMs are integrated into the operating system, not requiring any additional software for example Apple's Keychain.
2. **Browser built-in PMs**: Many browsers ship with a PM built into the browser interface. For instance, Chrome and Firefox both come with such PMs and provide mechanisms for generating random/secure passwords.
3. **Third-party PMs**: Third-party PMs are dedicated software for managing and generating passwords, often exceeding the features of the former categories. Third-party PMs require users to install browser-extensions as well as a mobile app to access passwords, and full functionality typically requires a fee-based subscription.

PMs have been widely recommended [25] to improve online security. However, adoption of PMs is generally considered low [12]. In contrast to prior research, we find that PM penetration is relatively high, with over 70% of our participants drawn from a large university in the US using PMs. Most of our participants use browser built-in PMs, while usage of third-party PMs is comparatively much lower.

Several studies have investigated the low adoption of PMs, particularly third-party PMs (see Section 6). A recent study by Pearman et al. [42] interviewed 30 participants to identify why users fail to adopt PMs. Pearman et al. identified several themes, most importantly that (a) convenience and usefulness drive adoption and (b) users of third-party PMs are less prone to password reuse. There are different reasons for adopting various PMs, with adoption of built-in PMs driven by convenience and adoption of third-party PMs driven by security. Following on Pearman at al. [42], we present the first large-scale quantitative survey investigating these themes by sampling from an institution-wide mailing list at the George Washington University, which is currently considering investing in a site-wide license for a third-party PM.

3 Methods

Research Questions Our study aimed to investigate users' perceptions and usage of PMs as well as their reasons for and against adoption of PMs. We ask four research questions:

RQ1 [Awareness] *Are participants drawn from members of the George Washington University aware of PMs and their different types?*

RQ2 [Password Strategies in General] *What are the current password handling strategies of institution members, and what role do PMs play in these strategies?*

RQ3 [Institutional Account Management] *What are the strategies members of the George Washington University employ specifically for their university account passwords?*

RQ4 [Motivations & Barriers] *What are the reasons for use and non-use of PMs?*

In **RQ1**, we seek to better understand our participants' awareness of PMs and the three varieties of PMs. In **RQ2**, we explore password and account management strategies more broadly, such as how our participants create, recall and reuse passwords. We correlate account management strategies with usage of a PM during analysis, exposing how PMs impact account management. In **RQ3**, we explore our participants' specific password management strategies for their university accounts. This is of particular interest to the George Washington University because a site–licensed, third-party PM would use the organizational account password as the vault password. Finally, in **RQ4**, we seek to understand the motivations and barriers to adoption of PMs.

Survey Structure Our survey was administered online, and lasted, on average, 16 minutes. As an incentive to participate, we raffled off one $10 gift card for every 20 participants that opted to be considered. In total, we gave out 10 gift cards. All procedures were approved by the George Washington University IRB and IT department. Our survey structure is described below. The full survey is provided in Appendix A.

1. *Informed consent*: Participants were informed about the survey's purpose, structure, length, and raffle.
2. *Affiliation with the George Washington University*: As an institutional study, we asked participants if they were affiliated with the George Washington University and their role (e.g., faculty, staff, student).
3. *General password management*: Participants were asked to describe how they manage their passwords across different accounts as an open-ended question. They were additionally asked to select from a list of password management techniques (including PMs), and if multiple were selected, how they combined these techniques. Lastly, participants were asked if they re-use passwords.
4. *Password synchronization methods*: Participants were asked how they share and synchronize (or fail to do so) across devices. For example, if a participant stores their passwords in a text document, we asked if and how they share that text document across computers and devices.
5. *University account password management*: Participants were asked about password management strategies for their university account, as well as how it compares to

other accounts on a Likert scale.

6. *Introduction to PMs*: We described PMs using the explanatory text developed by Pearman et al. [42] before asking participants to indicate if they use any of the three types of PMs. Participants were further asked a series of Likert-scale questions regarding their perceptions of PM usage. Specifically, we included questions pertaining to the six aspects of usability and security used by Colnago et al. [11] in their institution-wide study (see Section 6), but adapted them from their 2FA context to the PM context in this work: (i) *Security* – whether participants perceive using PMs as preventing account compromise; (ii) *Tranquility* – whether participants believe that using PMs means one can worry less about account safety; (iii) *Fun* - whether participants perceive PMs as fun to use; (iv) *Ease-of-use* – whether participants perceive PMs as easy to use; (v) *Difficulty-of-use* – whether participants perceive PMs as difficult to use. (vi) *Annoyance* – whether participants perceive PMs as annoying to use. We complemented these aspects with two additional aspects, *trust* and *transparency*, which are relevant to PMs [3]: (vii) *Trust* – whether participants believe PMs can be trusted; (viii) *Transparency* – whether participants feel they know how PMs work.
7. *PM user questions*: PM users were asked where they had learned about PMs, as well as the PMs they use, and their reasons for using them. They were also asked about their satisfaction with PMs on a Likert scale.
8. *Non-PM user questions*: Non-PM users were asked to describe their reasons for not using a PM. They were also asked if they had used PMs before and why they had stopped. Lastly, these participants were asked if they would use a PM again and under which circumstances.
9. *IT Skills*: We asked participants about their IT background and familiarity with computer and internet concepts from the web skills measure [21] and the SA-6 security attitude measure [16].
10. *Demographics*: Participants were asked to provide their demographic information.
11. *Raffle*: Participants were asked whether they wanted to be considered in a raffle to win a $10 gift card.

Data Analysis We asked participants about the three types of PMs twice, once in step (3) and once in step (6). This was done to see whether participants would change their answer after reading the PM explanatory text. We report only the final responses from step (6), after the explanatory text, except when exploring changes in response between (3) and (6).

We applied logistic ordinal regression to analyze factors that are most influential in awareness and usage of PMs. When used as factors, the Likert responses to *security*, *tranquility*, *fun*, *ease of use*, *difficulty of use*, *annoyance*, *trust*, and *transparency* questions were binned into *agree* (Likert values 4 and 5) and *disagree* (Likert values 1, 2, and 3). We chose this more conservative binning without a neutral option, in order to prevent overestimating effects and render interpretation of the regression analyses more meaningful. Participants' roles at the university were binned into *students* and *non-students*. The web-skill and security attitude scales were calculated by averaging responses within the scale. Participant demographics (age, gender, ethnicity, race, role at the university) were control variables. We only report a model's output with these demographics when it has a better fit according to the Akaike information criterion than the model without; otherwise, we opt for the simpler model. The role had significant predictive value in only one model (see Section 4.4). Due to the low number of participants in these groups, we had to exclude (1) participants identifying as non-binary gender, and (2) participants that opted to not disclose their age or gender, when these factors were included in the models. Lastly, we used statistical tests to measure significant differences for Likert-scale and closed-response questions in the survey. The tests' specifics are discussed when reporting the results.

We used open-coding based on inductive coding [45, 49] to analyze open-ended responses. Two researchers independently coded the responses, with the primary coder developing the codebook and assigning codes to all responses and the secondary coder verifying the codebook by coding a random set of 20%. Cohen's κ was calculated and discrepancies were resolved by discussion. In case the kappa value was below $\kappa < 0.7$, another round of coding was performed. Across all questions, 1.5 rounds were needed on average to reach $\kappa \geq 0.7$ (average $\kappa = 0.77$, indicating moderate to strong agreement). For three questions (16, 17, 18 in Appendix A) there were insufficient responses to calculate κ reliably. In those cases, the primary coder and secondary coder collaboratively assigned codes. Qualitative results are reported using count data to avoid over-generalizing.

Recruitment and Demographics Our survey was administered at the George Washington University, a private university in the US and distributed by the the university's surveys office to a random sub-sample of 2,000 students, faculty, and staff in February 2021. A total of 277 participants responded, providing a response rate of 13.9%. The email subject line clearly stated that it was an invitation to a study about PMs conducted by the Computer Science department.

The sample (see Table 1) consisted of mainly younger (42 % between 18–34), female-identifying (65 % female, 31 % male, and 4 % other gender or prefer not to say) staff (47 % staff, 33 % students, 20 % faculty) and exhibited a medium web skill (mean = 3.35; sd = 0.92) as well as a medium security attitude (mean = 4.47; sd = 1.33).

Limitations As is typical, it is difficult to verify whether online participants followed instructions. We mitigated this by, first, requiring participants to spend a reasonable duration of time on certain pages and, second, by reviewing all open-ended responses to ensure consistency. We only excluded four

Table 1: Overview of participants' demographics and comparison to the the George Washington University population. Unfortunately, only gender and race/ethnicity data for faculty/leadership and staff was available as data for the entire the George Washington University population. Percentage totals may not add to 100% due to rounding.

	Faculty/Leadership		**Staff**		**Students**	**Other/Prefer not to disclose**	**Faculty & Staff**		**Total**
	Study	Uni	Study	Uni	Study	Study	Study	Uni	Study
Man	23 (40%)	51%	30 (25%)	39%	31 (34%)	2 (20%)	53 (30%)	43%	86 (31%)
Woman	34 (59%)	49%	82 (70%)	61%	58 (64%)	7 (70%)	116 (66%)	57%	181 (65%)
Non-binary	0 (0%)	0%	0 (0%)	0%	1 (1%)	1 (10%)	0 (0%)	0%	2 (1%)
Prefer not to disclose	1 (1%)	0%	6 (5%)	0%	1 (1%)	0 (0%)	7 (4%)	0%	8 (3%)
18 - 25	1 (2%)	-	10 (4%)	-	51 (18%)	0 (0%)	-	-	62 (22%)
26 - 35	4 (7%)	-	28 (9%)	-	21 (8%)	2 (1%)	-	-	53 (19%)
36 - 45	9 (16%)	-	28 (9%)	-	5 (2%)	3 (1%)	-	-	42 (15%)
46 - 55	14 (25%)	-	24 (8%)	-	5 (2%)	0 (0%)	-	-	43 (16%)
56 - 65	13 (23%)	-	12 (4%)	-	1 (0%)	2 (1%)	-	-	26 (9%)
>65	3 (5%)	-	3 (1%)	-	0 (0%)	0 (0%)	-	-	6 (2%)
Prefer not to disclose	12 (21%)	-	22 (8%)	-	8 (3%)	3 (1%)	-	-	45 (16%)
Black or African American	4 (7%%)	6%	15 (13%)	22%	9 (10%)	2 (20%)	19 (11%)	17%	30 (11%)
Hispanic	2 (3%)	4%	4 (3%)	6%	10 (11%)	0 (0%)	6 (3%)	6%	16 (6%)
White	40 (69%)	72%	74 (63%)	49%	49 (54%)	5 (50%)	112 (63%)	56%	168 (61%)
Other	4 (7%)	16%	13 (11%)	15%	20 (22%)	3 (30%)	20 (11%)	16%	40 (14%)
Prefer not to disclose blank/unknown	8 (14%)	3%	12 (10%)	6%	3 (3%)	0 (0%)	20 (11%)	5%	23 (8%)
SA-6 mean (sd)	4.53 (1.24)	-	4.50 (1.27)	-	4.35 (1.45)	4.85 (1.02)	-	-	4.47 (1.33)
Web Skill mean (sd)	3.48 (1.01)	-	3.22 (0.90)	-	3.43 (0.87)	3.43 (0.96)	-	-	3.35 (0.92)

participants out of the 281 that completed the survey.

This study was conducted at a private university in the US and may not fully generalize. While the 2 000 members of the George Washington University invited to the survey were chosen by the university's survey and research office to be evenly split along demographic lines and institutional roles, only a subset participated in the survey, leading to somewhat skewed demographics when compared to the university population (see Table 1). For both, gender and race/ethnicity, there is a higher percentage of participants with missing data (in our study "Prefer not to disclose") for both faculty and staff. However, despite these skews, we believe that some of the tendencies in our results (e.g. prevalence of Browser built-in PMs) likely reflect the population at the George Washington University and other institutions with similar demographic profiles, although we cannot speak to how these missing demographic factors may play a role. Our findings also closely match the qualitative findings of Pearman et al. [42], suggesting that our sample likely matches samples drawn from other institutions. Ultimately, additional work is needed to explore PM usage in other countries and contexts.

This study may also suffer from some social desirability bias where participants modify their responses or behavior to look more favorable in a security study, particularly for their university accounts. To mitigate this, we assured participants that all their responses were anonymous and no personally identifiable information would be collected.

Finally, our results may suffer from response bias, whereby participants with stronger opinions of PMs were more likely to respond to the survey. This could affect results estimating the awareness as well as usage or non-usage of PMs, and these measurements should be considered upper bounds. In the case that the response bias favored participants with positive experiences with PMs, this would further support the recommendations to focus on usability rather than security benefits as these were the primary motivators for adoption.

Ethical Considerations This study was approved by our Institutional Review Board (IRB), with each participant fully informed about the purpose, structure, and risks associated with taking part in the study. We did not collect any passwords or personally identifying information from participants to minimize any risks of loss of confidentiality. Those who optionally participated in the $10 raffle provided their email addresses, which were only used to distribute the gift cards, and were immediately deleted after the raffle was completed.

4 Results

4.1 RQ1 - Awareness

In response to **RQ1**: *Are participants drawn from members of the George Washington University aware of PMs and their different types?*, we investigate our participants awareness of PMs in general and of the three types of PMs.

Awareness of Password Managers In General We asked

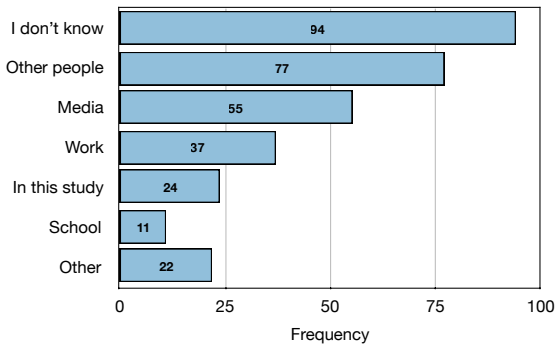

Figure 1: Where participants heard about PMs. Participants could check all that apply.

participants (n=277) whether they were aware of PMs and, if so, where they had first heard of them (multiple-choice). The vast majority were aware of PMs prior to the study (see Figure 1): only 9% of our participants heard about PMs "in this study" for the first time and thus were unaware (the only exclusive option). For those aware about PMs, 34% could not recall where they had first heard about them. Word of mouth was the most frequently recalled source, mentioned by 28% of participants. Consequently, it seems that positive experiences propagated by word-of-mouth might be an important way to foster awareness of PMs.

We also sought to understand which factors influence participants' awareness of PMs. We therefore ran a logistic regression on whether participants had heard about PMs before our survey. We included as factors the participants' scale scores for security attitude (SA-6) and web skills, as well as their demographics (see Table 2). Only the participants' web skill score seemed to be a significant factor ($OR_{\text{Web Skill}} = 1.90$, $p = .036$). For each one point increase in a participants' rating on the web skill scale, they were 1.90× more likely to be aware of PMs prior to the study. Thus, being knowledgeable about internet concepts generally seems to translate to knowledge of PMs. Surprisingly, higher security attitudes (SA-6) did not significantly explain the variance in PM awareness. This is not to suggest that security attitudes do not increase awareness of PMs, but rather that since awareness of PMs is already widespread, having strong security attitudes (as measured by the SA-6 scale) was not a strong predictor.

Awareness of Types of Password Managers We also investigated participants' awareness of different types of PMs (e.g., built into browsers, built into OS, and third-party PMs). We inquired twice about whether they use any of the three types of password managers: once during step (3) and once during step (6), right after participants read through the explanatory text about PMs (see Section 3). We asked twice to see whether participants would change their responses after reading our explanatory text about the different PMs. Table 3 shows how participants' responses changed.

Table 2: Logistic regression for participants' awareness. Significant factors are marked in bold italic.

	Est.	OR	95% CI	p-val
(Intercept)	−2.02	0.13	[0.01, 1.59]	.116
SA-6	0.18	1.20	[0.81, 1.77]	.356
Web Skill	***0.64***	***1.90***	***[1.07, 3.56]***	***.036***
Gender: Woman (vs Man)	0.88	2.42	[0.88, 6.63]	.081
Age (in years)	0.03	1.03	[0.99, 1.06]	.120

Table 3: Changes in PM use *before* (step 3) and *after* (step 6) participants were shown PM explanatory text.

PM type		No change	Change
OS built-in	use before	71	13
	non-use before	178	15
Browser built-in	use before	144	16
	non-use before	94	23
Third-party	use before	47	6
	non-use before	221	3

Participants' responses show that most people understand the differences between the various types of password managers. The majority of participants (75%) responded consistently to the two prompts, indicating the same type of PM used (or lack thereof). Among the 69 (25%) who made changes between the two prompts, 39 (14%) changed their answer about browser built-in PMs: 16 (6%) who originally said they were using a browser built-in PM realized they were not actually using one, and 23 (8%) realized that in fact they were. Changes to operating system built-in PM answers were similar, but slightly smaller in scale. This suggests that a small but noticeable portion of participants misunderstood either what a PM is or what type of PM they use prior to reading our definitions. On the other hand, few people changed their answer about third-party PMs, probably because they require explicit, intentional installation which is difficult to misunderstand.

4.2 RQ2 - General Password Strategies

In this section, we present the results for **RQ2**: *What are the current password handling strategies of institution members, and what role do PMs play in these strategies?* We begin by describing participants' password management strategies for all their online accounts and the role of PMs in these strategies. Thereafter, we describe if and how participants synchronize their passwords across multiple devices. Lastly, we discuss password reuse across accounts by participants.

Password Management Strategies We were interested in participants' password management strategies, and the role of PMs in the management of their online accounts. Pass-

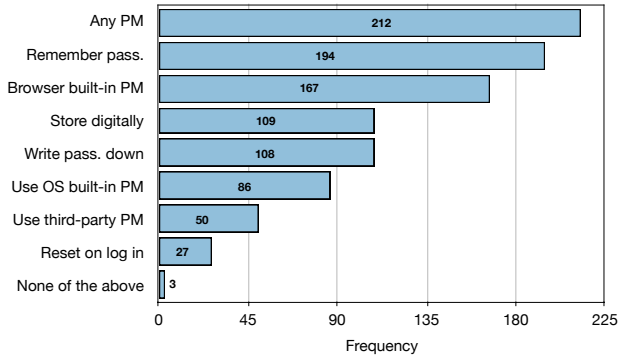

Figure 2: Password management techniques of participants after they saw PMs explanatory text in step (6) (see Section 3).

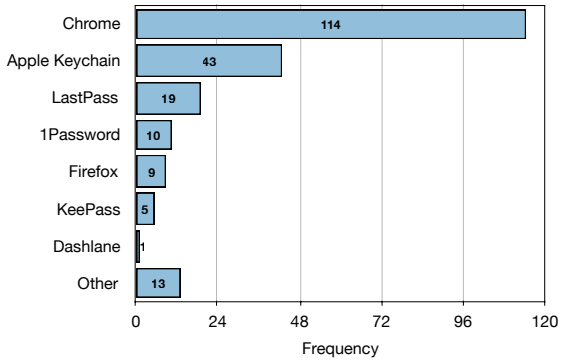

Figure 3: PMs used by our participants.

word management techniques were reported as closed-item responses based on Pearman et al.'s [42] interviews. The question was multiple-choice and thus the percentages do not add up to 100%. The primary results are presented in Figure 2, with most participants reporting using multiple strategies, with a mean of 2.6 (sd=1.3) strategies per participant.

The most common strategies are simply remembering the password (70%) and using a browser built-in PM (60%). Storing passwords digitally but not in a PM, such as in a text document, was also common (39%), as well as physically writing passwords down (39%). Many participants also reported using an operating system built-in PM (31%), but only 18% of participants indicated that they use a third-party PM. Surprisingly, 10% of participants said they prefer to reset their password on each login attempt, while not storing nor remembering the password at all. Our findings support the qualitative results of Pearman et al. [42], as all of the strategies reported in their work are also used by some of our participants.

We asked participants who use multiple strategies to manage passwords (n=211) how they combine these strategies in a free-text question. Thirty six participants primarily use one strategy, with others reserved for specific use cases, e.g.: *"I usually try to just remember the passwords but for less used accounts I will store the password in the browser or write it down on a post it next to my computer." (P220)*. Frequency of use was a common theme for differentiating between strategies, along with perceived security requirements for the account, the complexity requirements for the password, or the devices the participant needed the passwords on.

Twenty one participants mentioned using different techniques to create redundant means to access their passwords in case they forgot them, did not have access to a certain device, or for general safe-keeping, e.g., *"Third-party app for my personal computer and a paper/system method for my GW work computer. And a paper hard copy for both...just to be sure." (P250)*. Relatedly, 7 mentioned using different strategies for work and personal accounts while 19 participants stated they were transitioning from one technique to another, e.g., *"It's very challenging to find a strategy that works. 1Password has been the most successful. I am trying to transition to using it for everything." (P246)*.

Other ways of combining different strategies included: using one strategy for single-owner accounts and another for shared accounts (3), using one strategy for self-managed accounts and another strategy for accounts managed for others (1), writing passwords down on paper initially to memorize them (2), and resetting passwords if the password is needed infrequently (4) or in the face of complex requirements (1).

Lastly, 8 participants indicated not having a specific system to combine their strategies, e.g, *"it's a mess of strategies, I admit it" (P53)*.

PM Use and Satisfaction Overall, 77% of participants use either a browser built-in PM, an operating system built-in PM, or a third-party PM to manage their online accounts; this was higher than we expected. The least commonly used PMs were third-party PMs. They were used by 18% of all participants (24% of PM-user participants).

We further asked PM users the specific PM they use most frequently. This is summarized in Figure 3. The dominant browser built-in PM is Google Chrome's PM (54%). This follows popularity of Google Chrome, which is the most commonly used browser in the US[1]. Participants reported using four of the third-party PMs we had included in our list: LastPass (9%), 1Password (5%), KeePass (2%) and Dashlane by one of the 212 PM users. Participants also indicated using other PMs, with each of the following PMs used by two participants: Edge's browser built-in PM, the Roboform third-party PM, the Password Safe third-party PM, and Safari's browser built-in PM. Keeper, Bitwarden, Norton/Lifelock and 1 custom solution were used by 1 participant.

We also asked participants about their satisfaction with the PMs they use. Figure 4 gives an overview of the responses. Nearly all participants (94%) were extremely, moderately, or slightly satisfied with their PM. The remaining 6% were

[1] https://gs.statcounter.com/browser-market-share/desktop/united-states-of-america/#monthly-202010-202106

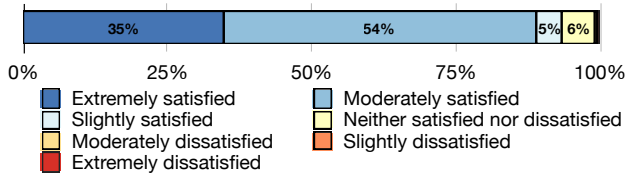

Figure 4: Satisfaction with PMs. Note that moderately dissatisfied and extremely dissatisfied had 1 response each.

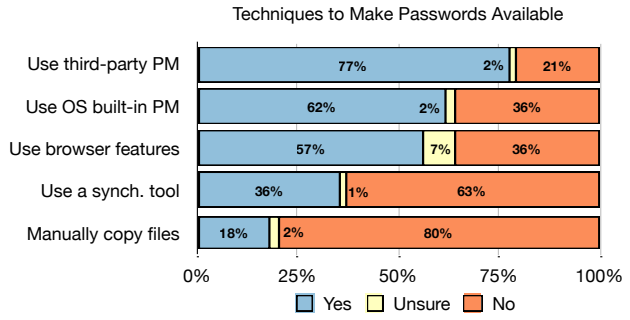

Figure 5: Techniques to make passwords available across multiple devices.

neither satisfied nor dissatisfied. This suggests that those who are using a PM are likely benefiting from them.

Synchronizing Passwords Synchronizing passwords across devices is critical in password management. Prior work with older users has reported a mistrust of cloud services and password synchronization [43]. We sought to understand synchronization habits generally. Figure 5 summarizes our results (participants could indicate using multiple synchronization techniques). For PM-users (n=212), synchronizing passwords across devices was very common: 62% for operating system built-in PMs, 57% for browser built-in PMs, and 77% for third-party PMs. About half of participants (57) who store their passwords digitally but not in a PM (n=109) make them available across devices (52%). The remaining of these 109 participants synchronize their passwords: 16 (15%) using manual methods, 34 (31%) using additional synchronization tools (like Dropbox or Google Drive), and 4 (4%) using both. Three participants were unsure about using synchronization. While synchronization is popular, it is most popular among PM users, potentially because of integrated functionality.

Password Reuse and Password Generators Unfortunately, password reuse was very common: 77% of all 277 participants indicated reusing passwords across accounts (see Figure Figure 6). Password reuse is least pronounced among users of third-party PMs. Only 47% of third-party PM users reuse passwords, only about half as prevalent as among those that write down their passwords (76%) or use an operating system built-in PM (77%). This is in stark contrast to those who use

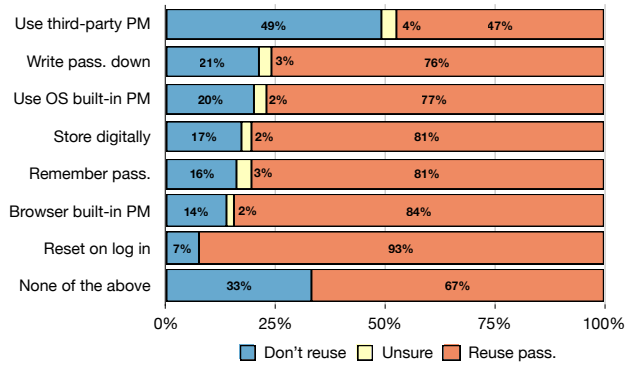

Figure 6: Password reuse across different password management strategies.

a browser-based PM, where 84% indicated they reuse passwords. A *chi*-square test showed that users of third-party PMs were significantly less likely to reuse passwords when compared to other password management strategies ($\chi = 39.22$, $p < 0.01$). These findings support those of Lyastani et al. [30] that users of browser built-in PMs are more likely to reuse passwords. Interestingly, participants who reset passwords on each login are the most likely to reuse passwords (93%), despite selecting passwords they choose not to remember.

One easy way to counteract reuse when using any type of PM is to use a password generator. Therefore, we asked PM users (n=212) whether they let the PM generate their passwords. The majority of PM users (67%) still create their own passwords, only using the PM to store them. Only 20% of PM users let the PM generate their passwords, with the remaining 13% of participants creating the passwords themselves and then remembering them without using the PM. The latter might be proof of participants combining strategies for redundancy with the PM as fail-safe. However, we can not draw this conclusion from our data. Even for third-party PMs, where automated generation is prevalent, only 54% use it. For browser built-in PMs (13%) and operating system built-in PMs (20%) password generation is even less prevalent. This indicates an opportunity to guide PM users towards more secure password generation strategies, regardless of PM type.

To understand what correlates with the use of password generators, we ran a logistic regression. We included the participants' scores for security attitude (SA-6) and web skill, calculated as described in Section 3, as well as the perceived security of their university account password (see Table 4) and the eight aspects from the literature (Section 3: security, tranquility, fun, ease of use, difficulty to use, annoyance, trust, transparency). Of these factors, security attitude ($OR_{\text{SA-6}} = 2.22$, $p = .002$) and perceived security of PMs ($OR_{\text{Security}} = 4.17$, $p = .023$) have a significant effect. Participants were 2.22× more likely to generate passwords for each one point increase in their security attitude and 4.17× more likely to generate passwords if they agree that PMs are secure.

Table 4: Logistic regression for participants generating their password with a PM. Significant factors marked in bold italic.

	Est.	OR	95% CI	p-val
(Intercept)	***-5.17***	***>0.00***	***[>0.00, 0.07]***	***<.001***
SA-6	***0.80***	***2.22***	***[1.38, 3.84]***	***.002***
Web Skill	−0.35	0.70	[0.34, 1.42]	.333
Security: Agree (vs Disagree)	***1.43***	***4.17***	***[1.23, 14.96]***	***.023***
Tranquility: Agree (vs Disagree)	0.49	1.63	[0.43, 6.20]	.469
Fun: Agree (vs Disagree)	−0.17	0.84	[0.26, 2.62]	.774
Ease of Use: Agree (vs Disagree)	−0.39	0.68	[0.18, 2.78]	.577
Difficulty: Agree (vs Disagree)	−0.71	0.49	[0.04, 4.24]	.537
Annoyance: Agree (vs Disagree)	0.47	1.60	[0.38, 6.17]	.503
Transparency: Agree (vs Disagree)	0.32	1.38	[0.44, 4.31]	.572
Trust: Agree (vs Disagree)	0.63	1.87	[0.60, 6.11]	.283
Uni. account: More secure (vs Less secure)	−0.25	0.78	[0.29, 2.02]	.615

4.3 RQ3 - Strategies for the George Washington University Passwords

We now discuss **RQ3**: *What are the strategies members of the George Washington University employ specifically for their university account passwords?* This includes participants' perceived security of their university account passwords, creation strategies, and their reasons for using these strategies.

Perceived Security of the George Washington University Password As discussed in Section 3, the password used to protect an institutional account might be particularly important if it becomes the vault password through an institution-wide deployment of PMs. Figure 7 shows participants' responses when asked how their university password compares to other passwords they have. Most participants (83.2%) said the password of their university account is at least as secure as other passwords they have.[2] When asked why they chose the respective security level for their university account password in a free-text question, the most frequent theme (45 participants) was the importance of this account. Often, participants referenced the functions or data that rendered the account important for them, e.g. *"Lots of important stuff in email including private student data" (P46)*. Other themes reported by at least 20 participants included trying to keep

[2]We note that perceived security can serve as a rough proxy for actual security against guessing attacks [50].

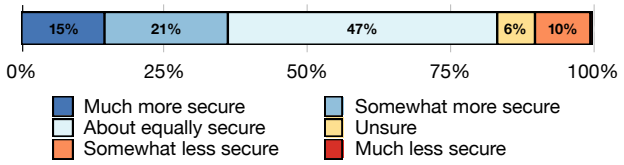

Figure 7: How secure the George Washington University account passwords are compared to other passwords.

all accounts as secure as possible (43 participants), trying to make it memorable (28 participants), having chosen the security level with the usage of two-factor authentication in mind (21 participants), and using the same strategy as for other passwords (20 participants).

Strategies for Creating the George Washington University Passwords When asked how they create their university account password in a free-text question, the most common response was reuse, named by 79 participants. Some detailed their specific reuse strategies, such as variations on existing passwords (34 users), e.g., *"I used the first half of my standard password but added a different ending" (P246)*, or *"Each time I am asked to reset my password, I simply change the [special] character I use while maintaining the base." (P17)*. A few (5) carried over passwords from previous institutions, e.g., a *"variation of the password that I used at my previous institution" (P26)*. Eight participants mentioned reusing existing passwords exactly: *"Same password I always use" (P142)*.

Another common strategy was to choose the password to include particular character classes: numbers (58 participants), letters (31 participants), or special characters (31 participants). For example, P164 stated, *"I thought of a memorable phrase and passwordified it with some special characters."*. The third most frequent strategy was to use personal information (25 participants) or dates (18 participants), e.g. *"I thought of my partner and used password based off him that no one would guess and I would always remember" (P144)*.

When asked why they use these strategies, the most frequent answer (154 participants) was to make the password memorable. Some participants detailed how their strategy helps with memorability, e.g., *"This strategy [. . .] allows me to record only the special character at the end since the password base always remains the same." (P17)*. Security was also popular, but named by only 34 participants. Despite the emphasis on memorability, a majority (57%) rely on autofill rather than memory to enter their university account password.

4.4 RQ4 - Motivations & Barriers

Finally, we describe the results pertaining to *What are the reasons for use and non-use of PMs?*. We first present our regression results, before discussing motivations and barriers.

General Influencing Factors To understand factors asso-

Table 5: Logistic regression for participants' use of PMs. Significant factors are marked in bold italic.

	Est.	OR	95% CI	p-val
(Intercept)	1.13	3.10	[0.41, 25.69]	.281
SA-6	−0.22	0.81	[0.53, 1.19]	.286
Web Skill	−0.15	0.86	[0.46, 1.59]	.624
Security: Agree (vs Disagree)	1.12	3.06	[0.79, 12.61]	.113
Tranquility: Agree (vs Disagree)	−1.45	0.24	[0.05, 1.01]	.0.56
Fun: Agree (vs Disagree)	0.19	1.21	[0.24, 9.27]	.835
Ease of Use: Agree (vs Disagree)	***2.68***	***14.53***	***[5.51, 43.83]***	***<.001***
Difficulty: Agree (vs Disagree)	1.41	4.08	[0.68, 28.34]	.135
Annoyance: Agree (vs Disagree)	−0.52	0.60	[0.16, 2.32]	.444
Transparency: Agree (vs Disagree)	***1.15***	***3.15***	***[1.05, 10.35]***	***.047***
Trust: Agree (vs Disagree)	0.84	2.32	[0.81, 7.01]	.122
Role: Student (vs non-Student)	0.16	1.18	[0.44, 3.26]	.750
Uni. account: More secure (vs Less secure)	−0.59	0.55	[0.21, 1.36]	.198

ciated with the use of PMs, we conducted a logistic regression. As factors we included participants' security attitude scores (SA-6), their web skill level, their role at the George Washington University, perceived security of their university account password and the eight perceptions of PMs: security, tranquility, fun, ease of use, difficulty to use, annoyance, trust, and transparency. Table 5 shows that only ease of use ($OR_{\text{Ease Of Use}} = 14.53$, $p < .001$) and transparency ($OR_{\text{Transparency}} = 3.15$, $p = .047$) significantly increased likelihood of adopting a PM. Specifically, participants are $14.53\times$ more likely to use a password manager if they perceive PMs as easy to use and $1.15\times$ more likely to use a password manager if they believe they know how PMs work. This shows that perceived ease of use is key in the adoption of PMs.

The picture gets more diverse when examining factors that influence adoption of each type of PM individually. Specifically, for browser built-in PMs, security attitude score ($OR_{\text{SA-6}} = 1.40$, $p = .025$) and ease of use ($OR_{\text{Ease Of Use}} = 2.99$, $p = .003$) showed significant effects. For operating system built-in PMs, ease of use ($OR_{\text{Ease Of Use}} = 14.53$, $p = .019$) was the only significant factor. In contrast, for third-party PMs, the factors security attitude ($OR_{\text{SA-6}} = 1.62$, $p = .034$), perceived security of PMs ($OR_{\text{Security}} = 15.82$, $p < .001$), and perceived transparency of PMs ($OR_{\text{Transparency}} = 4.91$, $p = .005$) are associated with increased adoption, while a participant's status as student (vs. non-student) ($OR_{\text{Role Student}} = 3.11$, $p < .028$) is associated with non-adoption. Full details of these three regression analyses can be found in Appendix C. Similar to Pearman et al. [42], our findings indicate that factors driving adoption of browser built-in PMs and operating system built-in PMs differ from those of third-party PMs. When trying to foster adoption of any such tool, it is important to tailor the effort accordingly.

Table 6: PM aspects most liked by PM users from a closed-answer question based on Pearman et al. [42].

Aspect	% of PM users
Not having to type my passwords (autofill)	49%
Not having to memorize passwords	32%
Sync. passwords for access across devices	7%
Generate strong passwords	6%
Having unique passwords	4%
Viewing my passwords	1%
None of the above	1%

Motivators for PM Adoption To understand the most important features of PMs to users, we asked PM users (n=212) about their main reason for using a PM (free-text). The responses align well with our regression results. Ease of use for managing passwords was the most frequently cited reason (60 participants), followed by convenience in managing passwords (37 participants). Memorability played an important role too, with 31 participants citing that PMs help them keep track of their passwords, 24 citing difficulties remembering their passwords without a PM, and 24 appreciating that they do not have to remember their passwords. Other usability reasons named by more than 2 participants include saving time during login (17 participants), avoiding repeatedly typing passwords (13 participants), and passwords being automatically available in browser built-in PMs (7 participants).

Some participants also mentioned security-relevant reasons. For 22 participants, the main reason to use a PM was to securely store passwords. Ten participants appreciated that PMs enable unique passwords for accounts, and for 9 participants the main benefit is allowing them to use stronger passwords.

We also asked PM users (n=212) about the aspect they liked most about using a PM, based on the aspects identified by Pearman et al. [42]. Table 6 summarizes these results. Named by almost half of the PM users (49%), the most frequent aspect was not having to type passwords (autofill). Memorability was the second-most important aspect (32%).

We also asked non-PM users who had not used a PM before (n=52) the main reason that could convince them to adopt a PM (free text). Most of these participants (18) said they would not consider using a PM, mostly for security reasons, e.g. *"I do not think that I would ever use a password manager. I am concerned that if someone were to gain access to my computer*

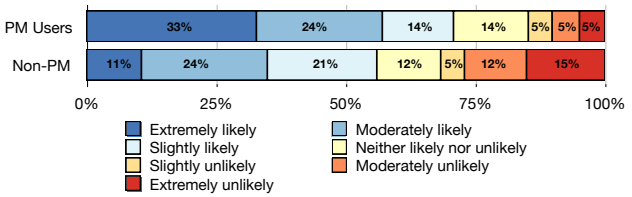

Figure 8: Password manager adoption if offered by institution.

with a password manager on it, then they could get into any of my accounts" (P80). Another 15 participants said they might consider a PM if certain conditions were met, e.g. *"Possibly if I diversify my passwords and have a lot of [accounts]" (P111)*. The most frequently cited considerations for the adoption of a PM were convenience (6 participants) and increased security (5 participants). Similarly, we asked non-PM users who had used a password manager before (n=13) about reasons they might adopt a password manager again. Most prominently, 4 participants said they would not use a PM again.

Lastly, we investigated whether participants would adopt a third-party PM if it was offered to them for free by the George Washington University. The results, depicted in Figure 8, show that most participants are willing to adopt a PM. For existing PM users, 33% are extremely likely, 24% are moderately likely and 15% are slightly likely to adopt a PM if it is offered to them. For non-PM users, 11% are extremely likely, 24% are moderately likely and 21% are slightly likely to adopt a PM if it is offered to them. Consequently, efforts to deploy a PM in an institution seem worthwhile and would likely see most institution members adopting use of the PM.

Barriers to PM Adoption Lastly, we sought to understand the challenges that prevent use of PMs by asking the 65 participants who did not use a PM for their main reasons (free-text). The most frequent response, given by 24 non-PM users, was a lack of trust in the PM, mostly regarding security, e.g. *"Why would I let a random machine know and then autofill my passwords? That just seems like an additional 'person' that knows my password, and is therefore additional exposure" (P27)*. The second most frequently named reason was that PMs are not needed (18 non-PM users). Trust seemed to play a key role, e.g. *"I trust my current method and don't need a change" (P102)*. Other reasons mentioned include lack of awareness of PMs (9 participants), lack of knowledge about PMs (8 participants), and the required effort (3 participants). Thirteen of the 65 non-PM users had used a PM before.

We also asked PM users what they liked least about a PM as a closed-answer question, based on Pearman et al. [42]'s themes. The most frequently cited concern was security, named by 38% of PM users. It was followed by ease of use: 11% of participants were frustrated with entering passwords on devices without the PM, 9% disliked entering passwords when the PM is not installed, and 9% complained that PMs do not work on some sites. Table 7 summarizes the responses.

Table 7: PM aspects least liked by PM users from a closed-answer question based on Pearman et al. [42].

Aspect	% of PM users
Security concerns	38%
Entering passwords on incompatible devices	11%
PMs do not work on all sites	9%
Entering passwords when PM is not installed	9%
Saves passwords that I do not want to save	7%
Vault password concerns	6%
Cannot view passwords	4%
Creates passwords with unacceptable symbols	1%
Other	6%
None of the above	9%

5 Discussion

This paper presents the results of a large-scale quantitative study of PMs at a large private university in the US. In this section, we first discuss the results of our study and their implications. Then, we offer recommendations to institutions and PM developers that can boost the adoption of PMs.

5.1 Results and Implications

Increasing Awareness of Password Managers Awareness of PMs is surprisingly high among our participants, with most learning about PMs via word-of-mouth. Story-telling approaches that outline positive experiences of using PMs and dedicated "PM advocates" could also foster adoption of PMs, harnessing word-of-mouth effects. This is similar to recommendations made by Haney and Lutters [19] for security practices, generally. They noted that advocates that can establish trust with the audience and be honest about risks involving security practices have the biggest impact; the same could be true with PMs, particularly in an institutional setting. Since they reflect earlier findings, we believe that our results on how people got aware of PMs are likely to generalize.

Increasing Use of Password Managers While our sample might be subject to bias as outlined in section 3, we observe an unanticipated high number of participants using PMs. Browser built-in PMs are the most popular option. In contrast, third-party PMs have substantially lower adoption, but still exceed previously reported adoption numbers [12]. This imbalance between the types of PMs is most likely a result of browser built-in PMs being more readily available within browsers, unlike third-party PMs that have to be separately installed on users' devices. Additionally, browser built-in PMs are freely available to users compared to most third-party PMs that require users to purchase licenses to access their full functionality. Nonetheless, additional work is required to explore the differences between different types of PMs, specifically

regarding their perceived and real benefits. We also found that perceived ease of use plays a key role in adoption of PMs, even more so that security; participants were 14.53× more likely to use PMs if they found them easy to use. In contrast, security only played a major role when exclusively considering third-party PM users, where these participants were 12.8× more likely to adopt PMs if they found them secure. These results suggest that institutions can play a key role in fostering the adoption of PMs. Specifically, third-party PMs can be set up for new users as they are on-boarded to the organization, similar to efforts to deploy 2FA at institutions [11] that have proven promising. Adequate support can then be provided early on to ensure that users can easily use the PM. For existing members, organizational campaigns promoting usage of PMs should focus on demonstrating how PMs will easily help members to manage their passwords, more so than their security benefits. Since our results regarding PM's ease-of-use and security reflect the qualitative findings of Pearman et al. [42], we believe that these results are very likely to generalize beyond our sample and setting.

Role of Trust and Transparency Besides ease of use, we also found that trust, or the lack thereof, plays a key role in PM usage. Several participants expressed hesitancy towards using PMs because of concerns with trusting these tools with all their account passwords. Analysis of the open-ended responses revealed that concerns surrounding security and trust were primary when choosing to not use a PM. The importance of these factors is also supported by our regression analysis, whereby the perceived transparency of how PMs work made PM adoption by participants 1.15× more likely. To further explore factors influencing trust and how well they generalize, and in particular potential ways to overcome them, future work is needed. This might include qualitative work focusing on PM users that had initial trust issues and how they overcame them or testing different PM descriptions highlighting the factors found to be influential in our investigation.

Confirming Prior Qualitative Results The findings of our study confirm earlier qualitative results by Pearman et al. [42] indicating that there are different factors driving the adoption of different PMs. For operating system built-in PMs and browser built-in PMs, ease of use appears key, while perceived security is significant for third-party PMs. We also find wide-spread password reuse, with 77% of our participants indicating to do so. However, this was significantly lower among third-party PM users. We also find that the usage of PMs' password generation features is relatively low. Further, the usability problems among PM users and security concerns for non-PM users are barriers to the use and adoption of PMs. Overall, the results from Pearman et al. [42] generalize to the quantitative results at our institution, which could indicate that these results might generalize beyond our sample and setting to other organizations with similar demographic profiles.

5.2 Recommendations to Institutions

One of our goals was to identify how institutions can best direct their efforts in increasing PM adoption. Here, we outline recommendations for such institutions.

Offering a PM to Members Will Lead to Adoption Our results seem to support institution-wide introduction of PMs as worthwhile. A majority of participants (even non-PM users) indicated willingness to adopt a PM if it was offered to them for free by an institution they are part of. Further, institution-wide adoption might be a way to overcome issues regarding members' trust in PMs. If the PM is endorsed by the institution, this signals trust, which might in turn inspire trust in the PM, further increasing the likelihood of adoption.

Exploit Word-of-mouth Propagation Our results indicate that word-of-mouth plays an important role in creating awareness about PMs. Consequently, institutions can facilitate PM users to recommend PMs to others if they want to create more awareness about them. One way to achieve this might be through rewards (for example software subscriptions or even movie tickets) for every successful referral. This could also be achieved by designating certain members of the institution, perhaps IT departments, to promote and support their usage through talks, workshops or other related events. These sessions can additionally be utilized to address concerns or misconceptions about PMs. For educational institutions, these efforts may include lessons on how to set up and properly use PMs, perhaps as part of coursework or other learning activities. These institutions can also establish clubs or other initiatives to promote secure password behavior within their institutions, specifically using PMs. When planning these activities, efforts should center around ease of use for built-in browser PMs, and security for third-party PMs. Further, such activities should be directed at new members of the institution during initial on-boarding and setup of their devices.

Fostering Trust in Password Managers Institutions can try to increase trust in PMs by investing in a third-party PM and availing it to members. This trust may be transitive, where demonstrating institutional support for a PM leads to higher trust in PMs. If synchronizing passwords in the cloud or using a third-party vendor is a barrier for the institution or users, the institution could consider deploying their own PM on-premise so that the hosting occurs on the institution's servers. However, to prevent negative effects that could possibly arise from a breach of their infrastructure, institutions must enforce relevant measures, particularly encrypting users' passwords stored in the PM using their vault password as the key, just like PMs do. Further, they must be ready to support users transition to other PM options when they leave the organization.

Build on Existing Potential Our study suggests that the usage of third-party PMs correlates with more secure password practices. In particular, our findings suggest that password

reuse is substantially lower with third-party PMs. Yet, browser built-in PMs are much more prevalent. We recommend that institutions build on the existing potential of third-party PMs by investing in transitioning users of browser built-in PMs to third-party PMs, for example via talks and workshops. Help desk staff could additionally assist users in this transition.

PM Functionality on Institution Websites Institutions should offer advice on known compatibility problems. Among the aspects least liked by PM users in our study was when PMs were not working as expected. The primary goal should be to ensure compatibility with all internal services, and recent work by Huaman et al. provides guidance to ensure better integration with PMs [23]. Internal incompatibilities should also be documented, with an end-goal of full compatibility in the future. Additionally, advice on incompatibilities with external sites could also be provided and would assist in mitigating negative experiences stemming from such incompatibilities.

5.3 Recommendations to PM Developers

Our results indicate the need for design improvements of PMs, particularly browser built-in PMs, to encourage more secure password behavior among users. These are described next.

Passwords Need to Be Easily Accessible While passwords can easily be accessed on browser built-in PMs, there is room to make them even better and more usable. For instance, a user of a third-party PM, like LastPass or 1Password, can easily access all their passwords, generate random passwords, search and even copy passwords through a quick pop-up provided by this PM's browser extension. This enables users of these PMs to easily access the PM's most important functionality while not having to navigate to a new (internal) web page, as is currently the case with most browser built-in PMs. While browser built-in PMs are great at generating random passwords when they detect password fields, they should consider implementing techniques such as pop-ups to make their features more readily available to users. Further, adding a visual icon of the PM, similar to third-party PM extensions, as part of the browser interface could serve as a useful reminder for users to utilize the browser built-in PM's features even more. Such affordances are a promising area of future research.

Password Generation Needs to Be Prominent in UI Third-party PM users were found to exhibit the lowest reuse rate among PM users. While this is likely a result of third-party PM users being more security-driven compared to browser built-in PM users who are more convenience-driven, browser built-in PMs can take some steps to reduce this reuse. While these PMs already check password reuse across accounts and inform users, it is likely that most users just ignore these warnings, as already confirmed by Huh et al. [24] in their study exploring the effectiveness of password reset emails. Therefore, browser built-in PMs should consider updating their warning dialogues to better focus on showing the associated security risks as well as conveying a sense of urgency to nudge users to update their reused credentials. Nonetheless, additional work is needed to explore why PM users, particularly browser built-in PM users, still re-use their passwords.

6 Related Work

6.1 User-perspective on Password Managers

Prior work has explored perception and usability, as well as factors fostering or hindering the adoption of PMs. Of these factors, ease of use and trust seem to be strong indicators for the adoption of PMs [1, 9, 31]. A recent investigation by Pearman et al. [42] found that usability and convenience drive adoption of PMs while security concerns hinder adoption. Their results also indicate that reuse of passwords seems to be lower with users of a third-party PM. We confirm these qualitative findings through one of the first large-scale quantitative measures of PM usage at a large institution, and offer recommendations that can further boost PM adoption.

For behavioral constructs, it has been reported that insufficient time for users, a low perceived threat, and a lack of immediacy hinder adoption of PMs [4], while autonomy i.e., the feeling of having control and being able to make free decisions, has the largest impact on PM adoption when considering factors from the Self-Determination Theory [2].

Comparing PM users to non-users, PM users have been shown to be more likely to find PMs easy to use, convenient, trustworthy, and secure [15], confirmed in our study. Non-PM users, on the other hand, see PMs as insecure and a single point of failure. They rate themselves worse at protecting their online security and feel they can do no better [15]. Further, it appears that experts are more likely to adopt PMs [48].

Ray et al. [43] demonstrated that older adults exhibit a higher mistrust in cloud storage of passwords and are afraid of the PM becoming a single point of failure. However, these barriers might be overcome by recommendations from family members, similar to social norms and influence driving adoption [1, 42]. Our results similarly confirm the important role of word-of-mouth propagation in creating PM awareness.

Finally, Lyastani et al. [30] showed that the use of a PM does not automatically bring all the potential benefits to users. PM users are still likely to choose weak passwords if they do not use a password generator (recently confirmed by Oesch et al. [40]), and even those using a password generator still end up with some weak passwords. This becomes more apparent through the effect found for Chrome auto-fill, which in the authors' analyses, was a significant precursor to password reuse. Our results similarly find higher password reuse rates for browser built-in PMs than for third-party PMs. Additional work is required to explore this further.

6.2 Technical Perspective on PMs

PMs have been found to exhibit a lack of resilience to internal observation [7]. Additionally, compatibility issues with websites have been found to persist [23, 39, 47]. Similarly, attacks that leak arbitrary credentials to attackers for several PMs also continue to persist as of 2020 [29, 39].

6.3 Password Security

As passwords are the dominant user authentication scheme [22], their security and usability has been the subject of a lot of research. One of the main usability challenges is the high number of passwords users have to manage. An average of 25 to 80 seems to be a valid approximation [17, 18, 48]. Yet, as Stobert et al. [48] note, this high number of accounts and passwords overwhelms users and drives them to insecure password management strategies. Reuse is one of the most prevalent insecure strategies, particularly for passwords users perceive as secure [20]. If a password is reused, a single leak is required to compromise all accounts protected by that password [26]. Estimates of password reuse range from 1.84 to 3.9 times per password [8, 17] or that 37% to 43% of passwords are reused across multiple accounts [13, 30].

While users generally seem to follow a well-defined password creation process, this process is sometimes based on misconceptions and produces weak passwords [34, 50]. Passwords created on mobile devices seem to be particularly easy to guess [36], similar to PINs [6, 32, 38] and unlock patterns [37] used for smartphone unlock. Further, automated approaches have been shown to rival the performance of professional password guessing specialists [52].

Mandatory password changes have also been shown to have limited security benefits, similar to PIN upgrades on smartphones [38]. Originally thought to mitigate undetected password leaks, frequent password changes hinder attackers less than originally thought [10] and lead users to create weaker passwords and derive new passwords from old ones [53]. Users, however, can be nudged towards more secure passwords. Stringent password meters seem to work well [51] and can be combined with modern password policies [46] and effective awareness materials [33]. Salience nudges also seem to hold value [27]. However, ethical aspects need to be considered when applying nudges [44].

6.4 Institution-wide Studies

Several studies have investigated passwords and two-factor authentication (2FA) at institutions. Parkin et al. [41] found in a university-wide setting that users preferred self-service password resets, despite this method's higher failure rate compared to help desk password resets. Measuring password security with a large university sample, Mazurek et al. [35] found that password guessability correlated with demographic factors and Awad et al. [5] found in their sample of a small university evidence of predictable password choice. Colnago et al. [11] recommend focusing on ease of use aspects and communication to convince users of the advantages of adopting 2FA. Dutson et al. [14] captured positive (e.g., ease of use) and negative (e.g., locked out of system) experiences after a university-wide roll-out of 2FA. Our study similarly finds that these factors can drive or hinder the adoption of PMs.

7 Conclusion

We investigated the state of Password Manager (PM) awareness and usage as well as general password habits at a private university in the United States through a large-scale quantitative study, finding that awareness and usage of PMs was generally high among our participants. Yet, password reuse was significantly lower when using third-party PMs compared to browser built-in PMs. We also found that perceived ease-of-use was the biggest factor in encouraging adoption of PMs overall, suggesting that campaigns encouraging the adoption of PMs should focus on PM's usability. Perceived security seems to play an important role for the adoption of third-party PMs. The vast majority of participants that were already using a PM, were satisfied with it. Finally, our results indicate the importance of organizations in fostering use of PMs as most users would adopt a PM if it was offered to them by an organization they are part of.

Acknowledgments

We thank Nelson Jaimes, Darika Shaibekova and Don Kim for their assistance in survey design and qualitative coding. We also thank Diane Hosfelt for shepherding this paper. This material is based upon work supported by the National Science Foundation under Grant No. 1845300. This research was further supported by funding from the topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

References

[1] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? In *Proc. EuroUSEC*, 2016.

[2] Nora Alkaldi and Karen Renaud. Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs. In *Proc. HICSS*, 2019.

[3] Fahad Alodhyani, George Theodorakopoulos, and Philipp Reinecke. Password Managers—It's All about Trust and Transparency. *Future Internet*, 12(11):189, 2020.

[4] Salvatore Aurigemma, Thomas Mattson, and Lori Leonard. So much promise, so little use: What is stopping home end-users from using password manager applications? Proc. HICSS, 2017.

[5] Mohammed Awad, Zakaria Al-Qudah, Sahar Idwan, and Abdul Halim Jallad. Password security: Password behavior analysis at a small university. In *Proc. ICEDSA*, 2016.

[6] Joseph Bonneau. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *Proc. IEEE S&P*, 2012.

[7] Joseph Bonneau, Cormac Herley, Paul C van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proc. IEEE S&P*, 2012.

[8] Alan S Brown, Elisabeth Bracken, Sandy Zoccoli, and King Douglas. Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6):641 – 651, 2004.

[9] Sunil Chaudhary, Tiina Schafeitel-Tähtinen, Marko Helenius, and Eleni Berki. Usability and Security in Password Managers: A Quest for User-Centric Properties and Features. *Computer Science Review*, 33:69–90, 2019.

[10] Sonia Chiasson and P C van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography*, 77(2-3):401 – 408, 2015.

[11] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proc. CHI*, 2018.

[12] Kaitlin Couillard. Password security survey results- part 1. Technical report, RoboForm, 2015.

[13] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The Tangled Web of Password Reuse. In *Proc. NDSS*, 2014.

[14] Jonathan Dutson, Danny Allen, Dennis Eggett, and Kent Seamons. "Don't punish all of us": Measuring User Attitudes about Two-Factor Authentication. In *Proc. EuroUSEC*, 2019.

[15] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, 7(1):12, 2017.

[16] Cori Faklaris, Laura A Dabbish, and Jason I. Hong. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proc. SOUPS*, 2019.

[17] Dinei Florêncio and Cormac Herley. A large-scale study of web password habits. In *Proc. WWW*, 2007.

[18] Ameya Hanamsagar, Simon S Woo, Chris Kanich, and Jelena Mirkovic. Leveraging Semantic Transformation to Investigate Password Habits and Their Causes. In *Proc. CHI*, 2018.

[19] Julie M. Haney and Wayne G. Lutters. "it's scary...it's confusing...it's dull": How cybersecurity advocates overcome negative perceptions of security. In *Proc. SOUPS*, 2018.

[20] S M Taiabul Haque, Matthew Wright, and Shannon Scielzo. Hierarchy of users' web passwords: Perceptions, practices and susceptibilities. *International Journal of Human-Computer Studies*, 72(12):860 – 874, 2014.

[21] Eszter Hargittai and Yuli Patrick Hsieh. Succinct Survey Measures of Web-Use Skills. *Social Science Computer Review*, 30(1):95–107, 2012.

[22] Cormac Herley and Paul C van Oorschot. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy*, 10(1):28 – 36, 2012.

[23] N. Huaman, S. Amft, 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 *Proc. IEEE S&P*, 2021.

[24] Jun Ho Huh, Hyoungshick Kim, Swathi S.V.P. Rayala, Rakesh B. Bobba, and Konstantin Beznosov. I'm too busy to reset my linkedin password: On the effectiveness of password reset emails. In *Proc. CHI*, 2017.

[25] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Proc. SOUPS*, 2015.

[26] Blake Ives, Kenneth R Walsh, and Helmut Schneider. The domino effect of password reuse. *Communications of the ACM*, 47(4):75 – 78, 2004.

[27] Shipi Kankane, Carlina DiRusso, and Christen Buckley. Can We Nudge Users Toward Better Password Management? In *Proc. CHI*, 2018.

[28] Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Christian Wiedeman, Lorrie Faith Cranor, and Julio Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Proc. IEEE S&P*, 2012.

[29] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. The emperor's new password manager: Security analysis of web-based password managers. In *Proc. USENIX Security*, 2014.

[30] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. Better managed than memorized? studying the impact of managers on password strength and reuse. In *Proc. USENIX Security*, 2018.

[31] Raymond Maclean and Jacques Ophoff. Determining Key Factors that Lead to the Adoption of Password Managers. In *Proc. ICONIC*, 2018.

[32] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. In *Proc. IEEE S&P*, 2020.

[33] Peter Mayer, Christian Schwartz, and Melanie Volkamer. On The Systematic Development and Evaluation Of Password Security Awareness-Raising Materials. Proc. ACSAC, pages 733 – 748, 2018.

[34] Peter Mayer and Melanie Volkamer. Addressing misconceptions about password security effectively. In *Proc. STAST*, 2018.

[35] Michelle L Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. Measuring password guessability for an entire university. In *Proc. CCS*, 2013.

[36] William Melicher, Michelle L Mazurek, Darya Kurilova, Sean M Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Usability and Security of Text Passwords on Mobile Devices. In *Proc. CHI*, 2016.

[37] Collins W. Munyendo, Miles Grant, Philipp Markert, Timothy J. Forman, and Adam J. Aviv. Using a blocklist to improve the security of user selection of android patterns. In *Proc. SOUPS*, 2021.

[38] Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv. "The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits. In *Proc. USENIX Security*, 2022.

[39] Sean Oesch and Scott Ruoti. That was then, this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers. In *Proc. USENIX Security*, 2020.

[40] Sean Oesch, Scott Ruoti, James Simmons, and Anuj Gautam. "It basically started using me:" an observational study of password manager usage. In *Proc. CHI*, 2022.

[41] Simon Parkin, Samy Driss, Kat Krol, and M Angela Sasse. Assessing the User Experience of Password Reset Policies in a University. In *Technology and Practice of Passwords*, volume 9551 of *International Conference on Passwords*, pages 21 – 38, Cham, 2015. Springer International Publishing.

[42] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Proc. SOUPS*, 2019.

[43] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why older adults (don't) use password managers. In *Proc. USENIX Security*, 2021.

[44] Karen Renaud and Verena Zimmermann. Guidelines for ethical nudging in password authentication. *SAIEE Africa Research Journal*, 109(2):102 – 118, 2018.

[45] Johnny Saldaña. *The coding manual for qualitative researchers*. SAGE, Los Angeles, 2nd edition, 2013. OCLC: ocn796279115.

[46] Richard Shay, Lorrie Faith Cranor, Saranga Komanduri, Adam L Durity, Phillip Seyoung Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, and Nicolas Christin. Can long passwords be secure and usable? In *Proc. CHI*, 2014.

[47] Frank Stajano, Max Spencer, Graeme Jenkinson, and Quentin Stafford-Fraser. Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers. In *Proc. PASSWORD*. 2015.

[48] Elizabeth Stobert and Robert Biddle. The Password Life Cycle. *ACM Transactions on Privacy and Security (TOPS)*, 21(3), 2018.

[49] David R. Thomas. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27(2):237–246, January 2006.

[50] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do Users' Perceptions of Password Security Match Reality? In *Proc. CHI*, 2016.

[51] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, et al. How does your password measure up? the effect of

strength meters on password creation. In *Proc. USENIX Security*.

[52] Blase Ur, Sean M Segreti, L Bauer, N Christin, L F Cranor, Saranga Komanduri, Darya Kurilova, Michelle L Mazurek, William Melicher, and Richard Shay. Measuring real-world accuracies and biases in modeling password guessability. In *Proc. USENIX Security*, 2015.

[53] Yinqian Zhang, Fabian Monrose, and Michael K Reiter. The security of modern password expiration: an algorithmic framework and empirical analysis. In *Proc. CCS*, 2010.

Appendix

A Survey Material

Purpose of Study
You are being asked to take part in a research study about the use of passwords in a variety of scenarios. You will be asked to complete a short survey that should take approximately 10 minutes and no more than 30 minutes. There are no expected costs, and you will be eligible to win a $10 gift card.
Password Management Techniques
In the following questions, you are going to be asked about your perceptions regarding password management.

1. Please describe how you manage your passwords across accounts. [free text]

2. Indicate if you have ever used any of the following password management techniques. Select all that apply.
   ☐ I remembered my passwords without writing them down or storing them digitally ☐ I reset my password every time I log in rather than remembering my password ☐ I stored my passwords in a digital file or files ☐ I saved my passwords in the browser (for example, passwords saved in Chrome) ☐ I used a third-party password manager (for example, Lastpass or Onepass) ☐ I used a system-provided password manager (for example, Apple's Keychain) ☐ I wrote my passwords down on paper or other physical media ☐ None of the above

3. Do you reuse passwords across different accounts?
   ○ Yes ○ No ○ Unsure

   If participants indicate storing their passwords as a digital file or files:

4. You indicated that you store your passwords as a digital file or files. Please answer the following questions:

   (a) I manually copy this file to multiple devices. ○ Yes ○ No ○ Unsure

   (b) I use a synchronization tool, like DropBox or Google Drive. ○ Yes ○ No ○ Unsure

   If participants indicated saving their passwords in the browser:

5. You indicated that you save your passwords in your browser (e.g., passwords saved in Chrome). Please answer the following questions:

   (a) Do you use your browser's features to make your passwords available on browsers installed on multiple devices? ○ Yes ○ No ○ Unsure

   If participants indicated using a third-party password manager:

6. You indicated that you use a third-party manager (e.g., Lastpass or 1pass) to save your passwords. Please answer the following questions:

   (a) Do you use your third-party password manager to make your passwords available on multiple devices? ○ Yes ○ No ○ Unsure

   If participants indicated using a system-provided password manager:

7. You indicated that you use the system provided PM (for example, Apple's Keychain) to save your passwords. Please answer the following questions:

   (a) Do you use your system-provided password manager to make your passwords available on multiple devices? ○ Yes ○ No ○ Unsure

   If participants indicated using multiple strategies:

8. You indicated that you use multiple strategies for managing passwords. Please describe how you combined these strategies for managing your passwords across different accounts. [free text]

General Strategies

9. Are there any other details you'd like to share about how you manage your passwords across different accounts? [free text]

Strategies For Managing the George Washington University Account Passwords
In the next section, we are interested in learning more about your password management for your university account password. This is the password you use to access your email and other George Washington University account services.

10. What strategy did you use to create your most recent George Washington University account password? [free text]

11. Why did you use that creation strategy for your most recent George Washington University account password? [free text]

12. When you are prompted to log into your George Washington University account, do you typically have the password automatically filled because you've saved it previously? ○ Yes ○ No

13. Please indicate how secure your George Washington University account password is when it is compared to other accounts where you use a password. [Much less secure, Somewhat less secure, About equally secure, Somewhat more secure, Much more secure, Unsure]

14. Please explain why you chose that level of security for your George Washington University account password. [free text]

Password Managers
In the next section questions we are going to ask you about password managers. Please read the following text carefully.

Password managers are tools that can securely handle passwords for you. They can remember your passwords, generate new ones, and even sync them across devices. **There are various types of password managers** with different features, but for the purpose of this survey, we will consider three of them. **One type of password manager is built into the web browser**, such as Chrome, Firefox, Safari, Internet Explorer, and Edge. These browsers can remember passwords for websites, as well as autofill them for you.

Another type of password manager is a third-party application (e.g., 1Password, LastPass). This can be software you install directly on to your devices or a service you can access on the web. It can also remember and/or autofill your passwords, including across browsers and devices.

Lastly, **your operating system can serve as a password manager** as well. For example, the Keychain functionality on MacOS can remember passwords in and out of your browser. It can also be used with iCloud to sync passwords across Apple devices.

Ultimately, the main purpose of password managers is to automatically handle your passwords for you.

15. Based on this description, do you use a password manager? (Select all that apply)
    ☐ I save my passwords in the browser (for example in Chrome).
    ☐ I use a third-party manager (for example, Lastpass or Onepass).
    ☐ I use a system provided password manager (e.g. Apple's Keychain).
    ☐ I do not use a password manager.

    If participants indicated using at least one of the above PMs:

16. 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 ○ I don't know (don't remember, not sure) ○ I first heard about it in this study ○ Other [free text]

17. 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 my 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.

Password Manager Users

18. What is the main reason you do use a password manager? [free text]

19. Which of the following password managers do you use most frequently?
○ LastPass ○ 1Password ○ Dashlane ○ KeePass ○ EnPass ○ Kaspersky Password Manager ○ Apple Keychain ○ Firefox ○ Chrome ○ Other

20. How satisfied are you overall with your experience using *[PM selected above]*? [Moderately satisfied, Slightly satisfied, neither satisfied nor dissatisfied, slightly dissatisfied, moderately dissatisfied, extremely dissatisfied]

21. 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 PM stores it for me.
○ I create the password myself and recall it without storing it in the password manager.

22. What do you like the most about using a password manager?
○ 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 ○ None of the above ○ Other

23. What do you like the least about using a password manager?
○ I have security concerns ○ Master password concerns ○ 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 ○ None of the above ○ Other

If participants indicated disliking something about the PM above:

24. You mentioned that *[least liked feature mentioned above]* was what you liked least about using a password manager. Please explain your answer? [free text]

Non-Password Manager Users

25. What is the main reason you do not use a password manager?

26. Have you used a password manager in the past? ○ Yes ○ No

If participants indicated using a password manager in the past:

27. When did you stop using the password manager and what was the main reason why? [free text]

If participants indicated not using a password manager in the past:

28. Could you imagine adopting a password manager? If so, for what main reason? [free text]

If participants indicated using a PM in the past:

29. Could you imagine using a PM again? If so, why? [free text]

Password Manager Adoption

30. 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 likely, Moderately likely, Slightly likely, Neither likely nor unlikely, Slightly unlikely, Moderately unlikely, Extremely unlikely]

IT Skills

31. 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 the 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.

32. Which of the following describes you best?
○ I am majoring / have a degree in IT security ○ I am majoring / have a degree in CS or a closely related field ○ I work in the field of IT security ○ None of the above ○ Prefer not to disclose

33. How well are you familiar with the following computer and Internet-related items? [No understanding, Low understanding, Medium understanding, High understanding, Full understanding] (a) Advanced search (b) PDF (c) Spyware (d) Wiki (e) Cache (f) Phishing

Demographics

34. What is your gender?
○ Woman ○ Man ○ Non-binary ○ Prefer not to disclose ○ Prefer to self describe [free text]

35. What is your age? ○ My age is [free text] ○ Prefer not to disclose

36. Are you Hispanic, Latino/a, or of Spanish origin? (One or more categories may be selected)
☐ No, not of Hispanic, Latino/a/x, or Spanish origin ☐ Yes, Mexican, Mexican American, Chicano/a/x ☐ Yes, Puerto Rican ☐ Yes, Cuban ☐ Yes, Another Hispanic, Latino/a or Spanish origin ☐ Prefer not to disclose

37. Which of the following racial designations best describes you? (One or more categories may be selected)
☐ White ☐ Black or African American ☐ American Indian or Alaska Native ☐ Chinese ☐ Filipino ☐ Asian Indian ☐ Vietnamese ☐ Korean ☐ Japanese ☐ Other Asian (for example, Pakistani, Cambodian, and Hmong) ☐ Native Hawaiian ☐ Samoan ☐ Google/Pixel/Nexus ☐ Chamorro ☐ Other Pacific Islander (for example, Tongan, Fijian, and Mashallese) ☐ Other (Designation not listed here) [free text] ☐ Prefer not to disclose

Raffle and Future Studies

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

If participant is willing to be contacted for future studies or the raffle:

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

B Codebook

• NA (224) • easy-to-remember (160) • memorize (134) *frequent (18), primary (10), sensitive (9), financial (5), reuse (4), outdated (3), guess-from-variations (2), similar-passwords (2), work (1), own (1), difficult (1), hard-to-recall-strong-pwds (1), typed-where-no-pm (1), SSO (1), multiple-devices (1), simple-pwds (1), not-browser (1), non-sensitive (1), familiar-ones (1), mnemonics (1), personal-system (1), never-changed (1)* **• secure (99)** *uni-protection (3)* **• password-manager (91)** *lastpass (27), icloud (16), google-auto-fill (14), 1password (11), password-safe (3), keepassxc (2), apple-key-ring-feature (1), keypass (1), chrome (1), firefox (1), vault-password (1), roboform (1), bitwarden (1), ewallet (1), dropbox (1), store-by-root-kdbx-database (1), vault (1)* **• memorable (85)** *uni-associated (1)* **• reuse (84)** *new-variation (34), same-as-other-accounts (8), from-previous-employment (4), work (2), non-sensitive (1), not-more-than-three-times (1), outdated (1), from-high-school (1), ensure-memorability (1), infrequent (1)* **• keep-record (78)** *hard-copy (32), save-in-excel (13), digital (11), notes-app (9), cell-phone (7), email (1)* **• numbers (75) • multiple-variations (70)** *category-dependent (4), unimportant-accounts (3)* **• same-password (63)** *uni-associated (7), category (5), similar-category-accounts (4), no-more-than-three-accounts (1), unimportant-accounts (1)* **• browser (63)** *chrome (23), non-sensitive (8), primary (5), frequent (4), sync (4), outdated (3), infrequent (3), firefox (2), convenient (2), trivial (2), autofill (2), not-preferred (1), no-regular-change (1), work (1), non-reuse (1), sensitive (1), no-sync (1), streaming-and-social-media (1), ease-of-use (1), complex-pwds (1), non-financial (1)* **• digitally (62)** *file (23), notes-app (16), local (3), google-drive (3), non-sensitive (2), password-protected (2), infrequent (2), saved (1), work (1), screenshot (1), sensitive (1), forgotten-multiple-times (1), phone (1), phone-autofill (1), email-self (1), google-doc (1), not-guessing (1), ease-of-use (1), regular-change (1), files (1), in--programs (1)* **• easy-login (60) • paper (60)** *sensitive (9), infrequent (8), outdated (7), regular-change (3), complex-passwords (2), if-difficult-to-remember (2), initially (2), shared-accounts (2), primary (2), incidentally (1), reminders (1), reuse (1), work (1), not-standard-set (1), difficult-pwds-that-cannot-be-pasted (1), obfuscated-notes (1), non-sensitive (1), unique (1), if-no-cookies (1), device-specific (1)* **• different-passwords (45)** *randomly-generated (11), important-accounts (7), category-dependent (4), non-sensitive (1), difficult (1)* **• important-account (45)** *more-secure (8), secure-base–password (1)* **• symbols (45) • letters (43) • convenient (43) • special-character (31) • helps-keep-track (31) • strong-password (30) • third-party (29)** *primary (13), last-pass (10), personal (5), 1password (5), keepass (2), sensitive (2), dashlane (1), financial (1), work (1), roboform (1), outdated (1), phone (1), overwhelming (1), password-safe (1), infrequent (1)* **• reuse-strategy (29) • system (25)** *keychain (23), non-sensitive (4), convenient (3), personal (2), primary (2), outdated (1), non-cross-platform (1), phone (1), not-often-typed (1), infrequent (1)* **• something-personal (25) • lacks-trust (24)** *security (17), privacy (3)* **• difficulty-remembering (24) • dont-need-to-remember (24)** *lazy (3)* **• redundancy (21) • authentication (21) • unique (20) • same-strategy (20) • transition (19) • similar-passwords (19)** *variation (4), non-sensitive (2), reuse (1), not-writing-down (1), outdated (1)* **• dont-need-it (18)** *use-different-solution (4), good-memory (1)* **• date (18)** *month (3)* **• phrase (17) • saves-time (17) • single-sign-on (16) • capital-letters (15) • hard-to-guess (15) • word (15) • password-requirement (14) • reset (14)** *if-forgotten (6), infrequent (4), financial (1), pwd-on-different-device*

(1), complex-pwd (1), specific-system (1), not-big-deal (1) • **personally-related (14)** *memorable (10)* • **association (13)** *uni (8), school (2), job (2)* • **characters (13)** • **unrelated-response (13)** • **avoid-repeat-typing (13)** • **random-password (12)** • **no-strategy (11)** • **satisfies-security-requirement (11)** • **name (11)** *family (3), pet (2), celebrity (1), hero (1)* • **saved-in-browser (11)** *frequent (1)* • **randomized (10)** • **personally-created (10)** • **same-level-of-security-as-other-accounts (10)** • **do-not-want-to-be-hacked (10)** • **able-to-have-unique-passwords (10)** • **pm (10)** *primary (3), regular-changes (1), outdated (1), work (1), similar-passwords (1), frequent (1), overwhelmed (1), infrequent (1)* • **frequent-login (9)** • **didnt-know-about-it (9)** • **difficult-password-organization (9)** • **different-strategy-by-category (9)** • **several-passwords-reused (9)** *four (4), three (4), two (1)* • **random (9)** *characters (1), numbers (1)* • **able-to-have-stronger–passwords (9)** • **used-required-elements (9)** • **frustration (8)** *two-factor-authentication (3), forced-reset-password (2)* • **no-management (8)** *ad-hoc (3), chaotically (1)* • **secure-place (8)** • **difficult-remembering-passwords (8)** • **do-not-know-how-secure (8)** • **lacking-knowledge (8)** *technical-skills (3)* • **not-important-account (7)** *uni-not-high-target (3)* • **automatically-available (7)** • **work-vs-personal (7)** • **no-reason (7)** • **used-password-generator (7)** *from-norton (1), password-safe (1)* • **password-protected (7)** • **it-works (6)** • **only-used-for-some-passwords (5)** • **non-pm (5)** *outdated (4), financial (1)* • **lowercase-letters (5)** • **sentence (5)** • **initials (5)** *pets (1), of-random-objects (1), personal (1)* • **reset-passwords (5)** *often (2)* • **alphanumeric (4)** • **dislike-password-manager (4)** *no-manual-entry (1), no-trust (1), time-consuming (1)* • **for-personal-use (4)** • **decline-to-answer (4)** • **two-step-authentication (4)** • **will-not-use-pm-again (4)** *need-remote-access-at-all-times (1), can-be-hacked (1)* • **uni-account (4)** • **received-recommendation (4)** • **no-issues (4)** • **rely-on-computer-to-save (4)** • **reuse-passwords (3)** • **prefer-not-to-use-password-manager (3)** • **cookies (3)** *frequent (1)* • **worried-about-security (3)** • **physically-store-passwords (3)** *print-out (1)* • **family-member-attribute (3)** • **created-new-password (3)** *did-not-allow-to-use-old-password (1)* • **prefer-one-password (3)** • **too-much-steps (3)** • **prefer-not-creating-new-passwords (3)** • **remember-me-feature (3)** • **difficult (3)** • **important-information (3)** • **personally-unrelated (3)** • **use-forgot-my-password (2)** • **able-to-have-randomized-passwords (2)** • **words (2)** • **autopopulate (2)** • **sync-accross-devices (2)** • **possibly (2)** • **fingerprint-authentication (2)** • **saved-via–cookies (2)** • **trust (2)** • **uni-generated-password (2)** • **forced-to-change-password (2)** • **not-for-work (2)** • **season (2)** • **memorize-passwords (2)** • **for-school (2)** • **required–to-use (2)** • **easy-password (2)** • **event (2)** • **simple (2)** • **store-in-phone (2)** • **at-risk (2)** • **dont-use (2)** • **ease-of-use (2)** • **password-access-across-devices (2)** • **cross-p-m-sync (2)** *not-sensitive (1)* • **save-in-emails (1)** • **dont-need-to-reset-passwords (1)** • **same-formulaic-approach (1)** • **password-formula (1)** • **prefer-password-manager (1)** • **considering-using-password-manager (1)** • **stopped-after-few-days (1)** • **saves-energy (1)** • **pwd-relates-to-self (1)** • **do-not-know-password-manager (1)** • **depends-on-location (1)** • **maybe (1)** • **non-systematic (1)** • **long (1)** • **firefox-algorithm (1)** • **anagram (1)** • **want-control-over-account (1)** • **returned-to-keychain (1)** • **not-against (1)** • **rely-on-google-security (1)** • **song-lyrics (1)** • **complicated (1)** • **dislike (1)** • **not-effective (1)** • **mnemonic (1)** • **no-cookies (1)** *financial (1), infrequent (1)* • **unify-passwords (1)** • **own-vs-others (1)** • **school-password (1)** • **secure-server (1)** • **cannot-tell (1)** • **incrementation (1)** • **unique-profile-identifier (1)** • **dont-use–password-manager (1)** • **fantasy-world (1)** • **received-email-with-personal-data-stored-in-password-manager (1)** • **difficulty-managing-passwords (1)** • **combination–makes-management-possible (1)** • **pwd-variation (1)** *number (1)* • **friend-attribute (1)** • **make-it-work (1)** • **able-to-share-passwords (1)** • **MFA-procedure (1)** *important-accounts (1)* • **feel-confident (1)** • **if-easier-to-use (1)** • **like-password-manager (1)** • **two-university-passwords (1)** • **do-not-remember (1)** • **feel-unsafe (1)** • **obfuscated-notes (1)** • **lazy (1)** • **different-strategies-for-different-platforms (1)** • **dont-care (1)** • **place (1)** • **store-in-spreadsheet (1)** • **best-right-now (1)** • **personal-joke (1)** • **not-familiar-with-security (1)** • **acronym (1)** • **efficient (1)** • **occasional-use (1)** • **exceed-password-requirements (1)** • **store-on-laptop (1)** • **did-not-keep-active (1)** • **no-patience (1)** • **rotating-suffix (1)** • **consistent-system (1)** • **mental-cypher (1)** • **do-not-prefer-random-passwords (1)** • **expire-at-different-times (1)** • **no-sync (1)** • **personal-use (1)** • **google-security (1)** • **if-needed (1)** • **impacted-ability-to-access-accounts (1)** • **weak-password-strength (1)** • **stopped-working-on-computer (1)** • **prefer-two-factor-authentication (1)** • **pseudoencryption (1)** • **store-on-usb (1)** • **open-to-use (1)** • **saved-in-google-account (1)** • **does-not-help (1)** • **not-sure (1)** • **use-apple-key-chain (1)** • **hackers-can-outsmart (1)** • **cannot-memorize-all (1)** • **non-reuse (0)** *more-unique (1)* • **long-random (0)** *sensitive (1)* • **uni-acount (0)** *unique-password (1)* • **non-memory (0)** *infrequent (1)*

C Additional Regressions

The following tables show the results for the regressions pertaining to users' adoption of one type of PM. Significant factors are marked in bold italic.

Table 8: Logistic regression for adoption of browser PMs.

	Est.	OR	95% CI	p-val
(Intercept)	0.81	2.26	[0.41, 13.05]	.354
SA-6	***-0.33***	***0.72***	***[0.53, 0.95]***	***.025***
Web Skill	0.14	1.15	[0.75, 1.80]	.524
Security: Agree (vs Disagree)	−0.40	0.67	[0.27, 1.65]	.383
Tranquility: Agree (vs Disagree)	−0.28	0.75	[0.28, 2.02]	.567
Fun: Agree (vs Disagree)	−0.28	0.76	[0.32, 1.81]	.526
Ease of Use: Agree (vs Disagree)	***1.09***	***2.99***	***[1.45, 6.30]***	***.003***
Difficulty: Agree (vs Disagree)	−0.40	1.49	[0.35, 6.47]	.588
Annoyance: Agree (vs Disagree)	−0.21	0.81	[0.30, 2.20]	.671
Transparency: Agree (vs Disagree)	−0.08	0.92	[0.42, 2.02]	.831
Trust: Agree (vs Disagree)	0.27	1.31	[0.63, 2.78]	.476
Uni. account: More secure (vs Less secure)	0.01	1.01	[0.52, 1.96]	.975
Role: Student (vs Non-student)	0.371	1.45	[0.74, 2.89]	.285
Gender: Woman (vs Man)	0.10	1.10	[55, 2.19]	.787

Table 9: Logistic regression for adoption of third-party PMs.

	Est.	OR	95% CI	p-val
(Intercept)	***-6.03***	***416.34***	***[>0.00, 0.02]***	***<.001***
SA-6	***0.48***	***1.62***	***[1.06, 2.60]***	***.033***
Web Skill	−0.06	0.95	[0.49, 1.81]	.866
Security: Agree (vs Disagree)	***2.76***	***12.82***	***[4.73, 61.28]***	***<.001***
Tranquility: Agree (vs Disagree)	−1.15	0.32	[0.08, 1.31]	.087
Fun: Agree (vs Disagree)	0.20	1.22	[0.37, 3.92]	.743
Ease of Use: Agree (vs Disagree)	0.56	1.76	[0.53, 6.40]	.369
Difficulty: Agree (vs Disagree)	0.44	1.56	[0.22, 10.54]	.648
Annoyance: Agree (vs Disagree)	0.34	1.40	[0.38, 5.03]	.601
Transparency: Agree (vs Disagree)	***1.59***	***4.91***	***[1.69, 15.76]***	***.005***
Trust: Agree (vs Disagree)	0.77	2.15	[0.77, 6.27]	.0.15
Uni. account: More secure (vs Less secure)	0.38	1.46	[0.57, 3.76]	.427
Role: Student (vs Non-student)	***-1.14***	***3.11***	***[0.11, 0.85]***	***.028***

Table 10: Logistic regression for adoption of OS built-in PMs.

	Est.	OR	95% CI	p-val
(Intercept)	***-3.10***	***0.05***	***[0.01, 0.18]***	***<.001***
SA-6	0.06	1.06	[0.83, 1.35]	.651
Web Skill	0.24	1, 27	[0.89, 1.81]	.0.191
Security: Agree (vs Disagree)	−0.01	0.99	[0.42, 2.35]	.982
Tranquility: Agree (vs Disagree)	−0.58	0.56	[0.23, 1.32]	.189
Fun: Agree (vs Disagree)	−0.58	0.56	[0.26, 1.17]	.133
Ease of Use: Agree (vs Disagree)	***1.34***	***3.83***	***[1.89, 8.27]***	***<.001***
Difficulty: Agree (vs Disagree)	0.48	1.62	[0.44, 5.64]	.457
Annoyance: Agree (vs Disagree)	0.38	1.47	[0.68, 3.14]	.324
Transparency: Agree (vs Disagree)	0.45	1.56	[0.82, 2.99]	.173
Trust: Agree (vs Disagree)	0.32	1.38	[0.75, 2.52]	.298
Role: Student (vs Non-student)	0.39	1.48	[0.83, 2.64]	.186

D Artifact Appendix

D.1 Abstract

This artifact comprises several files that aid in the replication of our study: (1) a QSF-file containing all questions in a survey format exported from Qualtrics and that can be easily re-imported there); (2) a CSV-file with the the data collected from our participants with identifiable information removed (to improve compatibility, also a tab-separated version is provided); (3) the analysis script with the majority of the quantitative analyses of the paper; (4) a Jupyter Notebook file with the CHI-squared test; (5) the codebook of the qualitative analysis with counts for each of the codes. Using the data set and the analysis script, all quantitative results in the paper can be replicated.

D.2 Artifact check-list (meta-information)

- **Program:** The analysis was run with R version 4.2.0 running in RStudio[3] 2022.02.3 Build 492 with knitr. The following packages are needed to run the script: dplyr, AICcmodavg. For the chi-squared test, we used a Jupyter Notebook, version 6.4.8 to conduct the analysis. The easiest way to use Jupyter Notebook is to install Anaconda [4] which comes pre-installed with the most popular Python libraries and tools. Anaconda navigator version 2.2.0 as well as Python version 3.9.12 were used for this analysis. The following packages are required to run this script: pandas, numpy, scipy, statsmodels.
- **Compilation:** Some of the R packages and their dependencies require compilation, but R should handle this automatically when installing the packages.
- **Data set:** The data set collected from the participants of our study is included in the artifact
- **Run-time environment:** Recommended is use of RStudio 2022.02.3 Build 492 with R 4.2.0. Other configurations are likely to work but are untested. A Jupyter Notebook version 6.4.8 is recommended but not required to run the .ipynb. You can easily access the Jupyter Notebook by installing Anaconda. All our analyses were run on macOS.
- **Hardware:** No specific hardwre is needed.
- **Output:** The output on the R console and Jupyter Notebook represent the analyses as they were reported in the paper.
- **Experiments:** For a full replication of our study, the QSF-file can be used to import the survey back into qualtrics and distribute it among new participants. Note that the survey requires Javascript and therefore will not work with free Qualtrics accounts. For replication of the results reported in the paper, the analysis script and the data set collected from our participants should be used.
- **How much disk space required (approximately)?:** Negligible, less than 1MB.
- **How much time is needed to prepare workflow (approximately)?:** This depends on whether the required environment (RStudio and Anaconda) and the required packages are already installed. If none of the aforementioned are present, setup should take 30 minutes or less on a modern computer.
- **How much time is needed to complete experiments (approximately)?:** This depends on hardware, but should take less than 5 minutes on any recent laptop.
- **Publicly available (explicitly provide evolving version reference)?:** The artifact will be made available in a GitHub repo with a tag marking the version submitted for the artifact evaluation.
- **Code licenses (if publicly available)?:** The R code and Jupyter Notebook script are lincensed under the MIT license.
- **Data licenses (if publicly available)?:** The data is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.[5]
- **Archived (explicitly provide DOI or stable reference)?:** GitHub Commit ID for the version submitted for artifact evaluation: 2ead79bbe026789bc78d87b420c487da4d980ff5
  GitHub Commit ID for the version improved with the comments from artifact evaluation reviews:
  a90e474e2e2be23898b4b85570cd0daaba61970f

D.3 Description

D.3.1 How to access

The artifact can be downloaded from the GitHub repository.[6]

D.3.2 Hardware dependencies

N/A

D.3.3 Software dependencies

The analysis requires R to run. Recommended is RStudio 2022.02.3 Build 492 with R 4.2.0, since the authors used these versions. Other versions are likely to work but are untested. RStudio can be obtained for free online.[7] The following R packages are needed to run the script: dplyr, AICcmodavg. For the chi-squared script, Jupyter Notebook version 6.4.8 is recommended but not required. To quickly use Jupyter Notebook, download Anaconda. [8]

D.3.4 Data sets

No third-party data sets were used.

D.3.5 Models

N/A

[3] https://www.rstudio.com/products/rstudio/download/
[4] https://www.anaconda.com/products/distribution
[5] http://creativecommons.org/licenses/by-nc-nd/4.0/
[6] https://github.com/gwusec/2022-USENIX-Password-Managers
[7] https://www.rstudio.com/products/rstudio/download/
[8] https://www.anaconda.com/products/distribution

D.3.6 Security, privacy, and ethical concerns

N/A

D.4 Installation

The setup consists of two steps. First, R needs to be installed. Recommended is RStudio 2022.02.3 Build 492 with R 4.2.0, since the authors used these versions. Other versions are likely to work but are untested. RStudio can be obtained for free online.[9] After the installation of RStudio, R should be available as well.

When RStudio is installed it must be started and the analysis script can be opened using the `File` dialog. Then the following R packages need to be installed: dplyr, AICcmodavg. To install these packages using RStudio, open the `Tools` menu and then select `Install packages...`. In the search box enter the first package. Then click `install`. Repeat these two steps for the second package. Installation of the packages might take some time if they need to be compiled. Once the two packages are installed, the analysis script can be run.

To run the .ipynb stats script that has the chi-squared test, first ensure you have Python installed as well as all the required dependencies. Python version 3.9.12 was used for this analysis. In addition to Python, the following dependencies also need to be installed: pandas, numpy, scipy, statsmodels. You can install them one by one from the terminal using pip (which is automatically installed with Python):

```
pip install pandas
pip install numpy
pip install scipy
pip install statsmodels
```

Once Python and all the above dependenices have been installed, you will be ready to run the Jupyter Notebook script. It is recommended you download Anaconda which comes pre-installed with Jupyter Notebook. Anaconda can be obtained for free online.[10] Once Anaconda is installed, open it and launch Jupyter Notebook, and browse to the location of the script. Run all the cells, one by one from top to bottom. It should print the results to the screen.

D.5 Experiment workflow

The R analysis script is divided into several segments called "chunks", each pertaining to the preparation of a specific variable or performing a specific analysis. These chunks are delimited by three accents before and after the block. Each chunk is labeled. The label is enclosed by curly brackets. The respective syntax looks like this:

```
```{r <section label>}
    <R code>
```
```

The easiest way to run the analyses is to run the script chunk-by-chunk from the top in RStudio. Running a chunk can be achieved in RStudio in three ways. Firstly, RStudio provides a small green right-arrow button on the top right for each chunk. Clicking it will run the respective chunk. Secondly, with the curser in a chunk, you can use the shortcut `Ctrl + Shift + Enter` (on macOS: `Cmd + Shift + Enter`) to run the respective chunk. Thirdly, with the curser in a chunk, you can use the menu `Code` → `Run Region` → `Run Current Chunk`.

The Jupyter Notebook script is similarly divided into several cells. Run the cells one by one, from the top to the bottom and the results will be displayed on the screen.

D.6 Evaluation and expected results

Claim 1: Awareness and use of PMs is much broader than previously reported The overall high awareness and use of password managers are supported by the analyses in section "prepare pwdm awareness variable" and "prepare password manager use variable" respetively.

Claim 2: The vast majority of respondents reuse passwords across accounts The results pertainig to password reuse can be found in section "RQ-2 reuse."

Claim 3: Perceived ease-of-use overall plays a key role in password manager adoption The results for the regression analysis identifying ease-of-use as predictor when all PM-users are considered can be found in section "pwdm use." The regression analyses for only browser-based password managers, system password managers, and third-party password managers can be found in the sections "browser pwdm use," "system pwdm use," and "third-party pwdm use" respectively.

Claim 4: Third-party password manager users are significantly more likely to use the PM to generate passwords The results for this can be replicated by running the Jupyter Notebook file called chi_test.ipynb. These will be printed to the screen.

Claim 5: The majority of participants would adopt a PM if it was offered to them for free by their organization The analysis pertaining to the adoption of password managers when one is offered by the participant's organization can be found in section "prepare pwdm use in organization variable."

D.7 Experiment customization

N/A

D.8 Version

Based on the LaTeX template for Artifact Evaluation V20220119.

[9] https://www.rstudio.com/products/rstudio/download/
[10] https://www.anaconda.com/products/distribution