'*The more accounts I use, the less I have to think*': A Longitudinal Study on the Usability of Password Managers for Novice Users

Patricia Arias Cabarcos
Paderborn University and KASTEL Security Research Labs [*]
pac@mail.upb.de

Peter Mayer
University of Southern Denmark and Karlsruhe Institute of Technology
mayer@imada.sdu.dk

Abstract

Despite the security benefits of password managers (PM), many users refrain from adopting them, usability being a major friction point. In this work, we go beyond prior research that captures usability issues as isolated snapshots. Instead, we provided $n = 37$ novice participants with a 3-month license for a commercial password manager and captured their experiences in weekly questionnaires over the first month and at the end of the trial period. Our findings highlight the strong impact of first-impression usability, with initial hurdles in managing primary passwords making adoption cumbersome. While trust in the password manager improves over time, perceived usability stays unchanged. Users tend to ignore credential audit flags, potentially undermining the security benefits the password manager provides. Based on these insights, we provide recommendations to enhance password manager adoption and usability so users can benefit from the full functionality and protections password managers provide.

1 Introduction

Password managers (PMs) are widely recommended as a solution to both security and usability challenges in password management [20, 24, 44]. These tools allow users to generate, store, and auto-fill strong passwords, reducing cognitive load and mitigating risks associated with password reuse and weak credentials. However, as seen with many security technologies, usability concerns remain a key barrier to widespread adoption [2, 15, 48, 54].

One of the first influential works addressing the usability of password managers was *Chiasson et al.*'s study [15], which revealed that users' struggles with interface complexity, trust issues, and learning curves deter long-term adoption. Despite the almost 20 years that have passed since this study, and the significant research and advancements in both the usability and functionality of modern password managers, adoption has not peaked. Recent statistics indicate that only 12% of users use dedicated password manager applications, and 11% rely on browser-based password storage [18], suggesting that underlying challenges persist.

While prior research on password managers has extensively studied usability issues through expert reviews and controlled experiments or snapshot usability evaluations where the user performs a set of one-time predefined tasks [2, 6, 41, 54, 55], little is known about how users' perceptions, experiences, and adoption intention evolve longitudinally.

The goal of our work is to fill this knowledge gap and provide a long-term view on usability issues encountered by first-time users. To this end, we conducted a one-month longitudinal study with $n = 37$ users who have never used a PM before. By tracking participants' experiences over time, our research design allows us to observe usability challenges as they emerge in real-world contexts, including different scenarios where usage patterns might differ, such as during traveling or weekends. Furthermore, studying first-time interactions from novice users over time offers unbiased insights into natural adoption barriers and misconceptions.

We hypothesized that trying a password manager increases the intention to adopt this type of tool, and that usability perceptions improve with prolonged use – as users get familiar with the software, understand its usefulness, and pass the learning curve. Contrary to this expectation, our results show that first-impression usability has a strong impact. The 42% of participants that stopped using the PM between week 1 and week 4, rated its usability significantly lower than users that completed the whole usage period (58.6 vs 71.8 points in the System Usability Scale [12]). Additionally, our study reveals hurdles with primary passwords and passivity against credential audit information. It also provides insights into trust evolution and social aspects related to PM adoption. Based on these findings, our study offers practical recommendations for improving password manager adoption and long-term usability.

[*]Current affiliation: European Commission, Joint Research Centre (JRC), Ispra, Italy.

2 Related work

In the following, we present work relevant to the context of our study. We first discuss motivators and barriers to PM use, i.e., factors that make individuals adopt and continue to use (or stop using) PMs. We then discuss how adopting a password manager might affect individuals' security posture. Last but not least, we discuss other longitudinal studies in the field of authentication.

2.1 Motivators and Barriers to PM Use

Human factors aspects relating to password managers (PMs), i.e., their usability and user perceptions, have been widely studied. Specifically, the pivotal role of ease-of-use [2, 7, 14, 16, 22, 33, 37, 41, 48, 54] and usefulness [2, 4, 14, 22, 38] in the adoption and use of password managers has been repeatedly shown in the literature. Munyendo et al. [43] have shown that this also holds when switching from one PM to another. Security aspects often take a secondary role behind these two aspects [33, 41]. Interestingly, this is the inverse for the adoption and use of password audit features of PMs. Kablo et al. [32] found that security was the most important motivator for adoption of these features.

Due to the prevalence of ease-of-use and convenience as factors influencing the adoption and use of PMs, the usability of password managers has been a subject of intense study and has unveiled several issues with PMs. Most notably, PMs' compatibility with users' use cases plays a pivotal role, e.g., auto-fill during login and recognition of entered information or generation of incompatible passwords during enrollment [2, 14, 28, 41], but also recognition of login fields in applications [54]. Other issues reported in the literature include UI issues and performance issues [14, 15], learnability [14], having to transcribe passwords to unsupported devices [41, 46], and feeling overwhelmed [32].

However, ease-of-use and usefulness are not the only factors which were found to positively influence the adoption of PMs. Other influencing factors include: trust [22], subjective norms [2, 48, 57], and the three factors of self-determination theory (autonomy, competence, relatedness) [3]. Additionally, expert users seem more likely to adopt PMs [56].

Focusing on a specific demographic, Ray et al. [51] investigated what factors are most influential for older adults in adopting and using PMs and found a higher level of mistrust towards cloud storage and a higher fear of the PM being a single point of failure. They also note that, similar to reports by Pearman et al. [48], social support can overcome these barriers.

Several factors have been identified that generally act as barriers. Aside from a lack of ease-of-use and usefulness, security concerns [2, 14, 22, 41, 43, 48], involved cost [2, 4], privacy concerns [2, 14], low perceived risks [4, 7, 57], perceived loss of control over one's passwords [15], no perceived need for a PM [15, 16, 22], the PM acting as single point of failure [14, 16, 22], and having to use passwords on devices without the PM being available there [46] have been found to hinder adoption of PMS and using them to their full potential.

2.2 Password Managers & Security Posture

While using PMs has clear security advantages, security issues with the potential to negatively influence users' security posture can arise as well. Even if users choose to adopt a PM, it is not guaranteed that they will use it to their full potential. Lyastani et al. [37] showed that (a) password reuse was widespread among users of the PM integrated into the Chrome Browser (later corroborated by Mayer et al. [41]), and (b) that PM users still use a substantial number of weak passwords. While password audit features of PMs could potentially be a piece of the puzzle in addressing this problem, Hutchinson et al. [30] found that these audit features fail to report breached credentials and under-report weak passwords. However, even accurate reports might be misinterpreted by users [29].

From a more technical perspective, PMs have been found to be susceptible to a variety of attacks. For instance, Li et al. [36] found in their investigation of web-based PMs severe vulnerabilities that would allow attackers to learn arbitrary credentials saved in the PM. The causes for these vulnerabilities were very diverse. Oesch et al. [45] successfully recreated some of these vulnerabilities, in particular the usage of unencrypted metadata, insecure defaults, and vulnerabilities involving clickjacking.

Additional defenses have also been an important direction of work on password managers, targeted at improving users' security posture. Juels and Ristenpart [31] proposed to use Honey encryption, a technique that would allow generating decoy plaintexts in case a wrong key is used. Almeshekah et al. [5] harnessed physically unclonable functions or hardware security modules to a similar effect in their honey-pot proposal for PM vaults. Bojinov et al. [9] proposed an approach in which a large number of decoy PM vaults would be created. The goal of this approach, named Kamouflage by the authors, is to make it difficult for attackers to know which vault is the correct one. Chatterjee et al. [13] built on the previous approaches by combining Honey Encryption and Kamouflage. They proposed to use a natural language encoder to create decoy vaults on the fly, thereby improving the storage efficiency of the Kamouflage approach. While Golla et al. [25] could show that honey encryption is not effective in protecting PM vaults since an attacker can distinguish between real and decoy vaults, they also proposed improvements based on Markov models, which greatly enhance the resistance of PM vaults to these kinds of attacks.

2.3 Longitudinal Studies on Authentication

Many longitudinal studies have been conducted in the area of authentication. In particular, knowledge-based authentication has been studied in this fashion due to the involvement of human memory (e.g., [10,21,42,60]). Especially, research on graphical passwords includes retention sessions after longer periods of time in studies due to their improved memorability (e.g., [58]). Aside from the studies focused primarily on memorability, Hayashi et al. [27] performed a diary study in which participants recorded their daily password activities over the course of two weeks. Mare et al. [40] performed a similar study with participants over the course of one week, but instead of focusing solely on passwords, they included a greater variety of authenticators.

Apart from the password-related studies, several other technologies have been the focus of longitudinal studies. Colnago et al. [17] investigated the usability of two-factor authentication using log data spanning almost a year, and Owens et al. [47] investigated the perceived usability and security of FIDO2 roaming authenticators over the course of two weeks. Lassak et al. [35] investigated fallback authentication, i.e., secondary authentication used in case the primary authenticator is not available, in a long-term study over a duration of 18 months.

Very little longitudinal research on password managers seems to exist. Alkaldi et al. [3] tested their CyberPal PM recommender app over the course of two weeks with $n = 9$ participants. The feedback was used to improve the application, but no testing of actual PM usage was conducted. Aurigemma et al. [7] performed the study, which is closest related to our own. They investigated the motivators and barriers to voluntary use of PMs over the course of two weeks and found a variety of issues, ranging from low ease-of-use to a lack of trust in PMs as previously outlined in this section.

3 Methodology

3.1 Diary Study

We carried out a diary study to explore how first-time users use and value password managers (PM). Figure 1 shows the methodology overview, described in detail in this section. Participants used a PM in their day-to-day life for one month and evaluated it through weekly questionnaires. We selected novice participants to capture initial usability challenges and to get unbiased insights from first-time users, highlighting early adoption barriers. In our study, we defined novice users as those who had no prior experience using password managers. While we recognize that "novice" could also refer to individuals who are generally less tech-savvy, our sample consisted mostly of technically literate participants (see § 4). The PM we used in the study is 1Password [1]. We chose this PM because it is one of the most popular and consistently well-rated ones, contains a wide range of features – including checking the security status of all the stored passwords – and provides a free trial period.

Structure. Before starting the study, we run a screening phase to select participants who had never used a PM before and who would agree to submit screenshots of their basic PM usage statistics during the study, i.e., the number and quality of passwords as shown in Figure 2. The purpose of submitting usage statistics was to validate whether and to what extent they were using 1Password. The main study ran for one month and involved the following steps:

- **Introductory Questionnaire (Questions: QI-1-QI-32).** The goal of this survey was twofold. First, we captured non-users' habits in relation to passwords, i.e., how they store, create, and manage secrets. Second, we instructed them to install 1Password as part of a 3-month free trial family subscription we provided to the participants. Then we ask questions about the setup process to understand how they create the vault passwords, initialize the PM, and what type of problems appear at this initial stage. We asked for proof of successful installation and the stats screenshot showing the stored passwords. The questionnaire concluded by collecting demographic information, specifically: age range, gender, education, IT background, and English proficiency.

- **Usage Questionnaires x3 (Questions: QU-1-QU-28).** This questionnaire is administered three times: at the end of the first, second, and third week of PM usage, respectively. The goal is to track users' experience with the PM over time. Quantitatively, we measure the perceived usability through the standard System Usability Scale (SUS), which has been widely used[1] and been proved to be valid and reliable [50] [34]. Additionally, we ask participants open questions about their usage experience, their perceptions about the value provided by the PM, and whether and why they trust it.

- **Conclusion Questionnaire (Questions: QC-1-QC-33).** This was the last questionnaire in the main study, administered at the end of the fourth week. It aims at capturing participants' final reflections on the usage experience with the PM over the full month of usage. We ask participants to complete a final usability assessment of the PM on the SUS scale, and inquire about (a) perceived value, (b) the main problems they faced, (c) suggestions for improvement, and (d) their intention to use.

After the main study was concluded, we reached out to our participants again to ask if they were using a password manager 3 months later (the end of the trial period). The goal with this follow-up questionnaire (QF-1-QF-4) was to

[1] Since SUS was developed by Brooke [12] in 1996, more than 2300 individual surveys were conducted using SUS in over 200 studies by 2008 [8].

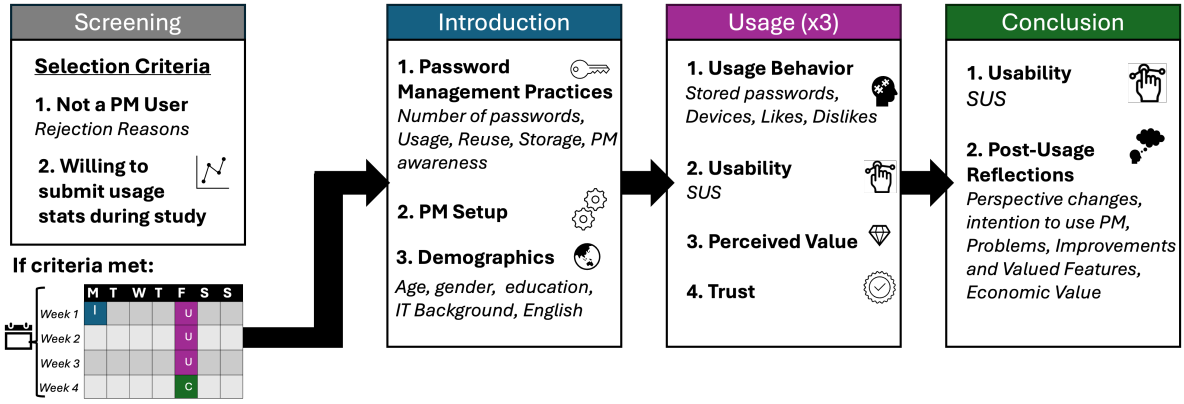


Figure 1: Structure of the user study. An initial screening is carried out to recruit participants that never used a password manager (PM). Then, the study is divided into three parts: (1) Introduction, instructing participants to use a PM; (2) Usage, a series of weekly questionnaires about the usage experience; and (3) Conclusion, to capture post-usage reflections.

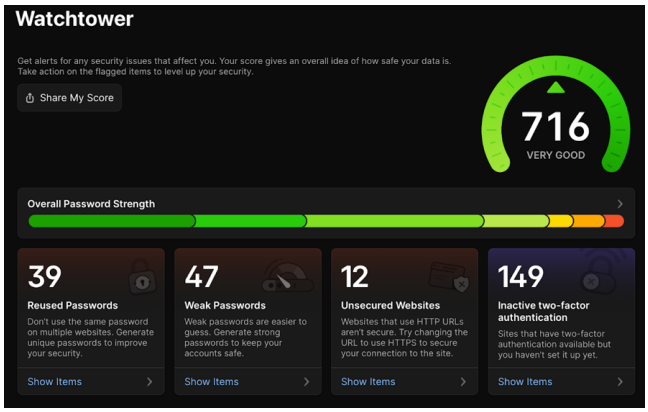


Figure 2: Interface of the 'Watchtower' functionality in the password manager 1Password. It provides a summary overview of the number of passwords stored and their security (e.g., reused, weak). Participants in the study should agree to provide screenshots of this interface during the usage period.

observe if the intention to use the PM voiced by participants was materialized in actual usage behavior. The complete survey instrument for the main study and follow-up is detailed in Appendix A.

Deployment and Ethical Assessment. The study was approved by the Institutional Review Boards of the universities the authors are affiliated with. We recruited participants using the KD²Lab panel run by Karlsruhe Institute of Technology in Germany. KD²Lab uses ORSEE [26]. The invitation email we used for the recruiting can be found in Appendix C. Participants were informed that the survey was anonymous, voluntary, and that all collected data would be processed according to the GDPR [19], before asking for consent and confirmation of being over 18 years old. We compensated participants according to the duration and effort involved in the questionnaires: 1€ for the screening, 5€ for the introductory questionnaire, 3€ for usage and concluding questionnaires, and 6€ for completing the follow-up. The screening was a 1-2 minute questionnaire, and the remaining questionnaires required an average effort of 15 minutes each. The introductory questionnaire was compensated higher to account for the time spent on installation and setup. The follow-up questionnaire payment was increased to motivate participants so that they would take part at the end of the trial period of 3 months.

During the study, participants were asked to submit a weekly screenshot with information about the passwords stored in their password managers. We informed them about this requirement in the screening questionnaire, explaining that this does not involve submitting any personal passwords or providing identifying information. For extra clarity, we included example screenshots and step-by-step instructions about how to generate them. The questionnaires were administered via a local SoSciSurvey platform instance hosted at Karlsruhe Institute of Technology.

We ask participants to install and use a tool that handles passwords and that can therefore impact their security. In this regard, we consider the benefits higher than the risks, given that using PMs is widely recognized as more secure than traditional password management strategies. Additionally, we selected a PM, 1Password, with a strong security reputation further mitigating risks.

3.2 Analysis

Quantitative Analysis. SUS scores were measured at four time points (weeks 1, 2, 3, and 4). To assess whether usability varied significantly across these time points, we performed a repeated-measures ANOVA with $\alpha = .05$. For participants who dropped out by week 4, we compared their week 1 SUS scores with those of participants who completed the full study with an independent t-test. For a meaningful interpretation of

the SUS scores, we report raw scores on a scale from 0 to 100 along with adjective-based ratings and acceptability classifications. According to *Bangor et al.*'s labeling scheme [8], SUS scores above 70 are generally considered acceptable. Specifically, scores up to 80 are labeled as 'good,' while scores above this value are deemed 'excellent' or 'best imaginable.' In contrast, scores between 51 and 70 fall into the 'marginally acceptable' category with an 'ok' rating, and anything below 51 is considered 'unacceptable.' These qualitative labels help to contextualize the numeric scores, providing a clearer understanding of users' perceptions of usability. In addition to measuring usability, we included two closed-ended questions assessing participants' trust in the password manager and perceived added value, both of which required a yes/no response. We used McNemar's test to detect whether participants' perceptions shifted significantly over time, by comparing responses collected in week 1 and at the end of the study.

Qualitative Analysis. We used a hybrid approach [23, 52] for coding the open-ended responses, combining inductive coding for questions without prior frameworks and pre-existing codebooks for questions where they were available [2, 48]. Due to the reduced sample size, we opted for a collaborative approach to coding instead of calculating inter-coder reliability metrics that would have been unstable [39]. Two coders worked together to develop and refine the coding scheme through iterative discussions, resolving discrepancies by consensus rather than relying solely on statistical agreement metrics. We report the percentage of times each code was mentioned when participants answered each question.

Pilot testing. We ran a pilot study in December 2022 with 7 participants to pre-test the six questionnaires of the study. To make the pilot quick, we adjusted the planning of the questionnaires to a 2-week schedule instead of the final 1-month duration. Participants would install the PM on day 1, report usage every two days, and answer the final questionnaire on the last day. Of the 7 participants who passed the screening, 2 completed all the questionnaires. Incomplete submissions were from 3 participants who confirmed they were already using a PM in the additional eligibility check in the introductory questionnaire, and 1 participant who abandoned the study. From the pilot results, we observed that participants did not completely follow the instructions to upload the screenshot about password statistics. We explicitly pointed them to the web interface because not all of the native interfaces of 1Password show the number of passwords stored, yet they submitted the summary provided by the non-web interface. To avoid this problem in the final study, we highlighted that part of the instructions in bold.

4 Results

The study was conducted between July and October 2023. It was advertised on July, 4th 2023 to potential participants: >=18 years old, fluent in English, and who did not participate in the pilot. In the next couple of days, 336 people took part in the screening. From this sample, 87 did not use a PM, of which 78 met the additional eligibility criteria on willingness to submit PM usage statistics. Finally, 62 people went on to initiate the introductory questionnaire, and 37 remained in the study after validating the eligibility double check in this questionnaire: participants who failed it were not truly novice PM users, but mostly stored their passwords in browser-based PMs. Table 1 summarizes the demographic information of the sample at the start of the study: skewed towards men (64.8%), covering ages from 18 to 34, most of them having completed post-secondary education (59.4%), and having a background in IT (67.5%).

Table 1: Detailed participant demographics.

		n = 37
Gender	Female	11
	Male	24
	Prefer not to say	2
Age	18-24	21
	25-34	16
Education	High school	14
	Bachelor's degree	15
	Vocational training	2
	Master's degree	6
IT	No	11
	Yes	25
	Prefer not to say	1

4.1 Starting Using a Password Manager

Despite not being PM users, the majority of participants (32, 86.5%) have heard about password managers before the study. The top reasons for not using them are "no perceived usefulness" (35.2%), "security concerns" (23.8%), and "perceived effort" (12.3%), echoing the findings in previous studies [2, 41, 48] .

Managing Passwords Without Managers. Participants reported having an average of 36 (*Min=5*, *Max=150*, *SD=34.5*) passwords and using an average of 7 accounts on a daily basis (*Min=2*, *Max=25*, *SD=5.1*). They mostly keep track of passwords by remembering them or writing them down. More than half (54%) of the participants report reusing passwords for some accounts. On average, they had 8 accounts with unique passwords. When deciding to reuse, the most common approaches consist of clustering the accounts by type and using the same password for accounts within the same category (82.14%). Grouping is based on: security level, importance, or service type (e.g., university-related services). Another common reason to reuse passwords is doing so for frequently used

accounts (10.7%). A few answers (7.1%) mentioned reuse based on the password policy requirements.

Setting up a PM for the first time. The first step to start using a PM is creating an account for it and setting up its primary password [2]. When confronted with the task of selecting a primary password, participants choose a secret similar to their other passwords (51%) and not difficult to remember (73%). Notably, 44% of the answers about how participants created a primary password involve total or partial reuse of existing secrets or personal data: 21% reused a password, 18% reused a password with some variation, and 6% used pieces of personal information with some tweaks or variations added. The most commonly reported approach to keep track of the primary password was remembering it (59.1%), followed by storing it somewhere (40.9%), from writing it in a notebook to storing it in the browser.

1Password offers an "Emergency Kit" option when setting up the PM, i.e., a PDF file that includes a secret key and space for the user to write their primary password. This information should be saved securely as a backup when the user loses access to the PM and needs to recover it. Only 5 out of the 37 participants wrote their primary password in the emergency kit, and the majority stored the file in their computer (67.5%). Interestingly, 4 people did not know where they stored the emergency kit. The rest chose to store it in a physical place or the cloud, and only 1 person did not store it.

After account creation, our participants were tasked with installing the password manager. They could do so on one or more devices. 35 participants installed the PM in a single device, while two persons opted for 2 devices (computer & smartphone). Table 2 gives an overview of the devices on which the participants used 1Password the most. Nobody reported problems during the installation, and successful installs were confirmed by the submitted screenshots.

The final step to starting to use the PM required saving passwords in it. Participants reported storing an average of 2.6 passwords (maximum 10). When saving passwords, the majority of participants (33, i.e., 89%) did it manually, while 4 participants used the import function[3]. The only report of problems during configuration was indeed related to importing passwords, which required the participant to consult the PM help documentation to solve the issues. No other problems appeared. The most common reason to decide which accounts to store in the PM was frequent usage (36%).

At the end of the configuration process, we asked participants if they had changed any of their passwords during the process, as this type of behavior could be triggered when learning about the quality and reuse frequency of the stored passwords. This piece of information is provided right away by the PM. Only one participant did so, reasoning that:

> *"[I] felt like I used one of my password options too often so I decided to set a new one following my password scheme" - P1*

Overall, inaction regarding password improvement was common despite the PM alerting users about their weak passwords, as will be discussed in the next section.

4.2 Usage Experiences

Study participants used the password manager for one month and reported their experience weekly. The first week retained 33 users, a number that decreased to 28 by the second week, and dropped to 23 and 19 in weeks 3 and 4, respectively.

Usage Behavior. Participants reported using the password manager initially for an average of 5 accounts, increasing to 6 accounts by the end of the study. The most used types of accounts were social media, emails, and online shopping. In turn, the most common type of account that users deliberately opted out of storing in the PM was bank accounts. The reasons behind this choice included fear of data breaches, the conviction that financial-related passwords should not be saved anywhere, and being unsure if they trusted the PM:

> *"I did not use it for bank accounts, because I know too little about the app to enter highly sensitive information." - P30.*

This opinion shifted for some participants during the course of the study: while nobody stored bank accounts at the beginning, 3 participants started doing so in the second week.

Regarding likes and dislikes of using the password manager, our findings partially overlap with those from previous studies [41,48]. Participants' top liked aspects are not needing to type or remember their passwords, while common negatives are complexity and incompatibility issues. The most common new reason for not liking password managers is the need to (frequently) unlock them with the primary passwords. According to our participants, this makes the process inefficient:

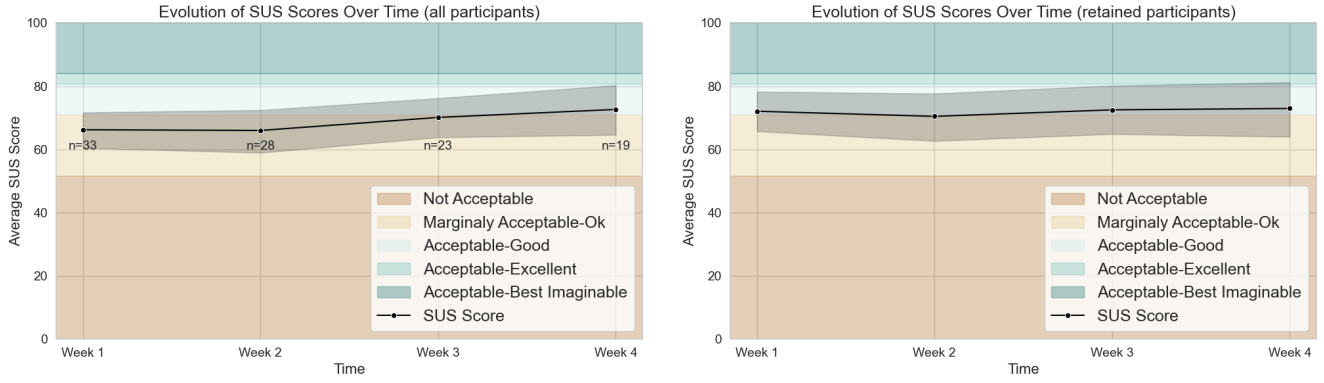
> *"Always [have to] enter the master password. It's easier for me to just enter my normal password of the website." - P28.*

> *"I have to enter my general password every day to log in to the software. In that case, I may as well log in to the website I need with my username and password." - P24.*

Usability. Participants rated the usability of the password manager on the SUS scale at the end of each week. The average usability was lower at the beginning, with a score of

[2] Primary password (also referred to as *master password*, *main password*, or *vault password* in some literature) is the single password required to unlock a password manager's vault, granting access to all stored credentials.

[3] Note that participants using the import function does not necessarily indicate that participants used another password manager previously. 1Password allows importing passwords in CSV format, which can also stem from, e.g., manually created spreadsheets.



(a) All participants

(b) Retained participants

Figure 3: (a) Shows the average SUS scores given by all study participants to the password manager each week. While there is a positive usability trend, the number of users evaluating the tool varies, decreasing from $n = 33$ to $n = 19$ over time. If we consider the $n = 19$ retained participants, the average usability shown in (b) is higher and stable over time.

66.25 ($\pm$ 16.35), increasing up to 71.62 ($\pm$ 18.1) after one month. However, when looking only at the ratings given by the users who completed the four questionnaires, the usability varies minimally over time and is not statistically significant, staying between ~70-73 points, which is considered a "Good" usability level [8]. This could suggest that users who had a more negative experience were more likely to drop out. Indeed, when comparing the average SUS scores given in the first week by participants who continued using the password manager (71.8) versus participants who abandoned the study (58.57), the stark difference of around 13 points is statistically significant ($t(31) = 2.48, p = .019$). Figure 3 summarizes these differences, highlighting how usability lies at an acceptable level for retained users, while it is only marginally acceptable when considering dropouts.

Trust and Perceived Value. Most participants reported trusting the password manager at the beginning of the study (69.7%), and this ratio increased after usage (78.3%). The most common reason to place trust in the PM was transitive trust (28% of mentions). Participants trusted the research institutions conducting the study and, therefore, the PM to be used in it:

> *"Because it is part of a study of well-known research institutes" - P33.*

Other frequently mentioned reasons to trust the PM were *"because it is well designed"* (10%) or *"looks serious"* (7%), and because of the *"good online reviews"* (14%).

Over the course of the study, no participant changed their opinion from trusting to not trusting the PM, and 4 participants went from no trust to trust. Those users who shifted their trust perception positively named reasons related to good usage experience, such as *"nothing bad happened"*, *"seems to work fine"*, or they educated themselves by reading online reviews. Still, 5 participants used the PM by the end of the study while reporting no trust in it. The reasons for distrust are not knowing enough about how the PM works to protect their data, or they trusted it to a high degree but not completely, because *"you can't guarantee 100% that this software is not hackable" (P12).*

When it comes to the value of using a PM, 51.5% of our participants reported seeing a great value at the beginning, and this perception increased slightly during the study (56.5%). Positive participants appreciated the convenience of the PM (62%), especially in terms of reduced memory burden (21%):

> *"Saving some time and the more accounts I use the password manager for I less have to think about the password of each account." - P16.*

The most frequent reasons for skepticism among the participants who did not see a great added value in using the PM were: having another strategy for managing or storing passwords (50%) and the need for extra steps to log in to the PM (10%).

> *"In order to use this software you have to type in your general password every day or even worse you have to type it in again after 10 minutes of no activity. There is no additional value because I do not save any time. Moreover there is still one problem: Where do I store my general password?? How is this more safe than a sheet of passwords?" - P24.*

The skepticism about the password manager providing a great added value is also reflected in the participants' subscription sharing behavior. Only 2 people shared their subscription. The most popular reasons not to do it are because they see no need or are not convinced about the usefulness of the tool

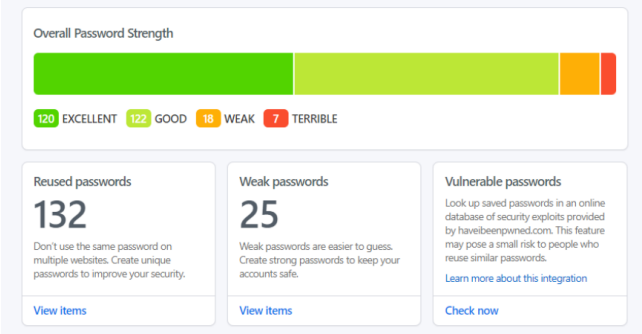


Figure 4: Overview of participant P15's password health at the end of the study. The password manager flags 25 passwords as weak or terrible and 132 as reused. This same status was kept during the whole 1-month usage period, showing the user took no action to address the warnings.

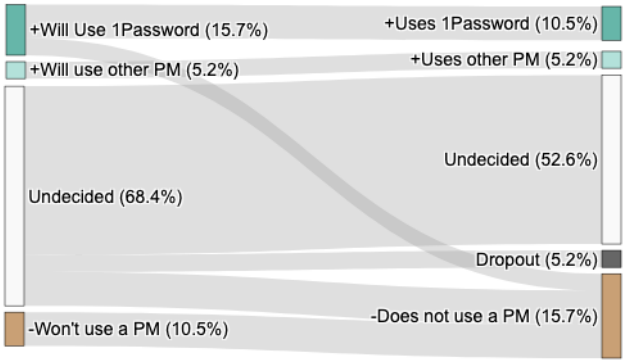


Figure 5: User decisions regarding adopting a password manager after trying one for 1 month (left), and 3 months later (right). Of n=19 participants, 3 decided to use a PM, 3 decided against, while the majority remains undecided.

(20%), and because the topic did not come up with their acquaintances (15%) or there was no interested person (16%). Another non-negligible type of reason was security and not needing or wanting other persons to see their passwords (8%), which points at a misconception in what sharing in the family subscription model entails: it is about sharing the cost of the subscription and the ability to share password vaults, but each user would still have an independent account and private credentials. Additionally, other reasons for not sharing were related to social aspects, such as thinking their acquaintances would not be interested or require support from them, or they found password managers an uncommon topic to discuss in social situations:

> *"Password security did not come to my mind when socializing with others." - P30.*

Observations on Password Hygiene. When analyzing the screenshots of the password manager usage uploaded by participants, we observed that some went on to store more passwords than those reported during setup. While the numbers generally aligned with the claimed moderate usage of accounts (5-6), two participants had a much higher number of passwords stored in the database by the end of the study (168 and 267). What is noticeable is that the majority of users (78.94%) in week 4 had warning flags indicating poor or reused passwords. Despite seeing these warnings every time they uploaded the screenshot throughout the study, nobody changed their credentials to improve security. Additionally, participants reported not using the password generator function embedded in the PM for all their passwords, mostly due to convenience issues: they want to remember their passwords, not depend on the PM, or it is too much effort to change passwords.

4.3 Post-Usage Reflections

Of the remaining 19 participants who answered the concluding questionnaire, only one reported problems during usage. The issue mentioned highlighted the importance of the user interaction experience in fostering trust:

> *"I received a pop-up window from the password manager at least twice which said that "Something went wrong: An unknown error occurred...." This is very scary considering that I am supposed to entrust this software with all my important passwords..." - P24.*

When asked about concrete suggestions for improvement, 7 participants did not offer any recommendations, many of them also specifying that the PM is fine as it is. The most common wishes for enhancement (72%) were related to convenience: streamlining the login process to avoid having to enter the primary password frequently, and facilitating password creation and storage, for example, through easier import mechanisms. The rest of the suggestions pointed to the need for better documentation, such as including how-to videos, and overcoming security concerns that users might have.

While the answers to problems and improvements reflect satisfaction with the PM, 10 out of 19 participants would not recommend using a password manager. Unfortunately, not all participants provided reasons as to why they would not recommend it, but simply stated they were 'not convinced' or 'not sure'. Others cited reasons such as poor user experience, wanting more time with the password manager before recommending it, or the desire to explore other password manager options before making the decision. Additionally, 8 participants are open to paying for using this type of tool.

When asked about their own intention to use a password manager after the study, only 2 people responded negatively; 3 participants said they will use 1Password, of which 2 actually

did so as reported in the follow-up questionnaire (the other participant changed their mind because the low frequency of using the PM did not justify the cost). The most common answer, though, was being uncertain: 13 users wanted to reconsider after the end of the license trial period. From these undecided users, 12 answered the follow-up questionnaire and 10 did not change their mind, being still undecided. The remaining 2 decided not to use the password manager because of a low frequency of usage and the cost of the license. The only person who said they will consider using another PM reported using iCloud in the follow-up questionnaire. Usage (intentions) are summarized in Fig. 5.

5 Discussion

5.1 From Setup to Security: Bridging the Gaps

All our participants succeeded in installing and setting up the password manager, but there is still a long way from setup to effective use. A majority (54%) of participants reuse passwords, including their primary password, demonstrating a strategic yet problematic approach to security. This weak foundation undermines the security benefits of using a password manager in the first place. Compounding this issue, many participants did not engage with the credential audit tools designed to highlight security risks. While, by study design, all participants saw their password health dashboard every week when uploading the respective screenshot and almost 80% had bad passwords, they did not act on this information. This suggests that visibility, clarity, and timing of security notifications may play a role in user disengagement, which aligns with previous research pointing to usability issues in credential audit tools [32, 46].

To address these issues, future designs should focus on (1) assisting users regarding primary password creation, thereby stressing the dangers of password reuse, (2) integrating nudges – such as commitment mechanisms [49] – that encourage users to change weak passwords immediately when entering them into the PM and to engage with security audits throughout use, and (3) improving the presentation of password health warnings to ensure they are actionable rather than ignored. Unfortunately, our study does not give concrete recommendations on how to achieve each of these. Studying effective designs and nudges represents an important direction of future work.

5.2 More Than Words: Improving Help

Our findings show that while users actively seek online reviews of PMs to judge whether they want to use them, users would like to have more than text-based explanations, suggesting the introduction of videos as support. Their behavior further reinforces the need for better documentation. One of the most common frustrations was the frequent need to reenter the primary password to unlock the PM. However, this inconvenience could be mitigated through existing customization options, such as adjusting auto-lock timing or enabling biometric authentication. The fact that users struggled with this (during 1 month of usage) suggests that documentation and onboarding failed to make these features discoverable and actionable. Future studies should investigate how to add proper affordances to PMs to make these features more easily accessible for users.

Future efforts should focus on (1) diversifying documentation formats to match different learning preferences, (2) embedding interactive guidance within critical workflows, and (3) ensuring that security settings are surfaced when they are most relevant. e.g., through designs with proper affordances. Considering the issues discussed in section 5.1, *just-in-time* help on choosing a primary password and support for understandable and actionable credential audits are clear points to support an efficient use of PMs. Similarly, resolving misconceptions on what it means to share a PM subscription could help improve social engagement, which increases adoption potential.

5.3 Usable, but not Recommendable

The literature on social cybersecurity shows that users engage in positive security and privacy behaviors more frequently when spurred on by social triggers than when forced to do so [61], be it through conversation, observation, or other broader forms of peer connection. The importance of word-of-mouth recommendations has even been shown specifically for the PM context [41]. In our study, however, we observe several behaviors that point to a lack of social engagement with PMs. Participants rarely shared their password manager subscription, with only 2 out of 37 participants doing so, and more than half (52%) not intending to recommend a PM. The reasons varied. Some were not fully convinced of the tool's value, while others felt their friends and family did not need it. And for many, security was simply not a topic that came up in conversation. This lack of social reinforcement may hinder broader adoption.

Another factor potentially influencing word-of-mouth recommendation of password managers is usability perception. Our study participants rated the PM with a SUS score of around 70 points. Prior research suggests a link between SUS and Net Promoter Score (NPS), where products with a SUS below the 80th percentile tend to have fewer enthusiastic promoters [11].

The observed barriers underscore the need to shift password managers from a personal security tool to a socially endorsed practice to positively influence adoption. Potential avenues for this are (1) encouraging trust in PMs and (2) having security champions endorse PMs in their social circles. As outlined above, increasing PM usability must come first, though.

5.4 Running Longitudinal Studies

One challenge in our study was participant retention over time. While 37 participants initially installed the tool, only 33 remained engaged after the first week, and 19 completed the full four-week study. This attrition rate aligns with previous research on longitudinal studies in usable security, specifically on authentication [25,27,40,47,53,59], where sustained engagement can be difficult due to participant fatigue, competing priorities, and perceived burden.

To mitigate dropout, we offered compensation and distributed incentives for partial completion. We also implemented weekly reminder emails to encourage continued participation. For future studies, we suggest experimenting with tailored engagement strategies, reaching out to inactive participants with personalized follow-ups [62].

5.5 Limitations

As with many user studies, the small sample size limits the generalizability of our findings to some extent. Although qualitative results are reported using count data for context, we acknowledge that the number of participants expressing a particular idea does not necessarily represent the true prevalence of any practice or belief. Our population demographic is fundamentally young (<35) and limited to people living in Germany. Future research should explore more diverse populations to uncover further usability issues with password managers.

Attrition was notable, with only 57% of participants who completed the first weekly questionnaire finishing the study. While some dropout was likely due to the challenges of using a PM, we did not collect specific reasons as to why participants dropped out. Future work could incorporate questions in this regard in order to achieve closer tracking and investigate potential dropout mitigations. Additionally, it must be noted that participants may have exhibited transitive trust in 1Password as this was the manager to be used in the study. Indeed, some participants reported trusting the PM because it was recommended in this study by reputable institutions. While this may introduce bias, participants' acknowledgment of trust by recommendation highlights the social dimension of security and its crucial role, if participants were more likely to recommend PMs among their peers.

Finally, while our study is the longest longitudinal study on password manager usability reported on in the research literature, it is still possible that the time frame of our study was too short, and some usability issues might decrease further with prolonged use. However, we chose the four-week time frame with a follow-up after the third month to balance research validity and feasibility. Most importantly, this time frame is aligned with the typical durations of trial periods for paid password managers, which increases external validity: It is reasonable to assume that our findings represent the experiences of users during the trial period, based on which the users would have to decide whether to continue using the PM. It also allowed us to collect participants' initial experiences as well as perceptions over time, while not overstraining our ability to recruit participants and retain them in the study. Yet, future studies exploring password manager usability as well as barriers and motivators to continued use of password managers over an even longer period of time would represent an important direction of future work.

6 Conclusion

Our longitudinal study highlights key barriers to password manager adoption that persist beyond initial exposure. While trust in the tool improved over time, perceived usability remained stable, with first-impression hurdles shaping long-term engagement. Many users struggled with primary password creation and ignored credential audit warnings, limiting the security benefits of the manager. To bridge these gaps, future designs must prioritize actionable security feedback, and methods to integrate PMs into everyday security habits.

Acknowledgments

We want to thank 1Password for providing the trial licenses to us and especially Thom Rhodes of the 1Password team for his support. We also would like to acknowledge the awesome help of Anke Greif-Winzrieth, who handled our study at the KD²Lab. We are grateful to Roberto Bifulco for his contribution to the coding of survey responses. Additionally, we want to thank Pavlina Nguyenova for her work on piloting the study.

This work was funded by the Topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and supported by KASTEL Security Research Labs. The study in this work was conducted in the Karlsruhe Decision&Design Lab (KD²Lab), an experimental lab funded by the DFG and KIT (INST_12138411-1_FUGG).

References

[1] 1Password. https://1password.com/. Accessed: 2024-10-15.

[2] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? pages 1–14, 2016.

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

Hawaii International Conference on System Sciences, 2019.

[4] Nora Alkaldi and Karen Renaud. MIGRANT: Modeling Smartphone Password Manager Adoption Using Migration Theory. *SIGMIS Database*, 53(2):63–95, 2022.

[5] Mohammed H Almeshekah, Christopher N Gutierrez, Mikhail J Atallah, and Eugene H Spafford. ErsatzPasswords: Ending Password Cracking and Detecting Password Leakage. Annual Computer Security Applications Conference, pages 311 – 320, 2015.

[6] Patricia Arias-Cabarcos, Andrés Marín, Diego Palacios, Florina Almenárez, and Daniel Díaz-Sánchez. Comparing password management software: toward usable and secure enterprise authentication. *IT Professional*, 18(5):34–40, 2016.

[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 *Hawaii International Conference on System Sciences*, Hawaii International Conference on System Sciences, pages 4061–4070, 2017.

[8] Aaron Bangor, Philip T Kortum, and James T Miller. An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction*, 24(6):574–594, 2008.

[9] Hristo Bojinov, Elie Bursztein, Xavier Boyen, and Dan Boneh. Kamouflage: Loss-Resistant Password Management. In *Proceedings of the 15th European Symposium on Research in Computer Security*, European Symposium on Research in Computer Security, pages 286–302, 2010.

[10] J Bonneau and S Schechter. Towards reliable storage of 56-bit secrets in human memory. USENIX Security Symposium, pages 607 – 623, 2014.

[11] John Brooke. Sus: a retrospective. *Journal of usability studies*, 8(2), 2013.

[12] John Brooke et al. SUS-A quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.

[13] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. Cracking-Resistant Password Vaults Using Natural Language Encoders. In *IEEE Symposium on Security & Privacy*, IEEE Symposium on Security & Privacy, pages 481–498, 2015.

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

[15] Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *Proceedings of the USENIX Security Symposium*, 2006.

[16] Mark Ciampa. A Comparison of User Preferences for Browser Password Managers. *Journal of Applied Security Research*, 8(4):455–466, 2013.

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

[18] Statista Research Department. Password storage habits in germany. 2023.

[19] EU. General data protection regulation. 2016. Available at: https://gdpr-info.eu/ (accessed: 15.09.2022).

[20] European Union Agency for Cybersecurity (ENISA). Cyber Hygiene, 2025. Accessed: 2025-02-07.

[21] Katherine M Everitt, Tanya Bragin, James Fogarty, and Tadayoshi Kohno. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Conference on Human Factors in Computing Systems*, Conference on Human Factors in Computing Systems, pages 889 – 898, 2009.

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

[23] Jennifer Fereday and Eimear Muir-Cochrane. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International journal of qualitative methods*, 5(1):80–92, 2006.

[24] Bundesamt für Sicherheit in der Informationstechnik (BSI). Sichere passwörter und passwort-manager empfehlungen. 2023.

[25] Maximilian Golla, Benedict Beuscher, and Markus Dürmuth. On the Security of Cracking-Resistant Password Vaults. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM SIGSAC Conference on Computer and Communications Security, page 1230–1241, New York, NY, USA, 2016. Association for Computing Machinery.

[26] Ben Greiner. Subject pool recruitment procedures: organizing experiments with ORSEE. *Journal of the Economic Science Association*, 1:114–125, 07 2015.

[27] Eiji Hayashi and Jason Hong. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2627–2630, 2011.

[28] Nicolas Huaman, Sabrina Amft, 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. *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1367–1381, 2021.

[29] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. Users' Perceptions of Chrome Compromised Credential Notification. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Symposium on Usable Privacy and Security, pages 155–174, Boston, MA, 2022. USENIX Association.

[30] Adryana Hutchinson, Collins W. Munyendo, Adam J Aviv, and Peter Mayer. An Analysis of Password Managers' Password Checkup Tools. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2024. Association for Computing Machinery.

[31] Juels, Ristenpart, Ari and, and Thomas. Honey Encryption: Security Beyond the Brute-Force Bound. In *EUROCRYPT 2014*, EUROCRYPT 2014, pages 293–310, 2014.

[32] Emiram Kablo, Katharina Kader, and Patricia Arias-Cabarcos. "i'm actually going to go and change these passwords": Analyzing the usability of credential audit interfaces in password managers. In *Extended Abstracts of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI EA '24, New York, NY, USA, 2024. Association for Computing Machinery.

[33] Sabrina Klivan, Sandra Höltervennhoff, Nicolas Huaman, Yasemin Acar, and Sascha Fahl. "Would You Give the Same Priority to the Bank and a Game? I Do Not!" Exploring Credential Management Strategies and Obstacles during Password Manager Setup. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, Symposium on Usable Privacy and Security, pages 171–190, Anaheim, CA, 2023. USENIX Association.

[34] Philip Kortum and S Camille Peres. The relationship between system effectiveness and subjective usability scores using the system usability scale. *International Journal of Human-Computer Interaction*, 30(7):575–584, 2014.

[35] Leona Lassak, Philipp Markert, Maximilian Golla, Elizabeth Stobert, and Markus Dürmuth. A Comparative Long-Term Study of Fallback Authentication Schemes. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2024. Association for Computing Machinery.

[36] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. USENIX Security Symposium, pages 465 – 479, 2014.

[37] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Sven Bugiel, and Michael Backes. Studying the impact of managers on password strength and reuse. *arXiv preprint arXiv:1712.08940*, 2017.

[38] 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.

[39] Catherine MacPhail, Nomhle Khoza, Laurie Abler, and Meghna Ranganathan. Process guidelines for establishing intercoder reliability in qualitative studies. *Qualitative research*, 16(2):198–212, 2016.

[40] Shrirang Mare, Mary Baker, and Jeremy Gummeson. A study of authentication in daily life. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*, pages 189–206, 2016.

[41] 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.

[42] Peter Mayer, Melanie Volkamer, and Michaela Kauer. Authentication Schemes - Comparison and Effective Password Spaces. volume 8880 of *International Conference on Information System Security*, pages 204 – 225, 2014.

[43] Collins W Munyendo, Peter Mayer, and Adam J Aviv. " i just stopped using one and started using the other": Motivations, techniques, and challenges when switching password managers. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 3123–3137, 2023.

[44] National Cyber Security Centre (NCSC). What does NCSC think about password managers?, 2021. Accessed: 2025-02-07.

[45] Sean Oesch and Scott Ruoti. That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers. In *29th USENIX Security Symposium (USENIX Security 20)*, USENIX Security Symposium, pages 2165–2182. USENIX Association, 2020.

[46] 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*, CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2022. Association for Computing Machinery.

[47] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. User perceptions of the usability and security of smartphones as {FIDO2} roaming authenticators. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 57–76, 2021.

[48] 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)*, pages 319–338, Santa Clara, CA, August 2019. USENIX Association.

[49] Eyal Peer, Alisa Frik, Conor Gilsenan, and Serge Egelman. "protect me tomorrow": Commitment nudges to remedy compromised passwords. *ACM Transactions on Computer-Human Interaction*, 2024.

[50] S Camille Peres, Tri Pham, and Ronald Phillips. Validation of the system usability scale (SUS) SUS in the wild. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 57, pages 192–196. SAGE Publications Sage CA: Los Angeles, CA, 2013.

[51] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why older adults (don't) use password managers. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 73–90. USENIX Association, August 2021.

[52] Johnny Saldaña. The coding manual for qualitative researchers. 2021.

[53] M Angela Sasse, Michelle Steves, Kat Krol, and Dana Chisnell. The great authentication fatigue–and how to overcome it. In *Cross-Cultural Design: 6th International Conference, CCD 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 6*, pages 228–239. Springer, 2014.

[54] 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.

[55] James Simmons, Oumar Diallo, Sean Oesch, and Scott Ruoti. Systematization of password manageruse cases and design paradigms. In *Proceedings of the 37th Annual Computer Security Applications Conference*, pages 528–540, 2021.

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

[57] Xiaoguang Tian. Unraveling the dynamics of password manager adoption: a deeper dive into critical factors. *Information & Computer Security*, 33(1):117–139, 2025.

[58] Thomas S Tullis, Donna P Tedesco, and Kate E McCaffrey. Can users remember their pictorial passwords six years later. In *CHI'11 Extended Abstracts on Human Factors in Computing Systems*, pages 1789–1794. 2011.

[59] Dirk Van Bruggen, Shu Liu, Mitch Kajzer, Aaron Striegel, Charles R Crowell, and John D'Arcy. Modifying smartphone user locking behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–14, 2013.

[60] Naomi Woods and Mikko Siponen. Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, 128:61–71, 2019.

[61] Yuxi Wu, W Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1863–1879. IEEE, 2022.

[62] Akira Yamada, Kyle Crichton, Yukiko Sawaya, Jin-Dong Dong, Sarah Pearman, Ayumu Kubota, and Nicolas Christin. On recruiting and retaining users for security-sensitive longitudinal measurement panels. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 347–366, 2022.

A Survey Instrument

A.1 Consent Forms

A.1.1 Screening Questionnaire

We are recruiting participants for a research study about password managers. The survey that follows will ask you a series of questions about your usage of password managers to evaluate if you qualify for the study. It will take you 1-2 minutes to

complete and you must be age 18 or older to participate. If you are eligible, we will reach out to you to give you further information. If you decide to join, you will have to install and use a password manager for 1 month, and answer questionnaires about your experience. By participating, will be compensated with up to 20 EUR if you use the manager and complete all questionnaires. Your participation in the eligibility survey is voluntary and you may abandon it at any time. The collected data will be used for scientific purposes only. We collect and store your email address to send you details about the study. Your e-mail address will be deleted immediately after the end of the study in accordance with data protection regulations.

We are a group of researchers from <Institutions>. If you have questions, you can reach us at <contact information>.

☐ I have read and understood these terms and conditions, and I agree to be contacted if I'm eligible for the study.

A.1.2 Diary Study - Consent

General Information Thank you for your interest in this survey. We are a team of researchers from <Institutions>. Your participation will help us to better understand the usability problems of password managers. You can participate if you are over 18 years old and have a laptop or desktop computer with Internet access. The study will include five questionnaires over the course of four weeks with an average effort of 15 minutes each questionnaire.

Procedure and Participation If you decide to participate, we will ask you to install and set up a password manager and use it for four consecutive weeks. Each week you must answer a set of questions. The possible risks for the participants in this online study are those associated with computer tasks, such as mild fatigue. The benefits for you are, among other things, the daily use of a password manager, which will help you to manage your various credentials. Participation in the survey is voluntary and you are free to leave the study at any time.

Data Collection and Processing For the purpose of your participation in this research study we process your e-mail address as personal data. Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Art. 4, No. 1 of the EU General Data Protection Regulation (GDPR)). We collect and store your email address so that we can use it to send you a weekly questionnaire. Your e-mail address will be deleted immediately after the research study is finished (when you complete the last questionnaire), in accordance with data protection regulations. The questionnaire answers will be kept and processed anonymously. Please do not enter any personal data, even from other persons, in the free text fields. The information collected in the study questionnaires is used only for research purposes. The collection of socio-demographic data such as gender etc. is carried out solely for the purpose of evaluating the statements group heterogeneously. No attempt will be made based on the information you have provided to draw conclusions about specific persons. The evaluation results will be published in an anonymous form (in tables and / or graphics), so that it is not possible to draw conclusions about individuals.

Data Controller Responsible for the data processing according to Art. 4, No. 7 GDPR as well as other data protection regulations: <Institution information>

Legal basis The legal basis for the processing is your consent in accordance with Art. 6, par. 1, clause 1 (a) GDPR. According to Art. 7 par. 3 GDPR you have the right to withdraw your consent at any time with effect for the future. The consent is voluntary. There are no disadvantages for you if it is denied or withdrawn.

Your rights You also have the following rights: You have the right to obtain information from <Institution> about the data stored about you and/or to have incorrectly stored data corrected. You also have the right of erasure or limitation of processing or the right to object to processing.

You have the right to withdraw your consent at any time, whereby the lawfulness of processing based on consent before its withdrawal is not affected. To assert these rights, please contact: <Contact Information>

You also have the right to lodge a complaint with a supervisory authority about the processing of the personal data concerning you by <Institution>. <Contact Information>.

A.2 Questionnaires

A.2.1 Screening Questionnaire

Password Managers
Password managers are tools that can securely handle passwords for you. They can remember your passwords, generate new ones, and even sync them across devices. There are various types of password managers:

- If you allow your web browser to save your passwords, you are using your browser's password manager.
- Third-party application password managers are software that you install directly onto your devices or a service you can access on the web.
- Your operating system can serve as a password manager as well. For example, the Keychain functionality on MacOS can remember passwords in and out of your browser.

QS-1 Based on our description, which password managers are you currently using? (☐ I don't use any password manager ☐ Password Manager as a third-party application ☐ Browser Password Manager (e.g., Google Chrome, Internet Explorer) ☐ ystem Password Manager (e.g., Keychain) ☐ Other _____)

If you decide to participate in our study, we will ask you to install and use a password manager. As part of the study, we need to collect anonymous data regarding usage. We will not ask you to submit any personal passwords or provide any information that would allow us to identify you.

QS-2 Would you be willing to submit a screenshot with the statistics shown in the image? (○ Yes ○ No)

QS-3 Why did you reject using a PM so far? (circText)

A.2.2 Introductory Questionnaire

Password Management Practices

QI-1 To the best of your knowledge, approximately how many online accounts do you have that use passwords? (Number)

QI-2 How many of your online accounts do you access on a daily basis? (Number)

QI-3 How do you keep track of your passwords? (☐ Password book ☐ Word Document ☐ Remember ☐ Lastpass ☐ Bitwarden ☐ Dashlane ☐ Keepass ☐ 1Password ☐ Firefox ☐ Chrome ☐ Other _____)

QI-4 Are your passwords different for each account? (○ Yes ○ No)

QI-5 Under what circumstances do you reuse your passwords? (for example: unimportant forums, frequently used websites, ...) (circText)

QI-6 How many of your accounts have unique passwords? (Number)

QI-7 Have you ever heard of password managers before this study? (○ Yes ○ No)

Account Creation

Start using 1Password, you need to create an account and install the password manager application on your computer. Account creation without interruptions takes between 5-10 minutes. Please use the following link to create your account and return to this questionnaire page when you are finished: [link]

QI-8 How did you create your master password? (The master password is the password you use to sign in to 1Password.com and unlock the 1Password apps, it's your account password) (Free text)

QI-9 Is your master password similar to your other passwords? (○ Yes ○ No)

QI-10 Is it difficult to remember your master password? (○ Yes ○ No)

QI-11 How will you keep track of your master password? (☐ Password book ☐ Word Document ☐ Remember ☐ Lastpass ☐ Bitwarden ☐ Dashlane ☐ Keepass ☐ 1Password ☐ Firefox ☐ Chrome ☐ Other _____)

QI-12 Did you write your master password in the Emergency Kit? (○ Yes ○ No)

QI-13 How did you store your Emergency Kit? (○ printed it and stored it in a physical place ○ stored it in my computer ○ I don't know ○ I didn't store it)

Password Manager Installation

Now you can install the password manager 1Password. Without interruptions, the installation process can take between 3-5 minutes.

Go back to your 1Password account, click the link "Get the apps". Alternatively, you can access directly from here: https://my.1password.com/apps There you will find links to install the 1Password app in different devices (Windows, Linux, Android, etc.) You can install the app on as many devices as you want to.

When you are done with the installation, don't log in immediately and return to this page.

QI-14 On which of your devices did you install 1Password? (☐ Computer/Laptop (Windows) ☐ Computer/Laptop (macOS) ☐ Computer/Laptop (Linux) ☐ Phone (iOS) ☐ Tablet (iOS) ☐ Phone (Android) ☐ Tablet (Android) ☐ Browser extension (Firefox) ☐ Browser extension (Chrome/Edge/etc.) ☐ Browser extension (Safari) ☐ Other _____)

QI-15 Did the installation on your [device] proceed without a problem? (○ Yes ○ No)

QI-16 (If QI-15 = Yes) What problems did you have for [device]] during the installation? (Free Text)

QI-17 If it was not part of this survey, would you have canceled the installation for [device]?

QI-18 Please upload a screenshot of the successful installation for [device].

Questions QI-15 to QI-18 are repeated for every [device] selected in QI-14

QI-19 How many accounts did you store in the password manager 1Password? (Number)

QI-20 How did you decide which accounts to store?

QI-21 How did you add your accounts to 1Password? How many passwords did you change? (○ Saved my accounts manually ○ Saved my accounts automatically using the import function)

QI-22 Have you changed any of your pre-existing passwords during this process? (○ Yes ○ No)

QI-23 Why did you change your passwords? (Free Text)

QI-24 How many passwords did you change? (Number)

QI-25 How did you create the new passwords? (○ I changed my passwords using the 1Password password generation functionality ○ I changed my passwords by new passwords I generated myself)

Statistics Screenshot

QI-26 Sign in to your account on 1Password.com, then choose a vault where you set up your passwords. Click "Watchtower" in the sidebar to create a Watchtower report and make a screenshot. It should look similar to the image shown below but with your own summary information.

Background

QI-27 What is your gender? (☐ Woman ☐ Man ☐ Non-binary ☐ Prefer not to say) ☐ Prefer to self describe:_____)

QI-28 How old are you? (○ 18-24 ○ 25-34 ○ 35-44 ○ 45-54 ○ 55-64 ○ 65-74 ○ 75 or older ○ Prefer not to say)

QI-29 How well do you understand English? (○ A1 – Beginner ○ A2 – Elementary English ○ B1 – Intermediate English ○ B2 – Upper-Intermediate English ○ C1 – Advanced English ○ C2 – Proficiency English)

QI-Q30 What is the highest degree or level of school you have completed? (○ No graduation (Kein Schulabschluss) ○ Basic School Education (Hauptschulabschluss) ○ Advanced school education (Mittlere Reife) ○ Higher education entrance qualification (Abitur oder Fachabitur) ○ Completed vocational training (abgeschlossene Ausbildung) ○ Bachelor's degree (Universität oder Fachhochschule) ○ Master's degree (Universität oder Fachhochschule) ○ Doctorate (Promotion) ○ Other _____)

QI-31 Which of the following best describes your educational background or job field? (○ I have an education in, or work in, the field of computer science, engineering, or IT. ○ I do not have an education in, or work in, the field of computer science, engineering, or IT. ○ Prefer not to say)

QI-32 How much time do you spend per day on the Internet/PC outside of work? (○ Less than an hour ○ 1-2 hours ○ 3-6 hours ○ More than 6 hours.)

A.2.3 Usage Questionnaire

Likes and Dislikes

Based on your experience using 1Password since the last questionnaire:

QU-1 What did you like about 1Password? (Free Text)

QU-2 What did you dislike about 1Password? (Free Text)

Usage Behavior

QU-3 How often did you use 1Password since the last questionnaire? (○ Daily ○ Almost daily ○ Several times a week ○ Once a week ○Not at all)

QU-4 On which of your devices did you use 1Password since the last questionnaire? (☐ Computer/Laptop (Windows) ☐ Computer/Laptop (macOS) ☐ Computer/Laptop (Linux) ☐ Phone (iOS) ☐ Phone (Android) ☐ Tablet (iOS) ☐ Tablet (Android) ☐ Browser extension (Firefox) ☐ Browser extension (Chrome/Edge/etc.) ☐ Browser extension (Safari) ☐ In the browser (website version))

QU-5 On which of your devices did you use 1Password most frequently? (○ Computer/Laptop (Windows) ○ Computer/Laptop (macOS) ○ Computer/Laptop (Linux) ○ Phone (iOS) ○ Phone (Android) ○ Tablet (iOS) ○ Tablet (Android) ○ Browser extension (Firefox) ○ Browser extension (Chrome/Edge/etc.) ○ Browser extension (Safari) ○ In the browser (website version))

QU-6 You indicated you have 1Password installed on the following devices. When you needed to enter a password on these devices, how often did you use 1Password for this? (○ Never ○ rarely ○ sometimes ○ Most of the time ○ Always ○ I uninstalled on this device)

Usability–SUS

You have indicated that you use 1Password most frequently on your <device in QU-5>. Based on your experience with 1Password on this device up to now, how much do you agree with the statements below?

(Answer choices: ○ Strongly agree ○ Agree ○ Neither agree nor disagree ○ Disagree ○ Strongly disagree)

QU-7 I think that I would like to use this system frequently

QU-8 I found the system unnecessarily complex

QU-9 I thought the system was easy to use

QU-10 I think that I would need the support of a technical person to be able to use this system

QU-11 I found the various functions in this system were well integrated

QU-12 I thought there was too much inconsistency in this system

QU-13 I would imagine that most people would learn to use this system very quickly

QU-14 I found the system very cumbersome to use

QU-15 I felt very confident using the system

QU-16 I needed to learn a lot of things before I could get going with this system

Account type and number

QU-17 For how many accounts did you use 1Password? (number).

QU-18 Which types of accounts did you use 1Password for? (For example social media, e-mails, bank accounts...) (free text).

QU-19 Are there accounts for which you have deliberately not used 1Password despite frequent use? (○ Yes ○ No)

QU-20 Why did you deliberately not use the password manager for some of your accounts? (free text).

Perceived Value

QU-21 Do you see a great added value in using a password manager for your everyday life? (○ Yes ○ No)

QU-22a (If QU-21 = Yes) Which great added value do you see in using a password manager for your everyday life? (free text).

QU-22b (If QU-21 = No) Why do you think that the use of a password manager brings no additional value? (free text).

QU-23 Did you share the subscription with another person this week? (○ Yes ○ No)

QU-24a (If QU-23 = Yes) Who did you share it with? (○ A family member ○ A friend ○ a flat-mate ○ Other, please specify:)

QU-24b (If QU-23 = Yes) What were the main reasons for you to share the subscription with that person? (free text).

QU-24c (If QU-23 = Yes) Did the sharing of the subscription proceed without a problem for you and the person you shared the subscription with? (○ Yes ○ No)

QU-24c1 (If QU24c = No) What problems did you or the person you shared the subscription with have? (free text).

QU-24d (If QU-23 = No) What were the main reasons for you to not share the subscription with another person? (free text).

QU-25 What could be reasons for you to share the subscription with another person? (free text).

Trust

QU-26 Do you trust 1Password? (○ Yes ○ No)

QU-27a (If QU-26 = No) Why do you not trust 1Password? (free text).

QU-27b (If QU-26 = Yes)Why do you trust 1Password? (free text).

Statistics Screenshot

QU-28 : Repeat QI-26

A.2.4 Concluding Questionnaire

Usage Behavior

QC-1: Repeat QU-5

QC-2 After this month using 1Password, approximately how many of your passwords are now created by the password generation functionality. (Slider 0-100%)

QC-3 (If QC-2 <100%) Why did you not use the password generation functionality for all your passwords?

Usability–SUS

QC-9 - QC-13: Repeat QU-7 - QU-16

Statistics Screenshot

QC- 14: Repeat QI-26

Post-Usage Reflections: Perspective Changes

QC-15 Before the survey, did you have any reservations (doubts) against password managers? (○ Yes ○ No)

QC-16 (If QC-15 = Yes) What were these reservations (doubts)? (free text)

QC-17 Do you still feel the same way about password managers? (○ Yes ○ No)

QC-18 (If QC-17 = No) What has changed in your view of password managers? (free text)

QC-19 You indicated that you shared the subscription with other persons.

What are your impressions after having used 1Password and shared the subscription. What are the issues you encountered? What are the benefits you see? (free text)

QC-20 You indicated that you shared your subscription with (<person indicated person in previous questionnaires> . Which other people would you consider sharing a subscription with (if any)? (free text)

Post-Usage Reflections: Intention to Use

QC-21 Will you continue to use 1Password? ○ I will continue to use 1Password ○ I will no longer use 1Password in the future, but will consider using other password managers ○ I will not use password managers in the future ○ I will decide once the trial expires

QC-22 You answered [intention]. What is the most important reason for this decision for you? (free text)

Post-Usage Reflections: Problems, Improvements, Valued Features

QC-23 Were there any problems you had while using 1Password? (free text)

QC-24a (If QC-24 = Yes) What problems did you have while using 1Password? (free text)

QC-25 What concrete suggestions do you have for improving the usability of password managers? (free text)

QC-26 Arrange the features of a password manager that are most important to you. Options: Possibility to share passwords, Automated change of a site's password from within the password manager, Generation of random and complex passwords, Notification of security problems (e.g., Data breaches), Multi-factor authentication to keep your data more secure, Safety analysis and suggestions fro improvement, Synchronization across different devices.

QC-27 Would you recommend the use a password manager to a friend or colleague? (○ Yes ○ No)

QC-28 What are the reasons you think would make them start using a password manager? (free text)

QC-29 Why would you not recommend using a password manager to others? (free text)

Economic Value

QC-30 Would you ever pay for a password manager? (one-time payment) (○ Yes ○ No)

QC-31 How much would you be willing to pay for the password manager? (Enter the amount in euros)

QC-32 What features would the password manager have? (free text)

QC-33 Many third-party password managers require a monthly fee to use their services. Would you be willing to pay for such a service? (○ Yes ○ No)

QC-33a (If QC-33 = Yes) How much would you be willing to pay monthly for such services? (Enter the amount in euros)

QC-33b (If QC-33 = No) Why would you not be willing to pay a monthly fee for the password manager services? (free text)

A.2.5 Follow-Up Questionnaire

QF-1 In the last questionnaire, you have stated that you will continue to use 1Password after the study. Are you currently using 1Password? (○ Yes ○ No)

QF-1a (If QF-1 = No) How and why has your mind changed since the last questionnaire? (free text)

QF-2 In the last questionnaire, you have stated that once the 1Password trial expires in 3 months, you will then decide if you want to continue using 1Password. Is this still true? (○ Yes ○ No)

QF-2a (If QF-2 = No) How and why has your mind changed since the last questionnaire? (free text)

QF-3 In the last questionnaire, you have stated that you will no longer use 1Password in the future, but will consider using another password manager. Are you currently using another password manager? (○ Yes ○ No)

QF-3a (If QF-3 = Yes) Which one?

QF-4 In the last questionnaire, you have stated that you wont be using password managers after the study. Is this still true? (○ Yes ○ No)

QF-4a (If QF-4 = No) How and why has your mind changed since the last questionnaire? (free text)

B Codebooks

- **Reasons to reuse** : • **account-type (23)** *unimportant-account (15), account-with-personal-financial-data(3), important-account (1)*, one-password-per-account-category (4) • **Situational-reason (5)** *password-policy (2), frequently-used-account (3)*
- **Primary password creation:** • **NA(5)** • **convenience (13)** *reused (7), memorable (6)* • **own-algorithm (11)** *reused-variation (6), personal-info-variation (2), unspecified-algorithm (3)* • **security (10)** *random (4), suggested-or-automated (3), unique (3)*
- **Accounts stored:** • **usage (23)** *frequently-used (17), not-frequently-used (3), will-decide-as-they-use-PM (3)* • **importance (13)** • *important-account (8), unimportant-account (5)* • **memory (5)** *memorable-passwords (3), forgettable-passwords (2)* • **no-criteria (4)** *all-accounts (2), randomly-selected (4)*
- **Accounts used (week 3):** • **NA(3)** • **Devices (2)** *router (1), TV (1)* • **specific-services (47)** *social media (16), education (4), online shops (5), entertainment (4), emails (10), forums (1), customer service (1), travels-booking (1), football (1), bank-or-payments-account (3)* • **other (2)** *important (1), every-account (1)*
- **Accounts not used (week 3):** • **NA (5)** • **type-of-account (11)** *bank-accounts (7), important-or-sensitive-accounts (3), email (1)* • **reason (18)** *security-or-trust-concerns (10), can-remember-password (3), no-need (3), wants-to-keep-secret (1), inconvenient (1)*
- **Added value:** • **Convenience (44)** *no-need-to-remember (15), time-saving (6), easy-login (7) efficiency (3), quick-login (11), comfort (2)*, • **Security (16)** *improves-password-strength (10)*, more-secure (6) • **Functionality (8)** *easy-multidevice(1), password-organization (3), password-storage (2), credential audit (2)* • **NA (2)**
- **No added value:** • **usability-issues (16)** *setup-initial-effort (5), extra-steps-to-login (5), difficult-to-understand (1), poor-usability (2), no-time-saving (2)* • **no-perceived-usefulness (26)** *own-strategy-works (18), other-ways-to-store-passwords (7), not useful (1)* • **security-trust-concerns (2)** *security-doubts (1), reliability-doubts (1)* • **practical-management-issues (4)** *many-password-managers (2), managing-primary-password (2)* • **situational-inefficiency (1)** *stored-not-needed-password (1)* • **NA (2)**
- **Trust:** • **general (8)** *feeling-impression (7), no-reason-to-distrust (1)* • **implementation (18)** *well-designed-implemented (8), safe (7), reliable (1), usage-works (2)* • **trust-mechanisms (48)** *trust-in-institution-researchers (22), online-reviews-information (11), serious (6), many-users (3), official-app (3), nothing-bad-happened (2)*, trust-many-other-apps (1) • **NA (4)**
- **No trust:** • **security (9)** *can-be-hacked-or-leaked (4), all-passwords-in-one-place (2) 3rd-party-app (3)* • **information (9)** *lack-of-information (5), transparency (3), bad-online-reviews (1)* • **novice-skepticism (1)**
- **Reasons not to share:** • **skepticism (30)** *not-convinced (8), no need (10)*, bad-experience-dislike (3), no-perceived-usefulness (6), not-using (1), limited-subscription (2) • **security (7)** *security (5), not-wanting-others-accessing-their-passwords (2)* • **acquaintances (37)** *did-not-think-or-come-up (13), no-interested-person (14), acquaintance-use-other-PM (4), takes-time-effort (3), no-common-accounts (3)* • **other (8)** *did-not-know-it-was-possible (7), forgot (1)* • **NA (6)**

C Invitation Email

The following email was sent as invitation to all potential participants in the local *KD²Lab* panel at KIT. It was sent by the panel staff.

Dear [first name] [last name],

we hereby invite you to participate in a KD²Lab study. The study in question is an online study.

Information on the study:
The study has two parts. You can only participate, if you are willing to participate in both parts.

Part 1: You fill out a short questionnaire regarding password managers.

- Duration: 1-2 minutes
- The survey must be filled out today or tomorrow ([DATES]])

During this part, you will also have to provide your bank details to the KD²Lab in order to receive your compensation. Personal data that you submit to KD²Lab for the payout will not be associated with your decisions in the study. To enter your bank data, you will need the following access key: [TOKEN]

Some of the participants will be contacted on the 7th July 2023 to take part in the second part. This second part will start on the 10th July 2023.

Part 2: In case you are selected for the second part, you will have to install the password manager 1Password on one of your devices. The license for 1Password will be provided to you free of charge. You will have to fill out overall six questionnaires in the second part of this study:

1. Monday on the day of installation/setup of 1Password (compensated with 5€)
2. Friday at the end of the first week (compensated with 3€)
3. Friday at the end of the second week (compensated with 3€)
4. Friday at the end of the third week (compensated with 3€)
5. Friday at the end of the fourth week (compensated with 3€)
6. Friday at the end of the twelfth week (compensated with 6€)

Compensation: All participants will receive a guaranteed compensation of 1€ for the first part of the study. Participants who also participate in the second part of the study can get up to additional 23€ (depending on the filled questionnaires as listed above). Compensations are paid out via SEPA bank transfer, see https://www.kd2lab.kit.edu/280.php.

The data protection information can be found at (and also at the beginning of the two parts in the questionnaires): [LINK]

Conditions for participation:

- The study will be conducted in English. Participate in this study only if you have a good knowledge in reading and writing of the English language or if you are a native speaker.
- You must not have used a password manager before this study.
- You must be willing to participate in both parts of the study.
- You own a personal device on which you can install 1Password.
- You are willing to actively use the password manager throughout the study period.

Ready to participate? Please make sure you that you have read and understood the above information on the procedure of this study. You can then start with part 1 of the study:

[LINK]

Please note that participants who fail attention checks or respond to questions in a non-sensical way will not be compensated. The same holds for participants that do not fulfill the conditions for participation.

We are looking forward to your participation!
Best regards
Your KD²Lab Team

D Longitudinal Use of Password Managers

Table 2: How participants used 1Password the most over the course of our study (question: *"On which of your devices did you use 1Password most frequently?"*). Use of browser extensions as a primary means is low, while the Windows and phone applications stand out as often-used.

		Week			
	Type	**1**	**2**	**3**	**4**
		n=33	*n=28*	*n=23*	*n=19*
Browser (Extension)	*Chrome/Edge/etc.*	1	2	2	2
	Firefox	2	3	3	3
	Safari	0	0	0	0
	None / web version	0	0	0	0
Computer/ Laptop	*Linux*	1	1	0	0
	Windows	14	11	10	8
	macOS	1	1	0	0
Phone	*Android*	6	3	3	1
	iOS	7	6	4	5
Tablet	*Android*	0	0	0	0
	iOS	1	1	1	0
Other		0	0	0	0