"Would You Give the Same Priority to the Bank and a Game? I Do Not!" Exploring Credential Management Strategies and Obstacles during Password Manager Setup

Sabrina Klivan, *CISPA Helmholtz Center for Information Security;*
Sandra Höltervennhoff and Nicolas Huaman, *Leibniz University Hannover;*
Yasemin Acar, *George Washington University and Paderborn University;*
Sascha Fahl, *CISPA Helmholtz Center for Information Security and Leibniz University Hannover*

https://www.usenix.org/conference/soups2023/presentation/klivan

This paper is included in the Proceedings of the Nineteenth Symposium on Usable Privacy and Security.

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

Open access to the Proceedings of the Nineteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

"Would You Give the Same Priority to the Bank and a Game? I Do Not!"
Exploring Credential Management Strategies and Obstacles during Password Manager Setup

Sabrina Klivan[C] Sandra Höltervennhoff[L] Nicolas Huaman[L] Yasemin Acar[WP]
Sascha Fahl[CL]

[C] *CISPA Helmholtz Center for Information Security*
[L] *Leibniz University Hannover*
[W] *George Washington University*
[P] *Paderborn University*

Abstract

Password managers allow users to improve password security by handling large numbers of strong and unique passwords without the burden of memorizing them. While users are encouraged to add all credentials to their password manager and update weak credentials, this task can require significant effort and thus jeopardize security benefits if not completed thoroughly. However, user strategies to add credentials, related obstacles, and their security implications are not well understood. To address this gap in security research, we performed a mixed-methods study, including expert reviews of 14 popular password managers and an online survey with 279 users of built-in and third-party password managers. We extend previous work by examining the status quo of password manager setup features and investigating password manager users' setup strategies. We confirm previous research and find that many participants utilize password managers for convenience, not as a security tool. They most commonly add credentials whenever a website is visited, and prioritize what they add. Similarly, passwords are often only updated when they are considered insecure. Additionally, we observe a severe distrust towards password managers, leading to users not adding important passwords. We conclude our work by giving recommendations for password manager developers to help users overcome the obstacles we identified.

1 Introduction

Despite investigations into new online authentication standards [11, 17, 41, 67], usernames and passwords remain the most widely used. Users need to manage an enormous amount of online credentials, which has only increased with the growth of online communication during the recent global pandemic [34, 69]. Due to the number of accounts, users face an immense cognitive burden when creating and memorizing strong and unique passwords for all of them [23, 24, 49, 52, 70, 71, 73].

A promising way to mitigate the above challenges is the use of password managers (PWMs). They allow users to maintain all their passwords and often additional information such as credit card data, addresses, or two-factor authentication secrets behind a single master password. Users therefore only need to memorize this one password, removing most of the cognitive load [59, 63]. Most PWMs furthermore provide password security checks, the generation of strong passwords [33, 46], and provide auto-save and autofill features. However, the initial PWM setup requires a lot of time and effort: Users need to choose and install a PWM as well as potential web browser extensions, gather their online accounts, add them one by one into the PWM and ideally also update weak, re-used or leaked passwords. All of this is time-consuming and requires users to have a list of all of their accounts ready if they want to set up their PWM as quickly as possible, but composing this list is often a challenging task. On the other hand, the effective security benefits of PWM are reduced if users do not add and upgrade their credentials when adopting the PWM, as passwords might remain reused or easily guessable. In this work, we extend previous work and aim to understand what strategies users actually apply during their initial PWM setup. This includes how they add new or existing passwords, if and how old passwords are updated, users' thought processes and perceptions, and finally, which obstacles they face during the setup. Based on our findings, we give recommendations to PWM developers on how to improve the process and help PWM users with password management tasks.

We initially collect helpful features for new users when first setting up a PWM by conducting an expert review, evaluating several popular PWMs. Based on this expert review and

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

extensive piloting to collect potential management strategies, we follow up with a survey with 279 users of built-in and third-party PWMs. To the best of our knowledge, we are the first to investigate PWM setup support features and credential management strategies users apply when setting up their PWMs.

In this work, we aim to answer the following research questions:

- **RQ1**: *What setup features do password managers offer to new users, who want to add their existing credentials?*
- **RQ2**: *What are common user strategies to add new and existing credentials? Why are these strategies used?*
- **RQ3**: *How can password manager developers help users with setup, and improve the overall process?*

Overall, we make the following contributions:

Existing Setup Features. We perform expert reviews of 14 popular PWMs and present and evaluate current built-in tools and features that help users to add new and existing credentials as quickly as possible, and to identify and update potentially weaker passwords efficiently.

Strategy Identification. We provide a first exploratory investigation, in which we identify seven PWM credential management strategies end users adopt, and obstacles they face during setup.

Frequency of Strategies and Issues. We design and conduct a survey study with 279 participants and report how common respective strategies and issues are. Furthermore, we investigate the reasons that influence users' strategy decisions.

Recommendations for Developers. Based on our findings, we give recommendations on how PWM developers could improve the setup process or aid (first time) users with the setup of their PWM, to help them improve their password strength and fully benefit from PWMs.

Replication Package Availability. To increase research transparency and allow for easier replication, we provide a comprehensive collection of our research artifacts on a complimentary website, including videos from our expert review, all text material from our survey, and additional aggregated survey results[1].

2 Basic Features of Password Managers

In the following, we present the prominent PWM functionalities, to help understand which tasks users face when initially adopting a PWM, and in which ways security and usability are influenced by them.

Store Credentials: At their core, PWMs are simple databases that store sensitive information including username and password pairs, and encrypt them using a master password.

Password Generation: PWMs can generate unique and strong passwords that end users can use when updating existing, or creating and storing new passwords. These generators often come with many options, allowing users to set length, include or exclude certain characters, and gain feedback on password strength. However, these generators can struggle with services' password policies, as websites might, e. g., not permit certain symbols and force users to manually adjust the generator's settings [26, 28, 36].

Auto-save/Auto-fill: Although this often requires separate browser extensions, PWMs can detect visited websites and login forms, and automatically save entered credentials, or match the website to a known one and automatically fill the credentials in. While this streamlines the user experience and increases usability, it requires the PWM to recognize the service as well as the login form correctly, which previous work found to be a non-trivial process [26]. Some PWMs further support fully automated logins [18, 35].

Additional Data: Many PWMs can also store additional data, e. g., addresses, credit card data, or secrets required to generate Time-Based One-Time Passwords (TOTPs). Additionally, some PWMs can not only store these secrets, but to also generate and autofill valid TOTPs [59].

Synchronization: Some PWMs offer applications on different devices, therefore enabling end users to access their passwords on multiple devices such as private or work computers, smartphones and more. In these cases, the encrypted password database is usually stored in a cloud. While some PWMs such as 1Password [1] provide fully automatic cloud synchronization, other purely offline PWMs such as KeePassXC [32] only support multiple devices if end users share or synchronize the encrypted database file with themselves.

3 Related Work

In the past, adoption sentiments as well as the usability of PWMs was researched exhaustively. We present and discuss related work in two key areas: *Motivation to Use Password Managers* and *Password Manager Usability*, and illustrate how our work extends previous studies and fills an important research gap.

3.1 Motivation to Use Password Managers

In 2016, Alkadi and Renaud collected reviews of two popular PWMs from Android and Apple app stores. Based on the user sentiments, they designed a survey and report an extensive list of reasons for and against PWM use, such as ease of use, perceived usefulness, cost, perceived effort and privacy or security concerns [4]. Similarly, in 2017, Fagan et al. conducted a survey with 137 users and 111 non-users of PWMs to understand their motivations. They find users to be mainly

[1] https://publications.teamusec.de/2023-soups-pwm-adoption/

driven by convenience and usability factors, while non-users mention security concerns [21]. In 2017, Aurigemma et al. surveyed 283 undergraduates to understand why they do not use PWMs, even if they have high intentions to do so. Their study indicates that users do not adopt PWMs due to various concerns about trust, costs or actual benefits, and that even users who are interested in PWM usage are inhibited by time constraints and a lack of immediate threats [7]. A 2018 survey conducted by Maclean and Ophoff examines adoption intentions based on technology acceptance and use, and finds the expectancy of functionality, trust into the system, and that usage becomes a habit to be leading factors [42]. Ayyagari et al. performed a survey in 2019 to investigate the low adoption rates of PWMs and report that the perceived severity of password loss consequences greatly influences end users' likelihood to use PWMs [8]. In 2021 Albayram et al. conducted a series of surveys to examine the impact of motivational text and video material about the benefits of PWMs on improving the understanding and adoption rate of PWMs. They find that both increased user comprehension, but that video material resulted in a higher adoption rate [3].

While the majority of these works researched mindsets of users that do not necessarily use PWMs, our work focuses on the experiences PWM users have when adding and maintaining passwords. Furthermore, our work provides insight into the impact of issues PWM users encounter, allowing us to determine the most important issues currently blocking the adoption of PWMs.

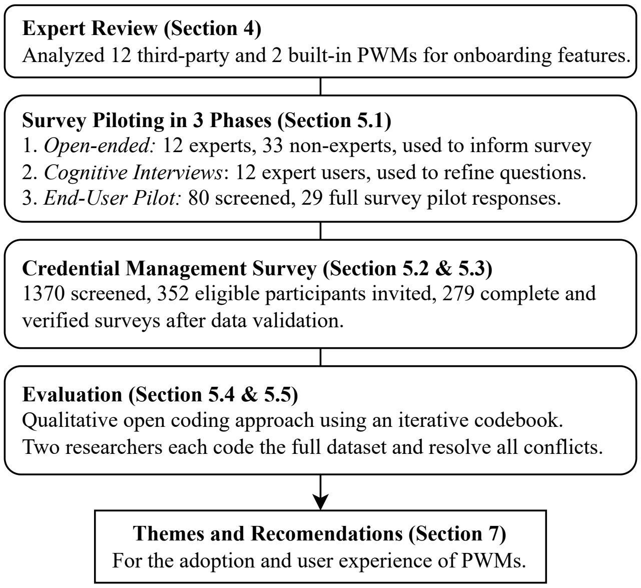
3.2 Password Manager Usability

Below, we discuss previous research that focuses on the usability of PWMs, as this can have a high impact on how likely end users keep or abandon a PWM. In 2006, Chiasson and van Oorschot compared the usability of two proposed PWMs in a user study. They find their participants to have strong misconceptions and conclude that not only were usability issues present, but that some of them could also lead to security problems [15]. Another usability comparison was conducted in 2010, when Karole et al. asked end users to test three different PWMs. They find that users preferred portable variants over an online PWM despite reporting lower usability, most likely due to concerns against storing passwords online [30]. Lyastani et al. conducted an in-situ examination of PWM usage and usability in 2018 and found that while PWMs increase security, the degree of this is highly dependent on a combination of password creation, storage, and entry behaviors as well as user's PWM choice [40]. In 2019, Alkadi et al. developed and distributed a recommendation app that allowed users to set several preferences and suggested the best-fitting PWM. Overall, only 5% reported installing and using it. Participants stated that the effort to set the PWM up, lack of trust and external factors such as lack of storage space are main reasons against the installation [5]. In the same year, Seiler-Hwang et al. instructed users to install a PWM on their phone and collected usability feedback with a survey. They find that even popular smartphone PWMs have severe usability deficiencies [65]. Also in 2019, Chaudhary et al. conducted a systematic literature review of 32 academic PWM proposals and examine them for usability and security. Discovering that most proposals are biased towards security and lack usability, they give recommendations for usability enhancements to PWM manufacturers [13]. Pearman et al. reported a series of semi-structured interviews in 2019, examining to what extent users utilized additional features such as strong password generation. They find that users of built-in PWMs without additional features often apply weaker passwords, and that the reasons to adopt differ between convenience for built-in PWMs and security concerns for additional installed PWMs [50]. This study was replicated in 2021 by Ray et al., with older adults. They find a higher mistrust in technologies such as cloud storage, but also motivation through family recommendations or education to be vastly more effective [57]. In 2021, Simmons et al. systematized 17 different use cases for PWMs, and performed a first usability investigation of these using cognitive walkthroughs [66]. In 2022, Oesch et al. performed 32 observational interviews to study how end users use their PWMs. They find that users are often overwhelmed or distrustful of PWMs, therefore using multiple ones as backups, and avoiding features such as, e. g., strong password generation [47]. In the same year, Zibaei et al. conducted a user study to investigate the effectiveness of secure, auto-generated password suggestions through PWMs built into Firefox, Chrome, and Safari. They find that Safari's approach to already pre-fill password fields with secure passwords led to the highest password adoption rate [76].

In contrast to the described related work, we focus especially on credential management strategies users apply to transfer their existing passwords or add new ones. While previous work discussed general user sentiments and adoption reasons, we investigate the behavior after adoption, and provide more in-depth insights into the impact of typical usability issues during PWM setup. We aim to improve the setup process and thereby overall security gain from using PWMs.

4 Password Manager Expert Review

With expert reviews of PWMs and their setup features, we aimed to answer RQ1. We were interested in features that can support users with the tedious initial setup processes when adopting a PWM, i. e., features that were designed to help them add passwords and replace them with strong alternatives where necessary to increase the security benefits from using a PWM. We used the expert reviews findings to inform our survey (cf. Section 5) and design recommendations for PWM developers. Figure 1 depicts the course of our research.



Expert Review (Section 4)
Analyzed 12 third-party and 2 built-in PWMs for onboarding features.

Survey Piloting in 3 Phases (Section 5.1)
1. *Open-ended:* 12 experts, 33 non-experts, used to inform survey
2. *Cognitive Interviews*: 12 expert users, used to refine questions.
3. *End-User Pilot:* 80 screened, 29 full survey pilot responses.

Credential Management Survey (Section 5.2 & 5.3)
1370 screened, 352 eligible participants invited, 279 complete and verified surveys after data validation.

Evaluation (Section 5.4 & 5.5)
Qualitative open coding approach using an iterative codebook.
Two researchers each code the full dataset and resolve all conflicts.

Themes and Recomendations (Section 7)
For the adoption and user experience of PWMs.

Figure 1: Overview of the methodology of our expert reviews and online survey with PWM users.

4.1 Methodology

Two authors conducted expert reviews of the 14 most popular PWMs, an approach used by previous work [20, 51] based on cognitive walkthroughs [53, 61].

We created a list of popular PWMs by collecting extension download counts for Chrome and Firefox. Since we did not aim for an exhaustive overview, and Chrome covers 65% of browser usage [68], we chose to only investigate extensions within the top ten of either. We additionally tested both browsers as well, as they offer built-in PWMs. Overall, we ended up with 14 different tools. The PWMs on this list include both offline PWMs and online PWMs with cloud storage back-ends. While we tried to use only free account plans for a better comparability, some PWMs only provided free premium trials (cf. Table 1).

For the expert reviews, we installed all PWMs on a Ubuntu 20.04. with clean Chrome profiles for each PWM. We performed a set of tasks users typically encounter after setting up a PWM, and aimed to include both common tasks, and workflows that increased security by, e. g., upgrading password strength. First, we installed the PWM including the browser extension, trying to set a bad master password to test if the PWM allowed the password that secured the remaining accounts to be weak. We followed all setup prompts or tutorials to experience every guide designed to help fresh users. Afterward, we searched for mass import features and took notes of their properties. To test in which ways the addition of account details was supported and how well users were aided in choosing strong passwords, we added several accounts. Overall, we searched for account suggestions and automated recognition of websites and their URLs, password generation features, flagging of weak, breached or reused passwords including reuse of the master password. We further searched for dedicated security centers that provide users with an overview of their account security and potentially vulnerable credentials, or for support of timed one-time passwords (TOTP) (cf. Appendix A for a full list of all tasks).

While working on these tasks, we recorded screencasts for later comparison and discussion to ensure nothing was missed and to improve the transparency of our work. Common for cognitive walkthroughs, we tried to simulate the perspective of new users by asking ourselves if the availability of features is apparent, whether the functionality and success of user actions is clearly communicated and easy to understand, and whether relevant features are present or missing. We present our findings, including the most commonly present features, in the following section.

Table 1: Overview of on-boarding features present in popular PWMs. The browser columns indicate that the respective PWM is present in the top 10 PWMs at the time of our analysis.

		Education			PW Storage				Secure PWs				
PWM	**Plan**	**Tutorial**	**Next Steps**	**Achievements**	**Bulk Import**	**Account Suggestions**	**AutoSave**	**TOTPFields**	**Security Center**	**Breach Warning**	**PW Meter**	**Enforces Secure MasterPW**	**Standalone**
LastPass^{F,C}	Paid	●	●	●	●	●	●	◐	●	●	●	●	○
Bitwarden^{F,C}	Free	○	○	○	●	○	◐	◐	◐	◐	○	●	●
Norton^{F,C}	Free	○	○	○	●	○	●	○	●	○	●	●	○
1Password^{F,C}	Paid	◐	●	○	●	○	◐	●	●	●	◐	●	●
RoboForm^{F,C}	Paid	●	○	○	●	●	◐	◐	●	●	○	●	◐
KeePassXC^{F}	Free	○	○	○	●	○	●	●	●	○	●	○	●
Kee^{F}	Paid	●	○	○	●	○	●	●	○	○	○	○	○
NordPass^{F,C}	Paid	○	●	○	●	●	●	○	◐	◐	●	●	●
Keeper^{F,C}	Paid	●	○	○	●	●	●	○	●	◐	●	●	●
Avira^{F,C}	Free	●	●	○	●	○	●	○	●	●	●	●	○
Dashlane^{C}	Paid	●	○	○	●	○	●	○	●	◐	◐	●	○
MultiPassword^{C}	Paid	○	○	○	●	○	●	●	●	○	●	◐	●
Chrome PWM	Free	○	○	○	○	○	●	○	○	●	○	◐	-
Firefox PWM	Free	○	○	○	●	○	●	○	●	●	○	◐	-
Total:		6	4	1	13	4	11	4	10	6	7	9	6

● = Feature found; ◐ = Feature conditionally found; ○ = Feature not found.
^{F} = From Firefox Top 10, ^{C} = From Chrome Top 10

4.2 Results

Overall, our main focus was to identify relevant features for secure addition of credentials that users can benefit from during setup. We found that the majority of tools only offered free premium trials. Where possible, we used the standalone program, which was the case for six PWMs and the two browsers. We identified three different categories of features that help users when initially adding their credentials, which we describe in the following:

User Motivation and Education. This type of feature serves as a first introduction to the PWM, and we distinguish between **tutorials** and **next steps**. A tutorial consists of simple, guided steps that are realized through, for example, pop-ups or interactive demonstrations, during which users are taught how they can work with the PWM and complete common tasks. In cases in which this process was not guided, but simply a non-enumerated list of available features and sensible next actions, we considered them as a list of next steps. We found tutorials present in half of all reviewed PWMs, while next step lists were offered in four. With LastPass, we additionally found one PWM that coupled its guides to **achievements** or badges to incentivize their completion and motivate users to get acquainted with the most important features. Users were further offered a 10% discount on premium memberships if they complete all achievements. Because this requires adding at least ten credentials, the achievement feature incentivizes active learning rather than simply reading a tutorial.

Ease of Password Storage. As the initial addition of account credentials is a time-consuming task, we found different functionalities aiming to ease the process. Most importantly, almost all tested PWMs except the Firefox built-in offered some kind of **bulk import** from other PWMs, browsers, or raw .csv files.

However, we found the expected import formats to differ widely, and we found different requirements for .csv files in terms of, e. g., required columns and data formatting. Users without a previous PWMs to import from would therefore need to create very specific files manually, while users whose previous PWMs export differs too much from the expected import format need to invest time to edit the data. As a result, this offers only a small benefit for users, who need to compile the respective file, requiring them to remember all their accounts in a similar problematic way than if they had added all credentials one by one. Additionally, this encourages them creating a non-encrypted collection of credentials they might not remove from their hard drive afterward [12,58]. A slower approach is the ability to **auto-save** passwords while browsing, in which the PWM extension offers to store credentials whenever the user logs into a website or registers new accounts. We found this available in almost all PWMs, however, it was only available as a premium feature in RoboForm. While both Bitwarden and 1Password in theory offered auto-saves, we experienced issues with this feature in both extensions. According to their forums, the Bitwarden issue has been known for a while, and they are working on a solution [10]. Finally, we found four PWMs that **suggested popular websites** when adding new accounts. This feature is useful to help users remember which accounts they might have, however, it is only occasionally offered.

Secure Passwords. Another important step of the initial PWM setup is the chance to upgrade old passwords if they are, e. g., weak or reused, which can be supported by PWMs through signalling which passwords may need to be changed. While **password meters** are the best-known features to help users create strong passwords, we only found them in seven PWMs. When included, we often perceived them as counterintuitive. In practice, changing settings such as increasing the length regenerates the password, and while longer, the new one might have a similar, but slightly decreased entropy. However, as this is often what password meters measure, the strength bar can go down when, e. g., the password length is increased. In other cases, the evaluation was performed after the entry was stored, requiring users to actively check for warnings instead of receiving them while saving the password. Two PWMs only used password meters while using the built-in generators, therefore not providing feedback to users who create manual passwords or copy and paste old ones. Other measures include **security centers**, i. e., dashboards in which users receive comprehensive summaries of insufficient credentials that are, e. g., weak, reused over multiple stored entries, generally common, or present in leaks. This enables users to purposefully upgrade insecure account credentials where necessary, and was present in a majority (ten) of evaluated PWMs. However, we found it often only available in premium account plans, and Bitwarden only offered it in its web client, with no further mention of the feature within the standalone app.

NordPass asked us to change older passwords, although research has found regular updates to have negative impacts on security [14]. A similar feature, often included within security centers, are **breach reports**, in which either the user's email address or the passwords within the PWM are scanned for their presence in credential leaks. While present in almost all PWMs, breach reports are typically a premium feature that is not accessible for non-paying customers. This is especially curious as it is often based on the free tool Have I Been Pwned [27]. In the case of Keeper, this was particularly severe, as we were informed that some of our accounts were breached, but then asked to pay to receive any further information of which account was affected.

5 Credential Management Survey

Following our expert review of PWM setup features within popular PWMs, we conducted a survey with 279 users of both built-in and third-party PWMs. We describe the methodology of our survey study below.

5.1 Survey Design & Piloting

For the initial survey design, we created an early draft of our survey and tested it with 12 usable security expert users, and 33 non-expert users in several rounds of piloting. The exploratory survey draft consisted of an early version of our final survey. It was modified to contain only free-text questions, which we used to collect options for multiple-choice questions in the final survey and to identify credential management strategies. For the expert survey, we additionally offered text boxes on every survey page to gather expert feedback on the question design. Based on results of this early version, we modified the survey to improve question and answer phrasing, and we used the responses to open-ended questions to create options for multiple-choice versions of some questions. Whenever a participant's answer was not yet collected as a closed-ended answer option for our final survey, we added it along with any related answer that came up during the result inspection. We stopped recruitment when we reached theoretic saturation, that is, when no new answer options emerged, and no participant answered any question in a manner that indicated a lack of understanding.

To improve survey quality and explore the area further, we additionally conducted 12 cognitive interviews [54] with associates of the authors who did not yet fill the pilot survey, and were not involved in this research project. While most of them were usable security researchers, one was an end user with a master's degree in computer science. We invited participants to a voice chat and asked them to screen share their completion of our survey. We encouraged participants to "think aloud", rephrase questions in their own words or elaborate on their thoughts to learn how they understood certain questions or why they answered in a certain way. Overall, cognitive interviews are a common approach to collect feedback and improve survey quality [2,31,39,60,74]. After each interview, two authors analyzed the responses, received feedback and agreed on survey changes. The survey was adjusted before moving to the next participant, to test changes. We recruited participants for the cognitive interviews until we found no major new misconceptions or problems.

Finally, we conducted several rounds of piloting with the closed-ended version of the survey, screening a total of 80 end users, of which we invited 33 to the full survey, and received 29 answers. We polished our question phrasing, and continued until all questions were answered with sufficient quality, indicating that the survey was now easily understandable.

5.2 Survey Structure

We designed the survey to explore which credential management strategies users apply when they initially set up their PWM, i. e., how they add their passwords, and in which ways they interact with their PWM to increase task efficiency or password security. The full survey can be found in Appendix C.

We first included PWM demographics such as when they started using a PWM (Q1), what their first PWM was (Q2) and if changed, what their current PWM is (Q3), whether they paid for it (Q4) and if they would recommend it to others (Q5). We further asked whether they added all private (Q6-Q7) or work-related (Q8-Q9) accounts to it. Afterward, we asked about their reasons to use a PWM (Q10), including who recommended it, if anyone did (Q11), and if they or somebody they knew experienced a password breach (Q12), as we deemed both relevant to their decisions regarding their PWM usage.

Overall, we aimed to investigate the spread of the PWM **credential management strategies** we identified during piloting, as well as what influenced a users' decision to apply a strategy. Therefore, we asked participants about the strategy they mainly applied (Q13) both in an open-ended question to gather unbiased experiences and sentiments, and a closed-ended version on the next survey page (Q14) to better pinpoint the precise strategy. We further asked participants to describe reasons for their strategy choice (Q15) and alterations in their current strategy to account for changes over time (Q16). Since these strategies might depend on specific website (types), we gave participants the option to share these priorities with us (Q17).

Furthermore, we were interested in how participants dealt with their existing passwords - i. e., whether they changed all, some or none of them when they set up the PWM (Q18), and their reasons for doing so (Q19-Q21). We were further interested in their password generation process (Q22-23).

Additionally, we asked broader questions regarding their experiences with the setup process (Q24-25), and which additional features of their PWMs participants were using (Q26).

Based on previous answers, we determined every participant who did not use the approach we deemed ideal from a security perspective(i. e., stated to not have updated all passwords when adding them or to not have added all accounts at once), and asked them an additional question regarding their reasoning (Q27).

To further collect insights into problems and usability improvements, we directly asked participants what their PWM could have done to improve their personal setup process (Q28).

Finally, the last part of our survey covered **common demographic questions**. This includes gender (Q29), age (Q30), and ethnicity (Q31), their highest formal education (Q32) and whether the participants ever studied a computer science related subject (Q33) or held a computer science related job (Q34).

5.3 Data Collection & Recruitment

We contacted expert users for our piloting through our professional network. For our survey study, we used the crowdsourcing platform Prolific [55] to gather participants due to their general high data quality [48] and in several rounds invited 1,370 participants to our screening survey. To uphold certain quality standards, we required participants to have a job approval rate of at least 90% and at least five previously submitted jobs, and excluded all users who participated in previous iterations of our pilot. To filter out participants who never adopted a PWM, or were unaware of the PWM functionalities within their browser or operating system, we used two questions regarding password management in our screening survey, but did not mention our focus on PWMs yet (see Appendix B). We further asked which PWM they used and since when, and used their answers to determine usage of built-in or third-party PWMs, and as an attention and sanity check between screening and full survey. From all participants we screened, we manually selected all who stated to use a third-party PWM, and a similar amount of users of built-in PWMs. Based on results from previous work, which found significant differences in the approaches and sentiments of both groups, we decided to invite equal participant numbers for both [43, 50]. This resulted in 352 participants we invited to complete the full survey, of which 304 completed it, and 279 yielded valid answers.

5.4 Data Cleaning & Analysis

We removed 25 participants whose answers contradicted their statements from the screening survey, and found none who finished the survey suspiciously quickly. In the case of open-ended questions, two researchers coded all answers using an iterative approach based on thematic analysis [16]. For each question, they individually created a codebook, in which they denoted recurring answer patterns. They discussed their individual codebooks and merged them to create a single codebook. The two researchers jointly read all answers and assigned matching codes from the corresponding codebook. In case of conflicts or changes in the codes, both researchers discussed the problem until they reached agreement. These discussions included adjustments in the definition of individual codes, and merges or splits of codes that were rarely or frequently assigned to account for nuances in answers. Both researchers revisited previously coded answers and updated the assigned codes for a consistent coding strategy. We did not calculate inter-rater reliability due to the exploratory nature of our coding, which in theory led to a perfect agreement since we solved all conflicts via discussion [44]. The final codebook with descriptions of the codes and their distribution onto the open-ended questions can be found in Appendix D. For some selected questions, we tested for significant differences between users of built-in and third-party tools using a Chi-square test (χ^2).

Table 2: Demographics for all valid participants.

Demographics	**Value**	**Percent**
Gender:		
Man	175	62.72%
Woman	103	36.92%
Genderqueer	1	0.36%
Age:		
Median	35.0	-
Mean	30.19	-
Standard Deviation	9.24	-
Ethnicity:		
White or of European descent	191	68.46%
Black or of African descent	59	21.15%
Multiple Ethnicities	15	5.38%
Hispanic or Latino/a/x	7	2.51%
East Asian	1	0.36%
South Asian	2	0.72%
Middle Eastern	3	1.08%
Southeast Asian	1	0.36%
Education:		
Bachelor Degree	108	38.71%
Master Degree	59	21.15%
Secondary School	33	11.83%
College/University Study (without Degree)	45	16.13%
Trade/ Technical/ Vocational	13	4.66%
Associate Degree	8	2.87%
Professional Degree	3	1.08%
Other Doctoral Degree	6	2.15%
Technical Background:		
Computer Science/ Technical Education	76	27.24%
Computer Science/ Technical Job	98	35.13%
Start with PWM		
In the last week	6	2.15%
In the last month	1	0.36%
In the last six months	15	5.38%
In the last two years	52	18.64%
More than two years ago	200	71.68%
I don't know	5	1.79%

5.5 Results

In this section, we describe the results of our survey study with 279 participants, asking about their strategies to initially add and update passwords to their PWM. Overall, we found that most participants add credentials whenever they access the respective services. This was often motivated by efficiency, convenience, or a lack of overview over their online accounts. Due to this, security was only a secondary factor. Many participants were deterred from investing time and effort to improve their online credential security.

5.5.1 Participant Demographics

In this section, we provide a summary of our participants' demographics (cf. Table 2). 175 (62.72%) of our participants identified as men, while 103 (36.92%) identified as women and one person self-described as genderqueer. Participants were 30.19 years old on average (std: 9.24, med: 35.0). The majority (191, 68.46%) described themselves as White or of European descent, which is not surprising for Prolific as a European crowdsourcing platform. This is followed by 59 (21.15%) who identified as Black or of African descent. Considering education, 108 (38.71%) participants stated to have a Bachelor's degree, 59 (21.15%) a Master's degree and 33 (11.83%) have completed secondary school. 27.24% of all participants declared that they received a degree in computer science or a related field, and 35.13% stated that they have worked in this area before. We acknowledge that computing professionals are over-represented, and assume that PWM use tracks with computer science experience. Overall, our recruited sample is in line with previous studies conducted on Prolific [31, 62].

We found that the vast majority of participants (200, 71.68%) reported using a PWM for more than two years or started using one within the last two years (52, 18.64%). Overall, 141 reported to mainly use PWMs built into their operating systems or browsers, while 138 stated to mainly use third-party PWM tools. We asked participants about their first PWMs, and which one they currently used, if it had changed. We found Chrome (84, 59.57%) and Apple Keychain (43, 30.5%) to be the most common currently used PWMs for built-in users. For third-party PWM users, the distribution was more even, with Bitwarden (39, 28.26%), KeePass variants (24, 17.39%), and LastPass (22, 15.94%) being the most frequently named. Finally, 27 (9.68% of all participants) stated uncommon PWMs that were overall only named at most three times, and 3 (1.08%) had stopped using a PWM.

5.5.2 Credential Management Strategies

In this work, we were most interested in how end users insert their account credentials when setting up a PWM, as this process can be tedious, but also crucial for improved security. Overall, we identified seven main strategies. We mainly distinguish them by the time passwords were added (e. g., immediately on install, or when services are accessed) or the choice of which passwords were added (e. g., for more or less important or frequently used accounts), and provide a description of strategies as well as their frequency in Table 3. We were unable to map 12 (4.3%) participant answers to one of our identified strategies. These participants reported to, e. g., be unable to recall, not having a strategy, or not having control over the process, as it was executed by a workplace. In other cases, the answer did not allow us to concisely determine which heuristic was used to prioritize accounts that were added, and we decided to merge them in an additional *Any Priority* strategy. Overall, we are confident to have uncovered all relevant credential management strategies in our analysis.

Adding Passwords on the Fly is Easier: The most frequent initial strategy was to add accounts whenever they were accessed for the first time after the PWM setup (108, 38.71%). This often uses auto-save features, i. e., the user does not necessarily need to consciously or manually add passwords, but can simply follow a prompt. Following, users reported to have added their most important or frequently used accounts first (81, 29.03%). This was most often reported as an attempt to save time when adding accounts. Additionally, accounts that did not contain sensitive information were typically not considered worthy of securing them. Note that we merged the strategies *most important* and *frequent* to improve reporting quality, as participants used the terms interchangeably. We found all other strategies to be less relevant in practice. From a security perspective, adding and updating all passwords at once would be ideal. However, we found only 31 (11.11%) participants to specify that their strategy was to add everything at once. We found that 28 (10.04%) users mentioned adding their least important or only rarely used accounts, often referring to security concerns or simply wanting to test the PWM before adding relevant accounts as reasons: "*I started with the less important accounts because I wanted to get used to the tool before importing my important account information.*" (P14) Other strategies our participants mentioned included importing accounts from, e. g., browsers (12, 4.3%), additions with other or unclear priorities (8, 2.87%), e. g. based on chosen passwords, or only adding accounts when a problem occurred such as forgetting the password (7, 2.51%). As these situations forced users to reset their password anyway, and to prevent the need to change it again, they decided to add it to the PWM.

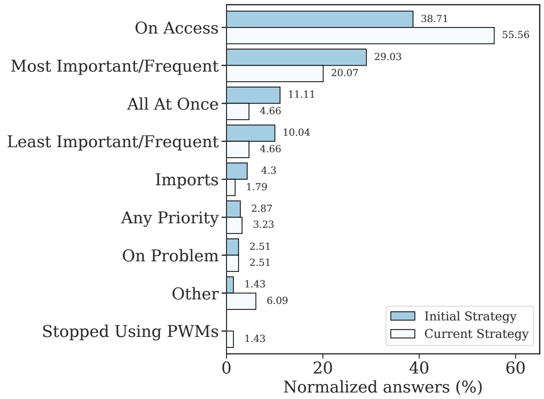


Figure 2: Distribution of the participants' initial and current main strategy in %.

In addition to their initial strategy, we asked participants to provide their current one, and to detail potential changes and reasons. We found a huge increase in users who add their credentials on access (155, 55.56%). As we were asking for the current strategy, this relates mostly to accounts that users freshly create, and that the majority of users immediately add to their PWM, presumably with the help of auto-save features. Again, the second-largest group of participants reported prioritizing important or frequently used accounts (56, 20.07%), suggesting that in these cases, lesser important accounts are never added. We found other previously mentioned strategies mostly irrelevant after the initial setup. Overall, the changes between initial and current strategy can be seen in Figure 2. Most participants chose their initial strategy due to its efficiency (113, 40.5%) or because it was perceived as the easiest approach (94, 33.69%). We found all other reasons less com-

Table 3: Participants' strategies to insert credentials into their PWM (cf. Section 5.5)

Strategy	Description	Initial	Current
All At Once	As far as practicable, users try to add all their accounts at once. Excludes *Imports*.	31 (11.11%)	13 (4.66%)
Any Priority	Users started by adding specific accounts, but described other/unclear prioritization methods.	8 (2.87%)	9 (3.23%)
Imports	Accounts were imported from, e. g., browser profiles or previous PWMs.	12 (4.3%)	5 (1.79%)
Least Important/Frequent	Users started by adding their least important and/or frequently used accounts first.	28 (10.04%)	13 (4.66%)
Most Important/Frequent	Users started by adding their most important and/or frequently used accounts first.	81 (29.03%)	56 (20.07%)
On Access	The accounts are added on the fly, whenever the account is accessed.	108 (38.71%)	155 (55.56%)
On Problem	Users enter accounts when problems occur, e. g., when they need to reset their password.	7 (2.51%)	7 (2.51%)
Other	Other strategies, mixes strategies, or unclear answers.	4 (1.43%)	17 (6.09%)
Stopped Using PWMs	Users have stopped using the PWM. This was only coded for the current, not initial strategy.	- (-%)	4 (1.43%)

mon, such as security increases (46, 16.49%), wanting to add or exclude specific accounts (43, 15.41%), or having problems remembering all accounts or passwords or not wanting to remember them (37, 13.26%). When regarding specific strategies, we found that imports were more often described as convenient, and that adding all accounts at once was more often done out of completion, but less often out of convenience or efficiency. The distribution of reasons per chosen initial strategy is shown in Figure 3.

Finally, we used participant answers to investigate whether they utilized the best-case strategy for security to not only add all of their accounts, but also update every password to a stronger alternative. We found that almost no participants (14, 5.02%) used this approach. Participants mainly argued that adding everything would have been too much work (97, 36.6%), but also that they did not trust their PWM enough to add all important passwords (42, 15.85%), which was a reoccurring theme throughout our whole survey.

We also found participants who stated to be unable to recollect all their accounts (40, 15.09%), as one participant explains: "*I can't even remember that they exist, I can't just suddenly remember all of them and add them to the manager.*" (P142) Other reasons focused on the lack of password changes, including 24 (9.06%) that claimed their passwords were already good enough, or 16 (6.04%) that wanted to keep them, e. g., because they were easily memorizable.

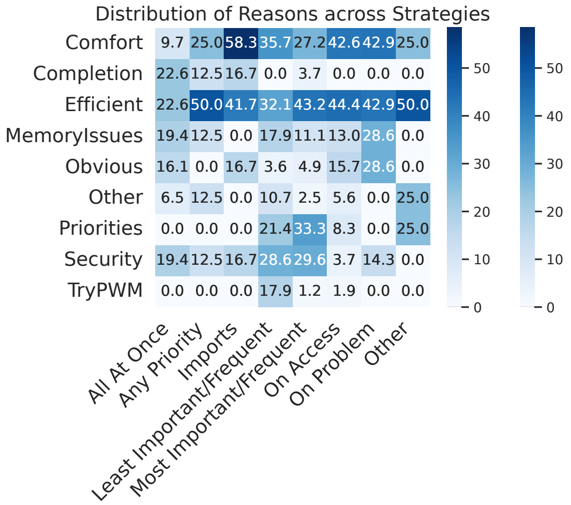


Figure 3: Distribution of reasons for different strategies applied by our participants in %. Our full codebook is described in Appendix D.

Users were largely happy, but workflows were not seamless: Besides the strategies users applied to initially add their credentials, we were also interested in how they rated their experience, i. e., if they were content with their approach, or encountered any issues that should be mitigated. We therefore asked them both what they liked and went well, and in which situations they struggled with their chosen strategy. We found that in general, a majority of users stated to be satisfied with their experience (157, 56.27%). Some mentioned specific properties they praised, such as PWM features and their usefulness (e. g., browser integration and autosave), that they did not need to remember their passwords anymore, the general increase in security, and how comfortable the whole process was (10.04–12.9%) "*My strategy always worked well, I had to do basically nothing, when the program asked me to add an account I just said yes.*" (P61) However, users also reported negative experiences. Most common were malfunctions or abnormal behavior of both PWMs (29, 10.39%) and websites (25, 8.96%), such as auto-saves not working properly, or too complex password policies. Other mentions included password resets that became necessary due to PWM usage, a lack of overview about their accounts, the high effort and issues due to a lack of synchronization support (3.23–5.02%), for example, one participant detailed why adding accounts on access did not always work for them: "*The accounts which I barely used my strategy didn't work cause I'd end up having to create new passwords time and time again*" (P101)

We found that despite some negative experiences, the majority of participants (231, 82.8%) stayed loyal to their initial PWM choice. For the 31 (11.11%) participants that switched to a different PWM, common reasons included changing personal devices, e. g., switching to a different browser and therefore using a new built-in PWM (11, 25.58%), and increasing costs and restrictions of free account plans (10, 23.26%).

In addition to asking for situations in which both PWM usage and the chosen strategy did not work seamlessly, we were interested in participants' wishes and preferences for improved or new features. We found 94 (33.69%) participants who stated to be happy with their PWM, and that they do not need any improvements. Others, who suggested changes, most frequently mentioned the addition of more features, such as better syncing between devices, more memorable password suggestions, or easier bulk imports, (43, 15.41%), or the addition or improvement of automation features (42, 15.05%) such as auto-save, autofill or automated password changes.

This was followed by ways for the PWM to detect their existing accounts based on browser sessions and history, or email inboxes (38, 13.62%), often accompanied by the wish to instantly add these accounts after detection, or improve import features overall (28, 10.04%). However, similar to previous questions, we again found a certain distrust towards PWMs, as 16 (5.73%) participants voiced concerns about their tools collecting too much data, or automated features without them clearly knowing what was happening and why.

5.5.3 General PWM Usage

Besides their initial strategies to set up PWMs, we also asked participants about their general usage to get a broader picture. We found that half of the participants stated to store all their private passwords (131, 46.95%), and an even higher portion that indicated to store every work-related password (183, 65.59%). For those who do not store all private passwords, common reasons included distrust towards the PWM (78, 52.7%) as well as prioritization which passwords should be added (68, 45.95%). We assume that participants are more likely to store all work passwords because they have a lower, more manageable amount that they on average use more frequently.

When asked which website types they prioritized to (not) add, users most commonly mentioned Social Media (78, 27.96%), followed by finance-related websites (47, 16.85%) and email credentials (44, 15.77%).

Since the opportunity to upgrade passwords is an important part of PWM usage, we wanted to know if users did this when they added credentials. Most frequently, they state to have changed some passwords (116, 41.58%), with only 59 (21.15%) who upgraded all of them, and 53 (19.0%) who kept all passwords. We found that reasons to change the passwords were mostly focused around general security increases (35, 22.29%), or to improve weak (55, 35.03%), reused (31, 19.75%) or leaked (14, 8.92%) passwords. Users who decided to keep their old passwords mentioned that their passwords were already strong enough (24, 28.92%), or, a lack of motivation and simply having no reason (26, 31.33%).

> "*And it is not enough to generate a password in the application, you also have to identify yourself on the website, change the password, verify the change... Would you give the same priority to the bank and a game page? Because I do not.*" - P117

When updating existing or new passwords, users typically used the built-in password generators their PWMs offer (56.99–66.86%) or generated the passwords manually (44.0–55.2%).

5.5.4 Comparing Built-in and Third-party PWMs

By design, built-in and third-party PWMs are different in many ways: Their availability, their feature range, as well as how seamless they embed themselves into a users' workflow. Built-in PWMs are by default part of almost any modern browser and operating system. While the feature range and baseline security of built-in PWMs is limited [38, 75], third-party PWMs require a deliberate choice to use the tool, as well as manual installation and some effort to get to know all relevant features. In our survey, we questioned users of both PWM types, and were therefore interested in possible differences between both groups. First, we found that the initial strategies were significantly different (χ^2 = 36.04, $p < 0.005$) between the groups, as third-party users tended to add accounts more often based on their relevance or to add everything at once. However, when regarding the current strategy, the difference was not significant anymore. This is likely because the process of initially adding existing accounts has concluded, and most strategies have shifted towards adding new ones on access. Furthermore, we found significant differences within the reasons for using the respective chosen credential management strategy (χ^2 = 20.03, $p < 0.05$). While built-in users were more often driven by comfort and efficiency, third-party users chose their strategy based on security concerns, and to make sure that either all accounts, or specific important ones were included within their PWM. Similar to this, when asked about their main reason to adopt a PWM (χ^2 = 42.85, $p < 0.005$), we found built-in users more likely to worry about issues such as an overwhelming amount of accounts or forgetting their passwords. However, third-party users were more interested in increasing their overall security, enjoyed the reduced cognitive load of having to memorize only one master password, and were curious to test the PWM, which makes sense as third-party tools require a conscious choice and installation. Additionally, third-party PWM users were significantly more likely to have changed their PWM at some point (χ^2 = 26.76, $p < 0.005$).

6 Ethics & Limitations

In this section, we discuss the ethical considerations and limitations of our work.

Ethics. This work was approved by our institution's Ethical Review Board. We did not collect any personally identifiable information (PII) except anonymous Prolific worker IDs. We made sure that our survey platform did not collect PII such as IP addresses, and we stored all data on our secured servers respecting GDPR requirements. Only researchers involved in this project had access to the collected information. Before starting our survey, all participants had to sign a consent form detailing the nature and content of our survey, as well as contact information. The consent form also informed all participants that they could quit the survey at any time without repercussions. Finally, we paid all Prolific screening participants $0.37 for their participation in the screening survey, independent of their eligibility for our surveys, and $3.71 for the full survey. With our generous estimates of two minutes for the screening and 20 for the full survey, we paid at least $11 per hour and are in line with Prolific's suggestions for minimum wage survey payment.

Limitations. As is typical for survey studies, our work is affected by self-report bias, recall bias, and social desirability bias. Especially for people whose adoption of the PWM dates further back, these memories may be skewed. Additionally, due to the nature of crowdsourcing platforms such as Prolific, there is also a certain self-selection bias as participants can pick studies they are interested in. However, we decided to use surveys to be able to collect self-reported experiences and thoughts of PWM users that we could not gather using more technical sources such as telemetry or lab studies. In our data analysis, we did not partition participants by the specific PWM they used to get a broader picture of credential management using PWMs. However, it is possible that individual PWMs strongly influence the adoption experience and the participants' satisfaction by, e. g., the presence or absence of certain features. During our early piloting (cf. Section 5.1), we might have missed user strategies. However, as we performed multiple rounds of piloting and collected answers until no new options emerged, we are confident to have gathered all options.

7 Discussion

In this section, we first provide answers to our research questions, then discuss our findings and make recommendations for PWM developers to better help users during PWM setup.

RQ1: *What setup features do password managers offer to new users, who want to add their existing credentials?* Within our expert review (cf. Section 4), we identified setup features present in 14 popular PWMs. These include tutorials and next steps to educate users about the PWMs functions, bulk imports, auto-saves, and account suggestions to help them fill their PWMs. Additionally, many PWMs offer security centers to inform users about their passwords' vulnerability. However, we find these centers often limited to premium versions, especially when regarding breach information. Overall, we find that no feature is available on every PWM and that they are most commonly able to bulk import passwords from other sources or to auto-save them while browsing.

RQ2: *What are common user strategies to add new and existing credentials? Why are these strategies used?* We identified seven user strategies that we mainly differentiate by the time passwords are added (e. g., immediately on install, or when services are accessed) or the choice of which passwords are added (e. g., for more or less important or frequently used accounts), We find the most common strategy to be adding passwords on access, followed by prioritizing more important or frequently used passwords. While present within our sample, other strategies are increasingly irrelevant with time, as users shift more towards adding accounts immediately on creation or when accessing the websites (cf. Section 5.5.2). Overall, users are mostly motivated by convenience or efficiency, and less commonly by security.

RQ3: *How can password manager developers help users with setup, and improve the overall process?* In the following sections, we first discuss our findings from both existing setup features (cf. Section 4), and the credential management strategies and obstacles users report (cf. Section 5). Afterward, we comprise several recommendations for PWM developers, as well as website maintainers.

7.1 Convenience Trumps Security

While researchers generally regard PWMs as security tools, as they enable users to store large amounts of passwords securely and issue complex, randomly generated passwords, end users mostly regard them as convenience tools. We find the main motivation for user strategies is convenience or efficiency, which are named much more commonly than security, confirming previous work on the subject [4, 21]. We additionally find users to voice a certain indifference to accounts they perceive as less important, often because these accounts do not include sensitive information, but also whenever users are not certain whether they will access the account again. This is reflected within the primarily chosen credential management strategies to either add every website whenever it is accessed for the first time, or cherry-pick which accounts are important or frequently used, and skip the storage of others.

7.2 Severe Distrust towards PWMs

In various questions, we find a severe distrust towards PWMs. While research previously found that a lack of trust can decrease PWM adoption [7, 8, 42], our finding is likely also related to recent data breaches and leaks with both LastPass [29] and Norton [9]. Hence, we find negative sentiments not only regarding malicious third parties, but also against PWM vendors that fail to secure user data or are in rare cases even suspected to be the actor that steals data: "*It would be simple for the owner of the software to see that I store most of my things in the application which will make it much more easier for them to hack me.*" (P73) While this does not apply to every PWM, their security practices, such as used encryption algorithms and key generation settings, are often neither accessible, nor easy to understand for end users. This becomes especially apparent as LastPass has been accused of using weak and insecure security mechanisms after the recent leaks, such as not enforcing long master passwords or not increasing the number of key derivation iterations for older accounts that were created with less secure encryption algorithms [45].

7.3 Complex Account Landscapes

A major issue that may influence users' decisions (not) to add all their accounts at once is that their online landscape can be vast and includes hundreds of more or less important accounts [34, 69]. In our survey, users reported struggling with remembering all accounts and are therefore unable to add them, and begin to prioritize which accounts they insert into their PWM. Furthermore, our survey confirms that adding accounts manually is a tedious and time-consuming process, leading to users choosing more convenient but less secure management strategies, skipping accounts or keeping insecure passwords, therefore not fully utilizing the benefits that come with the usage of a PWM [40, 50].

7.4 Recommendations

Based on our findings, we offer several suggestions for PWM developers and website maintainers to better support end users in the PWM setup process.

Automation: We find that users are motivated by convenience and efficiency, and less security, and therefore argue that processes to add and update passwords should work automated and seamless. Therefore, more automation is necessary. We propose the more widespread use of novel approaches such as well-known URLs for password change [72] that enables PWMs to quickly and easily upgrade passwords without much burden on the user sides. We further suggest creating a standardized format for password imports, to ease the migration between tools.

Account Scans: Besides the tedious task of adding accounts, users are often overwhelmed by their number of accounts, struggle with recollecting them all, and lack reasons to add lesser relevant or used accounts. By using automated scans PWMs can compile account lists by parsing, e. g., registration emails [64] or visited websites. By running these scans locally, they can be designed in a privacy-preserving manner. Based on a participant suggestion, this could be extended to analogue data, such as handwritten notes, by testing the use of optic character recognition, however, future work is required to evaluate its reliability.

Account Suggestions: If automated scans are not feasible, PWMs can suggest either popular sites, or use already added accounts to infer what users might additionally be interested in or whether typical accounts are missing, e. g., suggest adding an email account if none is present in the password database. Furthermore, this could flag, e. g., incomplete or outdated entries that can be deleted.

Guided Additions: We often find imports to require different formats, and especially to require first-time users to compile their own .csv files. To avoid creation and storage of local password lists, we suggest that PWMs offer their own table interface. Using data from either scans and suggestions, or allow users to edit password collections within the encrypted environment, allowing them to collect, revise and quickly add passwords in bulk.

Privacy Labels: We find severe distrust against PWMs, often due to unclear encryption and security mechanisms. Previous work presented privacy labels that both deliver information regarding the incorporated security, but also allow non-experts to quickly assess the vulnerability of their product [19, 37]. We argue that this could be helpful to address distrust that stems from a lack of knowledge and familiarity, and suggest that PWM developers adopt privacy labels for their programs.

Gamification & Nudges: We find that some users mention that adding accounts is a tedious task, and find one PWM to offer achievements for users to both introduce the PWMs main functions and motivate them to actively fill it. Since gamification has shown promising results in other areas [25, 56], we argue that it should be evaluated for PWMs as well. Related, PWMs could add nudges to motivate and remind users more firmly to store or update passwords at risk [6, 22].

8 Conclusion

The main benefits from using PWMs stems from adding all accounts as soon as possible, and updating every password to a strong alternative, since there is no need to memorize them anymore. In this work, we identified common setup features within 14 popular PWMs, and surveyed 279 end users regarding their credential management strategies. We find that while PWMs offer various setup features that help users add credentials and set secure passwords such as imports, autosave functions or password scoring, they are not present in all PWMs. We identified seven strategies users apply during PWM setup, most commonly adding passwords when accessing websites or when they are perceived as important. We found that end users are mainly motivated by convenience and efficiency, not password security. However, we also noticed distrust towards PWMs, leading to users not storing their accounts as they are concerned for the safety of their data. Due to a lack of motivation, perceived necessity and distrust towards PWMs, they often refrain from adding all accounts, thereby severely limiting the gained security benefits from using a PWM. Finally, we propose several recommendations how this problem can be approached by PWM developers, including more automated workflows and methods to increase user motivation.

Acknowledgements

We thank all participants for their valuable time and insights shared with us. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972.

References

[1] 1Password. The World's Most-Loved Password Manager. https://1password.com/ (visited on 01/18/2023).

[2] Ruba Abu-Salma, Elissa M. Redmiles, Blase Ur, and Miranda Wei. Exploring User Mental Models of End-to-End Encrypted Communication Tools. In *Proc. 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI'18)*. USENIX Association, 2018.

[3] Yusuf Albayram, John Liu, and Stivi Cangonj. Comparing the Effectiveness of Text-based and Video-based Delivery in Motivating Users to Adopt a Password Manager. In *Proceedings of the 2021 European Symposium on Usable Security*, pages 89–104, 2021.

[4] Nora Alkaldi and Karen Renaud. Why Do People Adopt, or Reject, Smartphone Password Managers? In *1st European Workshop on Usable Security*. Internet Society, 2016.

[5] Nora Alkaldi and Karen Renaud. Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[6] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 787–796, 2015.

[7] Salvatore Aurigemma, Thomas Mattson, and Lori Leonard. So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[8] Ramakrishna Ayyagari, Jaejoo Lim, and Olger Hoxha. Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers. *Contemporary Management Research*, 15(4):227–245, 2019.

[9] Bill Toulas. NortonLifeLock Warns That Hackers Breached Password Manager Accounts. https://www.bleepingcomputer.com/news/security/nortonlifelock-warns-that-hackers-breached-password-manager-accounts/ (visited on 2/14/2023).

[10] Bitwarden. Auto save newly created login info. https://community.bitwarden.com/t/auto-save-newly-created-login-info/13555/28 (visited on 05/18/2023).

[11] 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. 33rd IEEE Symposium on Security and Privacy (SP'12)*. IEEE, 2012.

[12] Jason Ceci, Hassan Khan, Urs Hengartner, and Daniel Vogel. Concerned but Ineffective: User Perceptions, Methods, and Challenges when Sanitizing Old Devices for Disposal. In *SOUPS @ USENIX Security Symposium*, pages 455–474, 2021.

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

[14] Sonia Chiasson and Paul C van Oorschot. Quantifying the Security Advantage of Password Expiration Policies. *Designs, Codes and Cryptography*, 77(2):401–408, 2015.

[15] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. A Usability Study and Critique of Two Password Managers. In *USENIX Security Symposium*, volume 15, pages 1–16, 2006.

[16] Victoria Clarke and Virginia Braun. *Thematic Analysis*, pages 1947–1952. Springer New York, New York, NY, 2014.

[17] James S Conners and Daniel Zappala. Let's Authenticate: Automated Cryptographic Authentication for the Web with Simple Account Recovery. *Who Are You*, 2019.

[18] Dashlane. Password Manager App for Home, Mobile, Business. https://www.dashlane.com/ (visited on 01/18/2023).

[19] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices? In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 519–536. IEEE, 2021.

[20] Shayan Eshkandary, David Barrera, Elizabeth Stobert, and Jeremy Clark. A First Look at the Usability of Bitcoin Key Management. In *NDSS Symposium 2015*, page 05_3_3. Internet Society, 2015.

[21] 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):1–20, 2017.

[22] Felix Fischer, Huang Xiao, Ching-Yu Kao, Yannick Stachelscheid, Benjamin Johnson, Danial Razar, Paul Fawkesley, Nat Buckley, Konstantin Böttinger, Paul Muntean, and Jens Grossklags. Stack Overflow Considered Helpful! Deep Learning Security Nudges Towards Stronger Cryptography. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 339–356, Santa Clara, CA, August 2019. USENIX Association.

[23] Xianyi Gao, Yulong Yang, Can Liu, Christos Mitropoulos, Janne Lindqvist, and Antti Oulasvirta. Forgetting of Passwords: Ecological Theory and Data. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 221–238, 2018.

[24] Hana Habib, Jessica Colnago, William Melicher, Blase Ur, Sean Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Cranor. Password Creation in the Presence of Blacklists. *Proc. USEC*, page 50, 2017.

[25] Katrin Hartwig, Atlas Englisch, Jan Pelle Thomson, and Christian Reuter. Finding Secret Treasure? Improving Memorized Secrets Through Gamification. In *Proceedings of the 2021 European Symposium on Usable Security*, pages 105–117, 2021.

[26] Nicolas Huaman, Sabrina Klivan, Marten Oltrogge, Yasemin Acar, and Sascha Fahl. They Would do Better if They Worked Together: The Case of Interaction Problems Between Password Managers and Websites. In *Proc. 42nd IEEE Symposium on Security and Privacy (SP'21)*. IEEE, 2021.

[27] Troy Hunt. Have I Been Pwned: Check If Your Email Has Been Compromised in a Data Breach. https://haveibeenpwned.com/ (visited on 10/20/2021).

[28] Philip G Inglesant and M Angela Sasse. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the sigchi conference on human factors in computing systems*, pages 383–392. ACM, 2010.

[29] Karim Toubba. Notice of Recent Security Incident. https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (visited on 2/14/2023).

[30] Ambarish Karole, Nitesh Saxena, and Nicolas Christin. A Comparative Usability Evaluation of Traditional Password Managers. In *International Conference on Information Security and Cryptology*, pages 233–251. Springer, 2010.

[31] Harjot Kaur, Sabrina Klivan, Daniel Votipka, Yasemin Acar, and Sascha Fahl. Where to Recruit for Security Development Studies: Comparing Six Software Developer Samples. In *31st USENIX Security Symposium, USENIX Security '22, Boston MA, USA, August 10-12, 2022*. USENIX Association, Aug 2022.

[32] KeePassXC. KeePassXC - Cross-Platform Password Manager. https://keepassxc.org/ (visited on 01/18/2023).

[33] Keeper. Generate a Strong Random Password. https://www.keepersecurity.com/password-generator.html (visited on 09/09/2021).

[34] Limor Kessem. Surge of New Digital Accounts During the Pandemic Leads to Lingering Security Side Effects. https://securityintelligence.com/posts/new-digital-accounts-pandemic-security-side-effects/ (visited on 01/18/2023).

[35] LastPass. LastPass | Password Manager. https://www.lastpass.com/ (visited on 01/18/2023).

[36] Kevin Lee, Sten Sjöberg, and Arvind Narayanan. Password Policies of Most Top Websites Fail to Follow Best Practices. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 561–580, 2022.

[37] Yucheng Li, Deyuan Chen, Tianshi Li, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I Hong. Understanding iOS Privacy Nutrition Labels: An Exploratory Large-Scale Analysis of App Store Data. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–7, 2022.

[38] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. The Emperor's New Password Manager: Security Analysis of Web-Based Password Managers. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 465–479, 2014.

[39] Gabriel Lima, Nina Grgić-Hlača, and Meeyoung Cha. Human Perceptions on Moral Responsibility of AI: A Case Study in AI-assisted Bail Decision-Making. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2021.

[40] 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 *27th USENIX Security Symposium (USENIX Security 18)*, pages 203–220, 2018.

[41] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285. IEEE, 2020.

[42] Raymond Maclean and Jacques Ophoff. Determining Key Factors that Lead to the Adoption of Password Managers. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pages 1–7. IEEE, 2018.

[43] Peter Mayer, Collins W Munyendo, Michelle L Mazurek, and Adam J Aviv. Why Users (Don't) Use Password Managers at a Large Educational Institution. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1849–1866, 2022.

[44] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–23, 2019.

[45] Mitchell Clark. The LastPass Disclosure of Leaked Password Vaults is Being Torn Apart by Security Experts. https://www.theverge.com/2022/12/28/23529547/lastpass-vault-breach-disclosure-encryption-cybersecurity-rebuttal (visited on 2/14/2023).

[46] NordPass. How Secure is my Password? https://nordpass.com/secure-password/ (visited on 01/18/2023).

[47] Sean Oesch, Scott Ruoti, James Simmons, and Anuj Gautam. "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In *CHI Conference on Human Factors in Computing Systems*, pages 1–23, 2022.

[48] Stefan Palan and Christian Schitter. Prolific.ac — A Subject Pool for Online Experiments. *Journal of Behavioral and Experimental Finance*, 17:22–27, 2018.

[49] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310, 2017.

[50] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why People (Don't) Use Password Managers Effectively. In *Fifteenth Symposium On Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA*, pages 319–338, 2019.

[51] Katharina Pfeffer, Alexandra Mai, Adrian Dabrowski, Matthias Gusenbauer, Philipp Schindler, Edgar Weippl, Michael Franz, and Katharina Krombholz. On the Usability of Authenticity Checks for Hardware Security Tokens. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 37–54, 2021.

[52] Denise Ranghetti Pilar, Antonio Jaeger, Carlos FA Gomes, and Lilian Milnitsky Stein. Passwords Usage and Human Memory Limitations: A Survey Across Age and Educational Background. *PloS one*, 7(12):e51067, 2012.

[53] Peter G Polson, Clayton Lewis, John Rieman, and Cathleen Wharton. Cognitive Walkthroughs: A Method for Theory-based Evaluation of User Interfaces. *International Journal of man-machine studies*, 36(5):741–773, 1992.

[54] Stanley Presser, Mick P Couper, Judith T Lessler, Elizabeth Martin, Jean Martin, Jennifer M Rothgeb, and Eleanor Singer. Methods for Testing and Evaluating Survey Questions. *Methods for Testing and Evaluating Survey Questionnaires*, pages 1–22, 2004.

[55] Prolific. Prolific | Online Participant Recruitment for Surveys and Market Research. https://prolific.co/, 2020.

[56] George E Raptis, Christina Katsini, Andrew Jian-Lan Cen, Nalin Asanka Gamagedara Arachchilage, and Lennart E Nacke. Better, Funner, Stronger: A Gameful Approach to Nudge People into Making Less Predictable Graphical Password Choices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2021.

[57] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. Why Older Adults (Don't) Use Password Managers. *arXiv preprint arXiv:2010.01973*, 2020.

[58] Joel Reardon, David Basin, and Srdjan Capkun. SoK: Secure Data Deletion. In *2013 IEEE Symposium on Security and Privacy*, pages 301–315. IEEE, 2013.

[59] Rebecca Stone. LastPass Now Offers Time-Based One-Time Passcode (TOTP). https://blog.lastpass.com/2020/12/lastpass-now-offers-time-based-one-time-passcode-totp/ (visited on 1/18/2023).

[60] Elissa M Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. A Summary of Survey Methodology Best Practices for Security and Privacy Researchers. Technical report, 2017.

[61] John Rieman, Marita Franzke, and David Redmiles. Usability Evaluation with the Cognitive Walkthrough. In *Conference companion on Human factors in computing systems*, pages 387–388, 1995.

[62] Daniel Russo and Klaas-Jan Stol. Gender Differences in Personality Traits of Software Engineers. *IEEE Transactions on Software Engineering*, 2020.

[63] Saferpass. Credit Card Support. https://saferpass.net/credit-cards (visited on 1/18/2023).

[64] Paul Sawers. Dashlane Launches Mobile Email Inbox Scanning to Assess Your Online Security Hygiene, 2018. https://venturebeat.com/2018/06/27/dashlane-launches-mobile-email-inbox-scanning-to-assess-your-online-security-hygiene/ (visited on 01/18/2023).

[65] Sunyoung Seiler-Hwang, Patricia Arias-Cabarcos, Andrés Marín, Florina Almenares, Daniel Díaz-Sánchez, and Christian Becker. "I Don't See Why I Would Ever Want to Use It" Analyzing the Usability of Popular Smartphone Password Managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1937–1953, 2019.

[66] James Simmons, Oumar Diallo, Sean Oesch, and Scott Ruoti. Systematization of password manageruse cases and design paradigms. In *Annual Computer Security Applications Conference*, pages 528–540, 2021.

[67] Frank Stajano. Pico: No More Passwords! In *Security Protocols XIX - 19th International Workshop*. Springer, 2011.

[68] statcounter GlobalStats. Chrome Market Share. https://gs.statcounter.com/browser-market-share (visited on 01/18/2023).

[69] Jack Turner. Study Reveals Average Person Has 100 Passwords. https://tech.co/news/average-person-100-passwords (visited on 06/23/2021).

[70] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do Users' Perceptions of Password Security Match Reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760, 2016.

[71] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "I Added '!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[72] W3C. A Well-Known URL for Changing Passwords. https://w3c.github.io/webappsec-change-password-url/ (visited on 11/29/2022).

[73] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 175–188, 2016.

[74] Dominik Wermke, Christian Stransky, Nicolas Huaman, Niklas Busch, Yasemin Acar, and Sascha Fahl. Cloudy with a Chance of Misconceptions: Exploring Users' Perceptions and Expectations of Security and Privacy in Cloud Office Suites. In *Sixteenth Symposium on Usable Privacy and Security, SOUPS 2020, August 12-14, 2020*, Aug 2020.

[75] Rui Zhao and Chuan Yue. All Your Browser-Saved Passwords Could Belong to Us: A Security Analysis and a Cloud-Based New Design. In *Proceedings of the third ACM conference on Data and application security and privacy*, pages 333–340, 2013.

[76] Samira Zibaei, Dinah Rinoa Malapaya, Benjamin Mercier, Amirali Salehi-Abari, and Julie Thorpe. Do Password Managers Nudge Secure (Random) Passwords? In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 581–597, Boston, MA, August 2022. USENIX Association.

A Appendix: Expert Review Tasks

1.1 Install PWM:

- (Omit and proceed with 1.4 if only a browser extension is found)
- Go to the respective website
- Find, download and install the PWM
- Start full-desktop recording
- Choose the most basic plan available (usually free or premium-trial)

1.2 Set a Bad Master Password:

- When prompted for the master password, set a bad password
- If required, provide a secure alternative

1.3 Search for Setup Features

- Follow the setup flow provided by the PWM
- Follow all references to tutorials, next steps, additional information, getting started areas, and similar

1.4 Install the Browser Extension:

- If available, install the complementary browser extension of the PWM
- If the PWM has no standalone version: Start full-desktop recording

- If the PWM has no standalone version: Perform Steps 1.2 and 1.3 for the browser extension

2.1 Search for a Mass Import Feature

- Search the PWM for a mass import feature
- If you cannot find the feature, conduct a Google search: "<PWM name> import feature"

2.2 Add a Password for a Popular Website

- Create a new account entry and add a password for a very popular website.
- Delete entry afterward

2.3 Add a Password for a Less Popular Website

- Create a new account entry and add a password for a less popular website

2.4 Generate a Password for Any Website

- Create a new entry and *generate* a password for any website

2.5 Add a Bad Password for Any Website

- Create a new entry and add a bad password for any website

2.6 Add a Reused Password for any Website

- Create a new entry and reuse a strong password for any website

2.7 Add the Master Password for Any Website

- Open any entry and add the current master password as password

2.8 Add a Password via Autosave

- Open a website and try to log in with activated *autosave* functions (if available)

3.1 Search for a Security Center

- Search the PWM for a security center
- If you cannot find a security center, conduct a Google search: [<PWM name> security center]

3.2 Check Password Strength

- Search for a feature to rate password strength (especially password meters)

3.3 Check Passwords for Leaks/Breaches

- Search for a feature to check passwords and other data for their appearances in leaks

4 Add Two-Factor Authentication

- Open any entry and add a (predetermined) two-factor authentication seed to it

B Appendix: Screening survey

SQ1 How do you manage your passwords? [multiple choice]

□ I memorize them

□ I write them on a piece of paper

□ I keep them in a (hidden) textfile

□ My browser/phone remembers them for me

□ I am using a password manager

□ Other (please specify): [free text]

SQ2 [If "My browser/phone remembers them for me" or "I am using a password manager" in SQ1:] When did you start using a password manager? [single choice]

○ In the last week

○ In the last month, but not in the last week

○ In the last six months, but not in the last month

○ In the last two years, but not in the last six months

○ More than two years ago

○ Never, and I do not plan to

○ Never, but I do plan to

○ I do not know / I do not remember

SQ3 [If "My browser/phone remembers them for me" or "I am using a password manager" in SQ1:] Please name your first password manager(s). [free text]

SQ4 [If "My browser/phone remembers them for me" or "I am using a password manager" in SQ1:] On which devices are you/have you been using a Password Manager? [multiple choice]

□ Windows

□ Linux

□ Mac

□ iOS

□ Android

□ Blackberry

□ ChromeOS

□ Other (please specify): [free text]

SQ5 [If neither "My browser/phone remembers them for me" nor "I am using a password manager" in SQ1:] Why are you not using a password manager? [free text]

C Appendix: Survey

Password managers are tools that can help you store passwords and create strong ones. This includes both programs or browser extensions you chose and installed (e. g., LastPass, 1Password), and the password managers included in your phone or browser (e. g., Chrome, Apple Keychain).

Q1 When did you start using a password manager? [single choice]

○ In the last week

○ In the last month, but not in the last week

○ In the last six months, but not in the last month

○ In the last two years, but not in the last six months

○ More than two years ago

○ Never, and I do not plan to

○ Never, but I do plan to

○ I do not know / I do not remember

Q2 Please name your first password manager(s) [free text]

Q3 Are you still using the same password manager? If not, which one are you currently using, and why did you decide to change? [free text]

Q4 Are you paying for your password manager? [single choice]

○ Yes

○ No

Q5 How likely is it that you would recommend a password manager to a friend or colleague? [Net Promoter Score, 11-point likert from *Not at all likely* to *Extremely likely*]

Q6 Are all of your private accounts stored inside of a password manager? [single choice]

○ Yes, all of them

○ No, not all of them

○ I am not sure

Q7 [If “No, not all of them” or “I am not sure” in Q6] Please share with us why you are not storing all of your private accounts in a password manager. [free text]

Q8 Are all of your work accounts stored inside of a password manager? [single choice]

○ Yes, all of them

○ No, not all of them

○ I am not sure

Q9 [If “No, not all of them” or “I am not sure” in Q8] Please share with us why you are not storing all of your work accounts in a password manager. [free text]

Q10 Please try to remember your thoughts when you first started using a password manager. Which of the reasons below best describe your main reasons to use a password manager? Please select all that apply to you. [multiple choice]

□ I wanted to increase security (e. g. I could use stronger passwords)

□ Creating passwords myself was tiresome

□ I only needed to remember one master password

□ It became easier to organize my passwords

□ All my passwords were in one place

□ I had too many accounts to remember my passwords

□ I kept forgetting my passwords

□ It was a requirement by my employer

□ I was curious to test password managers

□ Somebody recommended using them to me

□ The password manager can generate strong passwords

□ The free trial convinced me to use it

□ Other (please specify:) [free text]

Q11 [If “Somebody recommended using them to me” in Q10] Who recommended using a password manager to you? Please choose all that apply. [multiple choice]

□ A spouse/significant other

□ Family

□ Friends

□ Colleagues

□ Somebody else (please specify:) [free text]

□ Nobody

□ I do not remember

□ Prefer not to disclose

Q12 Were you or somebody you know the victim of a data breach or hack that leaked all or some of your login information (e. g. passwords, email addresses, hashes)? [single choice]

○ Yes

○ No

○ I do not know

○ Prefer not to disclose

Q13 For this question, try to remember how you started out with the password manager. What was your initial strategy to add existing accounts, e. g., did you add them all at once or did you prioritize certain accounts? Please include as many details as you can recall. [free text]

Q14 Which of the strategies below fits your main strategy to add existing accounts best? [single choice]

○ Added them whenever the account was accessed or visited

○ Started with rarely used accounts

○ Started with less important accounts

○ Started with more important accounts

○ Added all I could remember at once

○ Added them whenever I encountered a problem (e. g. needed to reset the password)

○ Imported my passwords from e. g. my browser

○ Other (please specify:) [free text]

○ I do not remember my main strategy

Q15 Why did you use your particular strategy of adding existing accounts to your password manager? (e. g., because it was time-efficient or less work to add only certain accounts, or because it increased security to add all accounts at once) [free text]

Q16 Please share your current strategy to add new or existing accounts into your password manager with us. We are especially interested in how it differs from your initial strategy, and why you decided to change your approach. If you kept your initial strategy, please write “no”. [free text]

Q17 If you stated to prioritize certain accounts in any of the previous questions: Please specify the type, e. g., social media. [free text]

Q18 Did you update your existing passwords when you added accounts to the password manager? [single choice]

○ Yes, all of them

○ Yes, some of them

○ No, none of them

○ I do not remember

○ Prefer not to disclose

Q19 [If “Yes, all of them” in Q18] Please elaborate in detail why you updated all of your passwords. [free text]

Q20 [If “Yes, some of them” in Q18] Please elaborate in detail why you updated some of your passwords, but not all of them. [free text]

Q21 [If “No, none of them” in Q18] Please elaborate in detail why you updated none of your passwords. [free text]

Q22 [If “Yes, all of them” or “Yes, some of them” in Q18] In which way do you update your **existing passwords** when adding them to your password manager? Please choose all that apply. [multiple choice]

□ Update them using the password manager’s built-in password generator

□ Update them using an external password generator

□ Update them with a manually created new password

□ I do not add existing accounts

□ Other (please specify:) [free text]

Q23 In which way do you generate your passwords when creating new accounts and adding them to your password manager? Please choose all that apply. [multiple choice]

□ Generate them using the password manager’s built-in password generator

□ Generate them using an external password generator

□ Manually create a new password

□ I do not add new accounts

□ Other (please specify:) [free text]

Q24 Please share your experiences with initially adding your passwords to your password manager with us. In which situations and for which accounts did your strategy work well? [free text]

Q25 In which situations and for which accounts did you stumble over problems with your strategy? Which problems did occur? [free text]

Q26 In addition to storing passwords, you use your password manager for: [multiple choice]

- □ Autofilling Two-Factor Authentication
- □ Storing banking or credit card information
- □ Storing address information
- □ Storing secret notes (e. g., Recovery codes, SSH keys, private encryption keys)
- □ Storing other data (please specify:) [free text]
- □ Checking your password strength
- □ Checking if your passwords were part of a data breach
- □ Checking your passwords for reuse
- □ Generating strong passwords
- □ I am not using additional functions
- □ Other functions (please specify:) [free text]

Q27 [If not “Added all I could remember at once” in Q14 or “Yes, some of them” or “No, none of them” in Q18] You have stated that you did not add and update all passwords at once when you initially started using your password manager. We are interested to learn why you did not do this. Please provide details for your reasoning. [free text]

Q28 In which ways could your password manager have supported **your** process of initially adding all your existing passwords better? Please assume that there are no technical limitations, e. g. that password managers can access all data they need. [free text]

Q29 What is your gender? We use this information to increase visibility of less represented genders. [single choice]

- ○ Woman
- ○ Man
- ○ Non-binary
- ○ Prefer not to disclose
- ○ Prefer to self-describe [free text]

Q30 What is your age in years? [integer input]

Q31 Which of the following describe your race and ethnicity, if any? Please check all that apply. [multiple choice]

- □ White or of European descent
- □ South Asian
- □ Hispanic or Latino/a/x
- □ Middle Eastern
- □ East Asian
- □ Black or of African descent
- □ Southeast Asian
- □ Indigenous (such as Native American, Pacific Islander, or Indigenous Australian)
- ○ Prefer not to disclose
- ○ Prefer to self-describe [free text]

Q32 Which of the following best describes the highest level of formal education that you have completed? [single choice]

- □ I never completed any formal education
- □ 10th grade or less (e. g., some American high school credit, German Realschule, British GCSE)
- □ Secondary school (e. g., American high school, German Realschule or Gymnasium, Spanish or French Baccalaureate, British A-Levels)
- □ Trade, technical or vocational training
- □ Some college/university study without earning a degree
- □ Associate degree (A.A., A.S., etc.)
- □ Bachelor’s degree (B.A., B.S., B.Eng., etc.)
- □ Master’s degree (M.A., M.S., M.Eng., MBA, etc.)
- □ Professional degree (JD, MD, etc.)
- □ Other doctoral degrees (Ph.D., Ed.D., etc.)
- ○ Prefer not to disclose
- ○ Other (please specify:) [free text]

Q33 Do you have a formal education (Bachelor’s degree or higher) in computer science, information technology, or a related field? [single choice]

- ○ Yes
- ○ No
- ○ Prefer not to disclose

Q34 Have you held a job in computer science, information technology, or a related field? [single choice]

- ○ Yes
- ○ No
- ○ Prefer not to disclose

D Appendix: Codebook

Table 4: The codebook with descriptions we used to code the open-ended questions. For questions Q13 and Q16 see Table 3.

Code	Q3	Q7	Q9	Q15	Q17	Q19	Q20	Q21	Q24	Q25	Q27	Q28	Description
Accounts										■	■		Problems gathering accounts, e. g., due to amount of accounts, lack of overview, old or rarely used accounts.
Administrative					■								Prioritization of governmental, civic or medical accounts.
Automatization												■	Desire for better automatization, e. g., autosave, autofill, or autochange of passwords.
Breach						■	■			■			(Some) Passwords appeared in a breach or data leak, passwords were changed to be safe.
ChangedDevice	■												Device, browser, or workplaces have changed, and the old PWM is not available or practical anymore.
Comfort				■		■	■		■				The process of, e. g., adding passwords, changing passwords, improving passwords, is easy to complete, or even enjoyable.
Completion				■									Desire to add all accounts into the PWM as soon as possible.
Cost	■												Old PWM became too expensive, or adjusted the feature range of its account plans (including free plans).
Distrust		■	■								■	■	Skepticism or fear towards the PWM, e. g., because it might break, leak data, or spy on its user, which influences participants behavior or perception.
EaseOfLogin									■				PWM eases login processes or remembers passwords, meaning the user no longer has to.
EaseOfUse	■												New PWM is easier to use and or more comfortable.
Education					■								Prioritization of educational accounts, e. g., school or university accounts, or platforms with educational content.
Efficient				■					■				Process of, e. g., adding or changing passwords, is very fast or simple (in terms of time or effort).
Effort		■	■				■	■		■	■		Strategy or process to, e. g., add or change passwords is too time-consuming, cumbersome, or too much work.
Email					■								Prioritization of email accounts.
Financial					■								Prioritization of accounts related to finances, e. g., banking accounts or cryptocurrency wallets.
GoodPWs							■	■			■		(Some) Passwords are good enough, no need to change them, or the account is already secure enough due to, e. g., multi-factor authentication.
Guidance												■	Desire to have more guides, tips and tricks, or explanation on how the PWM works.
Imports												■	Bulk password imports from different sources, e. g., browser, other PWMs, or .csv files.
HighSecurity					■								Prioritization of accounts with special access rights or containing sensitive or personal data.
MemoryIssues				■		■	■						Issues related to not being able or not wanting to remember accounts or passwords, e. g., it is hard to remember passwords without PWMs.
Misc					■								Prioritization of rarely mentioned account types, or those too unspecific or all-encompassing to assign them to a more specific code, e. g., “Google”.
MultipleDevices		■	■							■			Multiple devices or platforms are used, but the PWM is not (easily) available on all of them, e. g., participant cannot access PWM on their phone or devices such as smart TVs.
Obvious				■									Obvious choice, no good alternative, or most logical strategy.
OpenSource	■												The new PWM is open source and hence more trustworthy.
PasswordReset										■			Participant has to reset passwords they could not remember.
Priorities		■	■	■			■						Prioritization of specific accounts, e. g., (not) adding/updating accounts because they are (not) important, rarely/often used, or include sensitive data. Note that Q17 codes detailed answers regarding which accounts were prioritized.
PWMFeatures	■								■			■	Convenience due to PWM features and functions in all steps of the process, e. g., suggestions of popular accounts, allowing more content fields within password entries, or allowing syncing.
PWMLimitations		■								■			Problems due to PWM properties, e. g., features missing or not working (well) or limitations (e. g., only limited number of accounts or devices possible).
PWScoring												■	Desire for feedback regarding the password strength, and reused or breached passwords, and suggestion of better passwords.
QualityOfLife												■	Desire for better interfaces, easier handling, or in general higher usability of the PWM.
RegularUpdate						■	■						(Some) Passwords are changed based on undefined trigger or external policies.
Remembrance		■	■				■	■		■	■		Participant has easy memorizable passwords, or prefers to keep memorizable passwords.
Reused						■	■						(Some) Password were reused or only slightly modified, passwords were changed to be safe.
Satisfied	■								■	■		■	Participant is satisfied (with current situation) or highlights neither good nor negative aspects.
Scans												■	Desire to receive a list of websites/accounts based on scanning emails, history, or handwriting (OCR).
Security	■			■		■	■		■				Behavior, e. g., adding accounts, changing passwords or PWMs, that helps mitigate security issues or with the goal to increase security overall.
Shopping					■								Prioritization of online shops or accounts related to shopping.
SocialMedia					■								Prioritization of social media or forum accounts.
TryPWM				■							■		Participant (initially) wanted to test the PWM, which influences the strategy.
Unknown											■		Participant did initially not know about the strategy or did not think about using it.
Unwilling							■	■			■		Participant does not want to try the strategy or thinks it is not necessary, e. g., does not see the need to add/update more than the most important passwords.
WeakPWs						■	■						(Some) Password were weak, too old or considered bad for other reasons, passwords were changed to be safe.
Websites										■			Websites obstructed process, e. g., by adding complex password requirements or disabling autofill.
Work					■								Prioritization of work-related accounts, e. g., work accounts or career websites.
Workplace			■										PWM usage only for work or influenced by work (requirements).

■ Code used at least once for the respective question.