"I just stopped using one and started using the other": Motivations, Techniques, and Challenges When Switching Password Managers

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

Peter Mayer
University of Southern Denmark
Odense, Denmark
mayer@imada.sdu.dk

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

ABSTRACT

This paper explores what motivates password manager (PM) users in the US to switch from one PM to another, the techniques they employ when switching, and challenges they encounter throughout. Through a screener (n = 412) followed by a main survey (n = 54), we find that browser-based PMs are the most widely used, with most of these users motivated to use the PM due to convenience. Most participants that switch PMs do so for usability reasons, but are also motivated by cost, as third-party PMs' full suite of features often require a subscription fee. Some PM-switchers are also motivated by recent security breaches, such as what was reported at LastPass in the Fall of 2022, with some participants losing trust in LastPass and PMs generally as a result. Those that switch mostly employ manual techniques of moving their passwords, e.g., copying and pasting their credentials from their previous to their new PM, despite most PMs offering ways to automatically transfer credentials in bulk across PMs. Assistance during the switching process is limited, with less than half of participants that switched receiving guidance during the switching process. From these findings, we make recommendations to PMs that can improve their overall user experience and use, including eliciting and acting on regular feedback from users as well as making PM settings more easily reachable and customizable by end-users.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Social aspects of security and privacy**; **Usability in security and privacy**;

KEYWORDS

Passwords, Password Managers, Authentication, Security, Privacy

ACM Reference Format:
Collins W. Munyendo, Peter Mayer, and Adam J. Aviv. 2023. "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 (CCS '23), November 26–30, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3576915.3623150

CCS '23, November 26–30, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0050-7/23/11…$15.00
https://doi.org/10.1145/3576915.3623150

1 INTRODUCTION

Due to the demand of managing numerous online accounts and their credentials [20, 23, 44], password management remains a significant challenge for end-users, leading many to reuse passwords across different accounts [11, 18, 20, 30, 36] rather than creating a unique, strong, and random, password for each account. Ultimately, if one of these accounts is compromised, all other accounts using the same password risk similar compromise [27, 36].

To improve password security, password managers (PMs) have been widely recommended [26]. PMs assist users in creating and recalling unique, strong, and random passwords across accounts while only requiring the user to remember the vault password of the PM. There have been several studies investigating how and why users adopt PMs or choose not to [32, 39, 40]. A large motivator is both the convenience of saving and recalling passwords. However, the hurdle of adding all passwords to the PM can feel daunting for many adoptors [5], particularly for the less tech-savvy users [40]. There also remain usability challenges with PMs not "playing nice" with many websites [24], leaving some users frustrated.

Despite these challenges, many users have adopted a PM [32]. However, little is known about how and why users may transition from one PM to another. Such transitions could be critical for both security and usage of PMs. For example, prior work suggests that those using a third-party PM, like LastPass or 1Password, are less likely to reuse their passwords across accounts compared to those using browser-based PMs [32]. Transparency and security perceptions of PMs are also influential in the adoption and use of PMs [32]; therefore, the recent security breach involving LastPass could have far-reaching implications on users' attitudes towards PMs, and decisions to continue using PMs (or not). Further, if users' motives for switching are not addressed by their new PM or are frustrated by the switching process, they may abandon PMs.

In this study, we thus investigate the motivations for switching (or not switching) PMs, the techniques used in that process, and challenges encountered by posing the following research questions:

RQ1: What password managers (PMs) do users most commonly use, and what PM aspects do they like and dislike?

RQ2: Why do users switch password managers? What factors influence switching PMs?

RQ3: Is the process of switching password managers easy or hard? What are the sources of guidance?

RQ4: What are users' awareness, perceptions, and reactions to password manager breaches?

To answer our research questions, we conducted two online surveys with PM users in the US, a screener (n = 412) followed by a main survey (n = 54) with participants that had switched PMs. In

the screener, we asked participants about the PM(s) they use, their security and usability perceptions regarding their most-used PM and overall satisfaction using the PM. Participants that indicated switching PMs in the screener were immediately invited to the main survey where we asked them to indicate the PM they had switched from, techniques used to switch, challenges encountered, and advice sources and guidance during the switching process. We additionally asked participants about their awareness, perceptions, and reactions to the recent LastPass security breach.

Our key findings are summarized as follows:

- *Browser-based PMs are the most widely used due to convenience.* Our results indicate that browser-based PMs are the most widely used, matching inquiries from a prior study that focused on a private, educational institution in the US [32]. Most participants use PMs due to the convenience of not having to remember their passwords and not because of security, similar to previous work [5, 32]. Unfortunately, password re-use remains persistent even among PM users, with PMs' password generators not often used by users [38].
- *Most participants switch PMs for usability reasons.* When asked for their main motivation for switching PMs, most participants pointed to usability issues with their PMs. However, several participants also switched due to their PMs encountering breaches or charging subscription fees. We also find that participants that use browser-based or system-provided PMs were significantly less likely to switch PMs compared to third-party PM users.
- *Participants struggle when switching PMs because they mostly employ manual techniques when switching.* Most participants indicated using manual techniques when switching PMs e.g. copying and pasting their logins from their previous to new PM despite the fact that most PMs allow automatic export and import of logins. Most participants further indicated that switching manually was the most challenging part of the transition. At the same time, most participants did not use any guides when switching, suggesting opportunities for more guidance and support for those switching.
- *Most participants are aware of the recent LastPass breach and seem to lose trust in LastPass and PMs generally as a result.* A majority of participants were aware about the recent security breach of LastPass, with most participants concerned about the security of passwords currently stored in LastPass as well as how the incident was handled by LastPass. Some participants particularly indicated losing trust in LastPass and PMs generally as a result, with some stating that they would even discourage others from using LastPass.

Based on these findings, we make recommendations to PMs that can improve their overall user experience, adoption, and usage. For instance, we encourage PMs to regularly elicit and act on user feedback as well as make their settings more easily reachable and customizable by end-users. We additionally recommend transparency when handling and communicating about breaches to maintain trust which is critical in the adoption and use of security tools such as password managers.

2 BACKGROUND

2.1 Password Managers

Password managers (PMs) are applications that allow users to generate, store, and recall passwords for online accounts. PMs solve an important security problem with managing multiple online accounts; users need to generate and remember secure, strong, and unique passwords for each account. Such a task is nearly impossible without a PM, where, if used properly, the PM generates, stores and recalls passwords, which are then secured with a single vault password. The user can then invest in generating a strong vault password, instead of having to do so across different accounts.

There are multiple types of PMs, and similar to previous work [32, 39, 40], we categorize PMs into three broad categories:

- *Operating System built-in PMs:* These are password managers that are integrated or built into the operating system for example Keychain on Apple devices. These PMs do not require users to download or install any additional software beyond what's offered by the operating system.
- *Browser built-in PMs:* These PMs are typically offered as part of browsers' functionality. For example, common browsers such as Firefox and Chrome have built-in PMs that prompt users to both generate as well as save passwords across sites.
- *Third-party PMs:* These are dedicated software for password management that typically require users to install an application or a browser extension. Examples of third-party PMs include LastPass and 1Password.

Previous studies [24, 32, 39, 40] have investigated factors that drive or hinder the adoption of PMs, finding that convenience of PMs, essentially not having to remember and fill-in passwords, most influences their adoption. Poor usability (or even a perception of poor usability), in contrast, hinder their adoption [24]. Further, users of third-party PMs have been shown to exhibit secure password behavior compared to users of browser-based PMs [32]. However, what might motivate a user to switch from one PM to another and the process they take to do so is unexplored. This is in spite of the likelihood that the switching process may either improve users' password security, or frustrate them and lead them away from using PMs altogether. Our study, therefore, has direct implications on improving both the design and adoption of password managers.

2.2 LastPass Security Breach

In the Fall of 2022, LastPass published a series of blog posts and sent out emails informing their customers of a security incident involving LastPass [46]. In the first notification sent out on August 25, 2022, LastPass indicated that they had detected unusual activity in their development environment, but ruled out any potential access to customer data or their encrypted password vaults by unauthorized parties. However, in subsequent alerts, particularly on December 22, 2022, LastPass admitted that the unauthorized party had in fact gained access to their production environment by stealing credentials from an employee, and copied customer vault data containing customer account information and metadata, as well as encrypted fields including website usernames and passwords, secure notes, and form-filled data. However, LastPass maintained that these encrypted fields could not be decrypted without the unique

encryption key derived from each user's vault password, and thus advised its customers to follow password best practices, including using a strong vault password to minimize any potential risks of unauthorized access to their accounts. In this study, we seek to explore users' awareness, perceptions, and reactions to this breach.

3 RELATED WORK

3.1 Password Manager Adoption and Use

Many factors have been investigated regarding their influence on password manager (PM) adoption and usage. While the results for some of these factors were inconclusive [8], several factors have been found to foster PM adoption, namely perceived usefulness [1, 13, 31], ease of use [1, 16, 19, 32, 39], trustworthiness [19], subjective norms [1], learnability [14], and the three self-determination theory factors, i.e., autonomy, competence, and relatedness [2]. Some studies also investigated adoption factors of special populations. Specifically, Ray et al. [40] investigated factors influencing adoption of PMs for older adults. Their findings highlight the differences these demographic factors can make. For instance, older adults exhibit a higher mistrust in cloud storage of passwords, and they are afraid of the PM becoming a single point of failure. At the same time, it has been found that security concerns [16, 32, 39], insufficient time for users [7], a low perceived threat [7], a lack of immediacy [7], and a feeling of relinquishing control [15] act as barriers to the adoption of PMs. Yet, even if users adopt a PM, it does not mean they will use it to its full potential. Lyastani et al. [30] showed that a substantial number of PM users still use weak passwords and that – especially among users of the Chrome browser built-in PM who use auto-fill – password reuse was a common practice, a theme we similarly observe in our study.

Expanding on the works described above, we present – to our knowledge – the first study investigating users' reasons for switching from one PM to another, the techniques they use as well as challenges they encounter throughout the process.

3.2 Usability of Password Managers

As previously indicated, ease of use has been identified as a key factor fostering PM adoption. Consequently, multiple studies have investigated the usability of password managers (PMs). Chiasson and van Oorschot [15] presented one of the earliest usability studies of two PMs for desktop computers. They find that both PMs have major usability problems and that misaligned mental models about PMs are one of the key issues causing usability problems. The recent work of Seiler-Hwang et al. [42] confirms the prevalence of the themes identified 13 years earlier by Chiasson and van Oorschot. In their analysis of the usability of four smartphone password managers, they find that usability problems are still prevalent with System Usability Scale scores ranging from only 52.6 to 76.5.

In particular, auto-fill has been identified as a feature users like about PMs, also confirmed in our study. Consequently, several proposals have been made to increase the compatibility between websites and PMs. Stajano et al.'s [43] Password-Manager Friendly approach aims to help PMs identify relevant fields and error messages on websites through additional markup in the websites' code. Another approach by Gautam et al. [21] focuses on password generators included in PMs and their ability to create passwords that will conform to websites' password composition policies.

McCarney et al. [35] investigated the usability benefits of an alternative PM implementation that foregoes traditional vault passwords and instead requires two devices, e.g., a desktop computer and a smartphone. Their evaluation found their implementation of this alternative to be preferred over the browser built-in password manager of Firefox. However, such an implementation is yet to see adoption in practice.

Our work complements the body of research on the usability of password managers by identifying usability challenges that lead users to switch from one PM to another. Additionally, we are the first to identify — to our knowledge — usability issues of the switching process itself as well as guides that users rely on when switching.

3.3 Security of Password Managers

In comparison to other authentication technologies, PMs have been found to inherently lack resilience to internal observation [10], i.e., malware on the user's devices can steal all password data. Moreover, Li et al. [29] investigated the security of web-based PMs and found that several of the PMs they looked at can leak arbitrary credentials to an attacker. A recent re-visit to these attacks by Oesh et al. [37] in 2020 showed that many of these issues persist, particularly the usage of unencrypted metadata, insecure defaults, as well as vulnerabilities to click-jacking attacks.

Beyond the susceptibility of password managers to attacks, researchers have proposed additional defenses strengthening the security of the password vaults from different attacker models. Several more generic approaches can be applied to protect PM accounts and vaults. Juels and Ristenpart [28] propose Honey Encryption as a means to hide encrypted data by generating decoy plaintext when the data is decrypted using an incorrect key. In a similar proposal, Almeshekah et al. [3] propose a honey-pot approach based on physically unclonable functions or hardware security modules to prevent access to users' accounts. These approaches could be applied to protect accounts that users have with PM companies and the PM vaults. In work more focused on PM vaults directly, Bojinov et al. [9] proposed Kamouflage, an approach generating a large number of decoy vaults for each user so that even in case an attacker gets access to the vault password, they do not know which vault is the correct one. Combining the Honey Encryption and Kamouflage approaches, Chatterjee et al. [12] propose to use a natural language encoder to create decoy vaults on the fly, greatly improving storage efficiency of the Kamouflage approach. Golla et al. [22] improve on the approach by Chatterjee et al. by adapting the natural language encoder to be based on Markov models which greatly improves their resistance to attacks trying to identify decoy vaults based on the passwords they hold.

3.4 Passwords and Security Breaches

As discussed in section 3.1, a feeling of relinquishing control of data to the PM can be a barrier to PM adoption. The recent security breaches affecting Lastpass [46] show how relevant these concerns are. If access to all passwords in a PM vault is lost, this can be a data breach with severe consequences, such as identity theft. Identity

theft can be a traumatising experience leading to bankruptcy [6] or even inciting suicidal thoughts [25].

Of particular importance regarding data breaches involving a PM vault, is whether users change affected passwords as a response to the breach. In their investigation of individuals' reaction to data breaches, Mayer et al. [33] found that 69.7% of participants were somewhat likely or very likely to change the password of the account affected by the breach and 68.1% of participants were somewhat likely or very likely to change the password of other accounts protected by the same password. However, despite the participants' comparatively high concern when passwords leaked as part of a data breach, the authors found that only 34.4% of participants had followed through on changing the password of the affected account and 34.5% of participants had followed through on changing passwords of different accounts after six months.

Our work complements these results by providing additional insights on PM-specific data breaches by investigating the awareness, perceptions, and reactions to the LastPass data breach. We find that breaches reduce users' trust in affected PMs, and in PMs generally. Similar to usability issues, breaches can also severly undermine the adoption of password managers.

4 METHODS

To understand why and how users switch from one password manager (PM) to another as well as the factors that influence switching, we first conducted a screener survey (n = 412) with password manager users. In the screener, we asked participants if they switched PMs, and if so they were invited back to the main survey (n = 54) where they answered more questions about that experience. In this section, we describe the structure of the two surveys, followed by recruitment and our analysis of the data. Afterward, we detail the limitations as well as ethical considerations of the study.

4.1 Screener

We recruited n = 412 participants who reside in the US for the screener survey to answer questions about their current password manager. We broadly informed participants that the screener would explore their usage and behavior with password managers and purposefully did not mention anything about switching PMs to avoid bias and priming for those recruited to the main survey.

In the screener survey, we first described password managers using the PM explanatory text from Pearman et al. [39] before asking participants whether they use a PM (**P1**). Following, we asked participants to indicate all types of PMs they use (**P2**) and the one they most frequently use (**P3**), if multiple types were selected. Afterward, we asked participants to indicate their satisfaction as well as the one thing they like the most and the one thing they dislike the most about their most frequently used PM (**P4** - **P6**).

Similar to previous work [32], we then asked questions relating to security and usability aspects of PMs (**P7**) by adapting Colnago et al.'s [17] questions that were used to study the adoption of 2-factor authentication at an institution as follows: (a) *security*: whether participants believe using PMs will prevent their accounts from getting compromised; (b) *tranquility*: whether participants believe that using PMs means that they do not have to worry about the safety of their accounts; (c) *fun*: whether participants believe that PMs are fun to use; (d) *ease of use*: whether participants believe that PMs are easy to use; (e) *difficulty of use*: whether participants believe that PMs are difficult to use. (f) *annoyance*: whether participants believe that PMs are annoying to use. We additionally included *trust* and *transparency*, similar to previous work [4, 32]: (g) *trust*: whether participants trust PMs; (h) *transparency*: whether participants believe they understand how PMs work. Lastly, we asked participants if they had ever switched from a different PM to their current PM (**P8**), followed by their demographics including age, gender, level of education and IT background (**D1** - **D4**). The full survey is available in Section A of the Appendix.

4.2 Main Survey

Participants that completed the screener and indicated they had switched from a different PM to their current PM were invited to take part in the main survey. Fifty-four out of 65 participants that indicated they had switched PMs successfully completed the main survey. In this survey, we once again asked participants to restate their current PM(s) as well as the one(s) they were previously using (**Q1** - **Q4**). We then asked them to indicate when they switched (**Q5**), their motivation for switching (**Q6**) and overall satisfaction with their previous password manager (**Q7**). We then asked them about one thing they liked the most (**Q8**) and one thing they liked the least (**Q9**) about their previous password manager, focusing on the one they frequently used if they selected multiple.

Similarly to the screener, we asked questions relating to security and usability aspects [17, 32] of participants' previous password manager (**Q10**). Afterward, we inquired about their password selection first using their previous PM (**Q11** - **Q12**), and then with their current PM (**Q13** - **Q14**). We then asked about how they transitioned including any challenges and sources of guidance throughout the process (**Q15** - **Q28**). Lastly, we asked general questions regarding PMs including where participants first heard about PMs and password reuse (**Q29** - **Q31**) followed by questions regarding the LastPass breach including awareness and perceptions about the breach as well as willingness to continue using LastPass (**Q32** - **Q42**). The full survey is available in Section B of the Appendix.

4.3 Recruitment and Demographics

We recruited participants through Prolific, an online crowd recruitment platform for research participants. For the screener, all participants were required to be at least 18 years old, residing in the US and currently using a PM. To be eligible for the subsequent main study, participants were required to have switched a password manager. All data collection across both surveys took place between late March and early April, 2023. After excluding 27 responses from the screener and two from the main study due to inconsistent responses or not using a password manager, we recruited n = 412 and n = 54 participants for the screener and main survey respectively. Participants were compensated $1.25 for completing the screener which took on average 3.7 minutes, and $3.75 for completing the main survey which took 12.4 minutes on average.

Across both surveys, participants were mostly young (aged between 18 - 34 years), well-educated (a majority had a Bachelor's degree) but did not have an information technology or computer science background. While we had a roughly even split between

Table 1: Participants' demographics across both surveys.

		Screener	Main Survey
Gender	Female	202	17
	Male	201	35
	Non-binary	7	2
	Prefer to self-describe	1	0
	Prefer not to say	1	0
Age	18 - 24	93	12
	25 - 29	80	10
	30 - 34	84	10
	35 - 39	62	9
	40 - 44	38	6
	45 - 49	18	2
	50 - 54	12	1
	55 - 59	7	1
	60 - 64	12	2
	65+	6	1
Education	High School or equiv.	43	1
	College or Trade	82	11
	Associate's degree	40	7
	Bachelor's degree	176	27
	Master's degree	57	6
	Professional	9	1
	Doctorate	5	1
Background	IT/CS Background	95	21
	Non-IT/CS Background	307	31
	Prefer not to say	10	2

male and female participants in the screener, a majority of those that participated in the main study were male. Table 1 has the full demographic information of participants across both surveys.

4.4 Data Analysis

For the open-response questions across the two surveys, we performed analysis using open-coding techniques based on inductive coding [41, 45]. One researcher independently coded the two open-response questions in the screener as well as the 18 open-response questions in the main survey to develop a primary codebook. To verify the consistency of the codebook, a secondary coder applied this codebook to a random set of 30% of responses in the screener, and all the questions in the main survey before Cohen's κ was calculated. Throughout this process, the researchers met to resolve coding differences and update the codebook if agreement was low. It took, on average, 1.4 rounds across all the questions to reach $\kappa \geq 0.7$ (average $\kappa = 0.84$), indicating strong agreement. Note, the same response could be assigned multiple codes.

To investigate factors that influence users to switch from their previous PM, we ran a logistic ordinal regression. As factors, we included security and usability aspects of users' previous PMs (for those that switched) and current PMs (for those that had not switched) from Colnago et al [17] namely *security, tranquility, fun, ease of use, difficulty of use,* and *annoyance.* Users' Likert responses to these factors were binned to agree (strongly agree, somewhat agree, neither agree nor disagree) and disagree (strongly disagree, somewhat disagree). We also included users' demographics, binning age into those between 18-29 versus over 29, IT/CS background versus no IT/CS background, and male versus female (there were only a few samples of non-binary or prefer to self-describe, and were therefore dropped). We also dropped all responses that were "prefer not to say" for any of the factors as well as participants that were unsure about switching PMs. Lastly, we included the type of previous PM participants were using, binning them into browser-based and operating system built-in PMs versus third-party PMs.

4.5 Limitations

Our study has several limitations. Foremost, as this was an online survey, it is not possible to tell if participants were honest and accurately followed all our instructions throughout. However, we reviewed all open and closed responses and excluded inconsistent responses from our analysis, notably 27 from the screener and two from the main survey. Despite our best efforts running as many screeners as possible, only 65 participants indicated they had switched password managers, with 54 proceeding to participate in the main study. Further, our sample size was relatively young and more educated than the average US population. We do not claim our results to be representative of the US, but argue they capture common reasons why people switch password managers as well as challenges they typically encounter in the process. Our results regarding the most commonly-used PMs as well as challenges using them are also consistent with previous work [32, 39].

4.6 Ethical Considerations

This study was reviewed and approved by our Institutional Review Board (IRB). We fully informed participants about the purpose, duration, and associated risks of taking part. We additionally informed participants that they were free to withdraw from the study at any time prior to submitting the survey without any consequences.

5 RESULTS

Our results are structured around the four research questions outlined in Section 1. We first discuss common PMs from the screener (n = 412), followed by factors and motivations for switching PMs from the main survey (n = 54). We then discuss the techniques and challenges that participants encountered throughout the process of switching PMs before finally discussing their awareness, perceptions, and reactions to the LastPass security breach. We use *S001 — S412* when presenting quotes from the screening survey, and *M01 — M54* for quotes from the main survey. We report our qualitative findings using counts to avoid over-generalizing.

5.1 Common PMs and Password Management

Common PMs used by participants. Through our screening survey (n = 412) with PM users in the US, we find that browser-based PMs are by far the most commonly-used type of password managers, with 82.5 % of participants using browser-based PMs to manage their passwords (see Figure 1). System-based and third-party PMs, in contrast, were used by only 38.1 % and 32.5 % of participants respectively, with a majority of system-based PM users using Apple's Keychain. Our results confirm those of a recent study by Mayer et al. [32] that found browser-based PMs to be the most common PMs at a large, private, educational institution in the US.

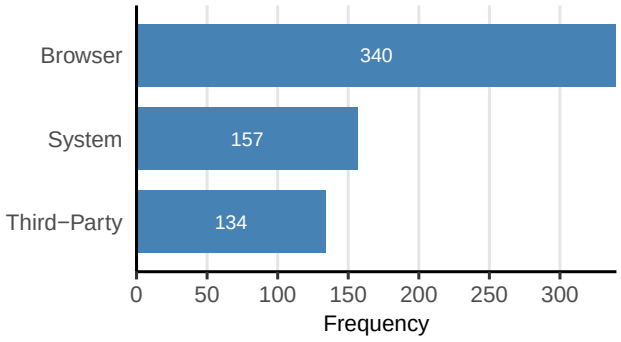

Figure 1: PM types used by participants in the screener (n = 412). Note, participants could select all PM types that apply.

For the specific password manager, Chrome[1] was by far the most commonly-used PM (see Figure 2). In the screener (n = 412), 70.6 % of participants stated using it followed by Apple's Keychain (38.1 %), FireFox (15.8 %) and LastPass (12.6 %). The widespread usage of Chrome and Keychain PMs can be attributed to the popularity of the Chrome browser and Apple devices respectively in the US. While these results are closely similar to Mayer et al.'s [32] findings at their institution-wide study, we additionally find that Bitwarden is emerging as a common third-party PM alternative [5], with 8.0 % of participants indicating they use it; no participant reported using Bitwarden in Mayer et al.'s study. Further, as we show later in Section 5.2, Bitwarden is the PM most participants switched to.

PM aspects that participants like. In the screener (n = 412), we asked participants to indicate one thing they like the most about their PM as an open-response question (**P5**). We find that most participants appreciate that PMs save passwords for them (91), are easy to use (87), synchronize across multiple devices (64), and are convenient (55). For example, S91 pointed to "*the fact that it can save new passwords and auto-fill them for websites*" while S252 added that their PM is"*easy to use and convenient.*" Other themes described by at least 20 participants include that PM's auto-fill (39), provide security (27), prompt to save their credentials (26), and generate passwords (24). For instance, S346 said that "*I like that when I go to a website that I'm not signed into, it auto-fills all my information so that all I have to do is click "Log In" and not type out everything.*" The strength of these themes suggest that participants more highly appreciate conveniences rather than security properties of PMs.

PM aspects that participants dislike. In the screener (n = 412), we asked participants to indicate one thing they dislike the most about their PM as an open-response question (**P6**), with most participants (70) indicating they did not dislike anything about their PM. However, 32 participants were worried about PMs being insecure, e.g., because other people might access their passwords if they access their devices. S229, for instance, said "*having my passwords saved onto my phone isn't necessarily the most secure option out there.*" Twenty four participants complained about PMs sometimes failing

[1]Starting in December 2022, Google started to re-brand the Chrome PM as Google Password Manager. In this study, we refer to both generally as the Chrome PM.

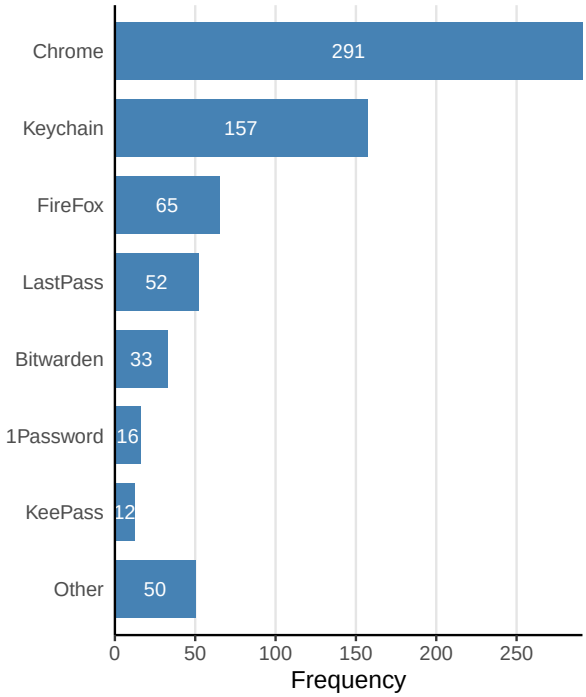

Figure 2: Common PMs used by participants in the screener (n = 412). Note, participants could select all PMs that apply.

to save their credentials while a further 24 were frustrated with usability issues. For example, S401 complained:

> "*I wish that whenever I made a password it'd save automatically. As there are times when looking up a password for one site only to find out there is no password saved. In which I have to reset the password in order to log in and then save that password.*"

Other themes described by at least 20 participants include PMs sometimes failing to work (22) as expected and PMs failing to sometimes update user credentials when they make changes (22) to them. For instance, S300 complained that "*it doesn't always work. Sometimes, answering security questions triggers my password saver to ask if I want to update my password. I hate when it makes an ultra complicated password and then doesn't save it.*"

Reasons for using PMs. When asked for their main reason(s) for using a password manager as a closed-item response (**Q30**) in the main survey (n = 54), most participants (46) indicated using PMs for convenience, followed by security (37), memory limitations (22), and prompts from the browser (12). Similar to Mayer et al. [32], the convenience of not having to remember passwords seems to be a common reason for using PMs, perhaps more than security. This result can inform campaigns seeking to encourage the adoption of PMs by focusing more on their convenience benefits.

Awareness about password managers. In the main survey (n = 54), we asked participants to indicate where they had first heard about

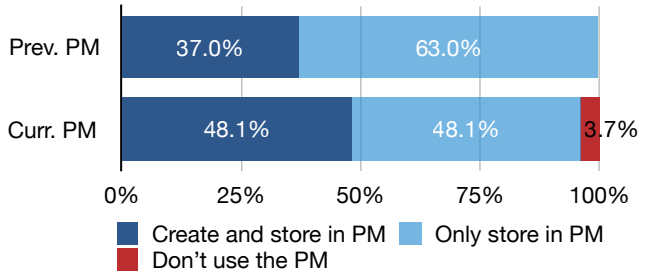

Figure 3: Password generation for important accounts in the main survey (n = 54) using previous and current PMs. Participants could only select 1 option for each of the PMs.

PMs as a closed-item response (**Q29**), with a majority of participants (24) indicating they had first heard about PMs via the media. Ten participants said they do not know or remember, while eight indicated hearing about PMs from other people. In contrast, Mayer et al. [32] found that most of their participants at a private US university did not remember where they had first heard about PMs, followed by hearing from other people and then the media.

Password generation. In the main survey (n = 54), we asked participants how they generate passwords for important accounts as a closed-item response, both with their current (**Q13**) and previous PM (**Q11**). Across both PMs, less than half of participants indicated using the PM to both generate and store passwords for their important accounts (see Figure 3). Surprisingly, two participants indicated they create and recall important passwords away from their current PM, with one of these participants specifically indicating they avoid PMs due to the recent breach that affected LastPass. Nevertheless, we find that PM's password generation features are under-utilized, likely leading to password re-use as we discuss next.

Password re-use. In the main survey (n = 54), we asked participants whether they re-use any of their passwords across accounts (**Q31**), finding that a majority of participants (29) reuse their passwords compared to those that do not (24). One participant was unsure. For those that re-use passwords, 11 use a browser-based PM, 11 use a third-party PM, while 7 use a system-provided PM, i.e., Apple's Keychain. For those that do not re-use, however, 15 use a third-party PM while 9 use a browser-based PM. Thus, slightly more third-party PM users compared to browser-based PM users do not re-use their passwords. In their study, Mayer et al. [32] found password re-use to be more pronounced among browser-based PM users compared to third-party PM users. This may be due to the fact that a majority of third-party PM users are motivated to use the PM because of security compared to users of browser-based PMs who are mostly motivated by convenience.

RQ1 Summary. Our results about common types of password managers as well as password habits with participants from the US confirm those of a recent study by Mayer et al. [32] that only focused on an institution-wide setting. We confirm that browser-based PMs are the most commonly-used type of PMs and that most users use PMs due to convenience rather than security. However, password re-use remains persistent, even among PM users, with most participants not utilizing PMs' password generators when creating passwords.

5.2 Motivations and Factors for PM Switching

Password managers that participants switched from and to. Out of the participants that switched PMs in the main survey (n = 54), a majority switched away from LastPass (22), followed by Chrome (11), and FireFox (8). On the other hand, most participants switched to Bitwarden (19), followed by Chrome (16), and Apple's Keychain (7). This is summarized in Figure 4. Most participants that switched away from LastPass did so before the LastPass security breach for various reasons which we discuss below, with only six participants switching from LastPass specifically because of the breach.

Motivations for switching PMs. In the main survey (n = 54), we asked participants to describe their motivations for switching PMs as an open-response question (**Q6**). Most participants (17) indicated switching for usability reasons. For instance, M33 pointed to the "*ease of use and functionality across devices*" of their new PM while M46 added that their new PM "*was just easier to use, seamless.*" The next most mentioned reason for switching was because of data breaches (10), mostly surrounding LastPass but also other PMs. For instance, M03 described how they lost trust in LastPass after their recent security breach:

> *"LastPass experienced a major breach of their data, including vaults and decryption information, after storing such information in Amazon Web Services. I thought they were storing it on servers they owned and controlled, were actively monitoring for threats, and were transparent about problems. Turns out, they claim they didn't know the extent of the breach which implies they weren't actively monitoring for threats, the servers were not onsite and fully under LastPass's control, and they downplayed the extent and severity of the breach and delayed informing customers about the breach at all."*

M38 similarly switched away from Chrome for the same reasons:

> *"I lost acess [sic] to my work chrome account and it was breached. This made me lose faith in my personal account protection and opted to switch to a different password manager."*

The next most mentioned reason for switching was because of previous password managers requiring a subscription fee (9). M12 indicated that *"LastPass used to be free and then they started charging"* while M26 was unhappy that some features of their previous PM required subscription: *"There were some features, such as cross platform access, that were locked behind a paywall."* M50 switched from LastPass because of a combination of the data breach they experienced and subscription fee that they started charging:

> *"There had been one or more security breaches related to LastPass, AND they started charging a fee around the same time. I didn't want to pay for a service that I wasn't very happy with."*

Other common reasons for switching password managers that were mentioned by more than one participant include convenience offered by the new PM (5), the need for more functionality (5), change of browsers (5), better auto-fill functionality offered by the

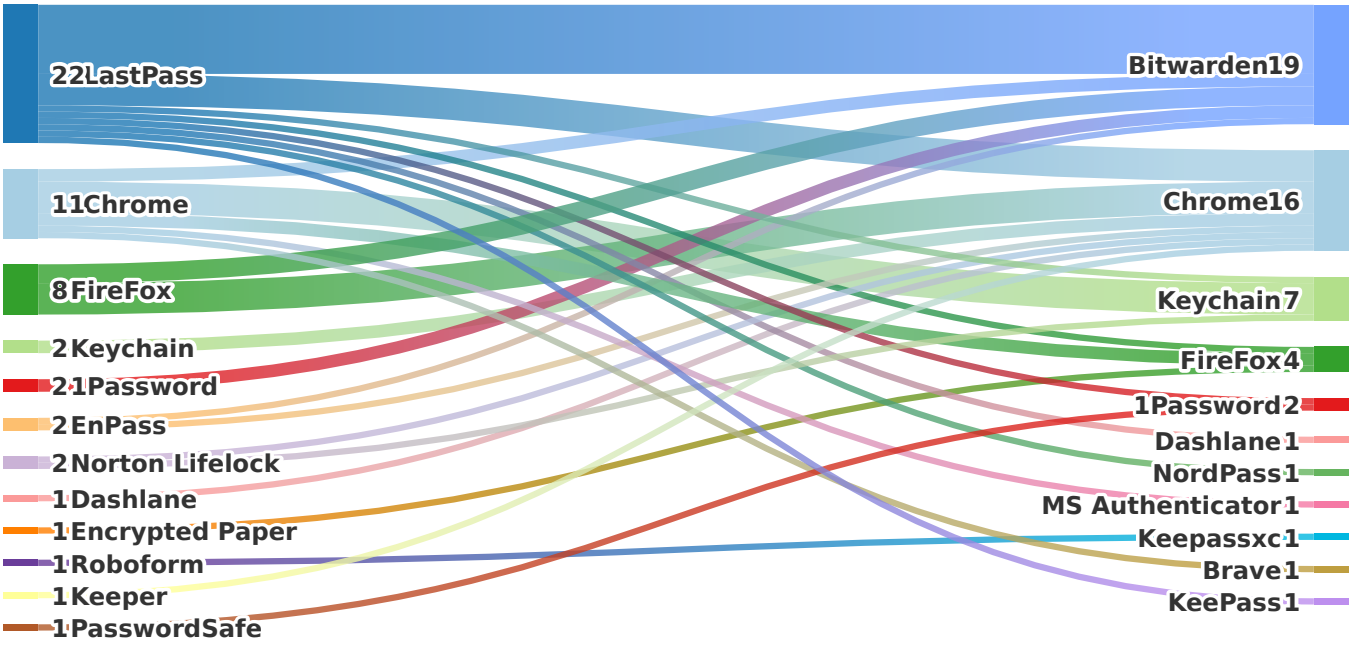

Figure 4: The password managers that participants indicated switching from and to in the main survey (n = 54).

new PM (3), a need for a PM that is open-source (3), change of operating systems (3), and security concerns (3).

Factors that influence switching of password managers. To understand the factors that influence users to either switch (or not) from their previous PM to a new one, we conducted a logistic regression. As factors, we included participants' perceptions of the security and usability of PMs (see Section 4.1) i.e. *security, tranquility, fun, ease of use, difficulty of use,* and *annoyance*, as well as *trust* and *transparency*. We also included participants' demographics i.e. age, gender, education level, and IT or CS background. Unfortunately, since only a few participants identified as non-binary for gender or "preferred not to answer" for other factors, we dropped these responses from our regression analysis. We also dropped responses from participants that were unsure about switching PMs. Lastly, we included the type of password manager participants were previously using, and their overall satisfaction with it. Note, for participants that did not switch, we used their responses to their current PM while for those that switched, we used their responses to their previous PM. In total, we had n = 366 responses for our regression analysis.

Out of the 14 factors that we considered for the regression, we found that only the type of previous PM that participants were using was significant ($OR_{\text{PM Type}}$ = 3.45, p = .001). Participants were 3.45× less likely to switch from browser-based or system-provided PMs compared to third-party PMs. This is likely because browser-based and system-based PM users are motivated by convenience, and thus perceive switching as an inconvenience compared to third-party PM users who are motivated by security, and are thus more likely to accept the inconvenience of switching to more secure password manager options.

RQ2 Summary. Overall, we find that most participants switch away from their previous PM for usability reasons, either because of usability issues with their previous PM or because of better usability offered by the new PM. Several participants also switch away from PMs due to data breaches e.g., what was reported at Lastpass, as well as subscription fees. At the same time, we find that users of browser-based or system-provided PMs are less likely to switch PMs compared to third-party PM users.

5.3 Techniques and Challenges When Switching

Techniques for switching PMs. In the main survey (n = 54), we asked participants to describe how they transitioned from their previous PM to their current PM (**Q15**). A majority of participants (24) indicated transitioning manually either by copying their usernames and passwords from their previous PM to their current PM one at a time, typing or manually entering them, or transitioning gradually. This is despite the fact that most PMs allow users to export their credentials, and import them into a new PM. For instance, M19 said that they "*manually copied them*" while M47 "*manually typed them.*" M07 *"didn't use any methods, I just gradually migrated my passwords and logins onto the new password manager as I encountered different passwords."* M35 "*didn't really transition. I just stopped using one and started using the other, entering passwords manually as needed."* Some of the participants that manually transitioned indicated that they chose to do so since they had to update all their passwords, for example due to a breach to their previous PM. M31, for instance, stated that they "*personally decided to manually transfer them over to NordPass. Since LastPass had a data breach, I was determined to change every single password I had.*" M05, on the other hand, "*did*

Table 2: Logistic regression for participants switching from their previous PM. Significant factors are marked in bold Italics and with an asterisk (*) while those trending towards significance are marked with Italics and a dot (.)

	Est.	OR (+)	OR (-)	95% CI	p-val
(Intercept)	1.98	7.26	0.14	[0.61, 86.29]	.116
Security: Agree (vs Disagree)	*-1.02*	*0.36*	*2.78*	*[0.12, 1.05]*	*.062* •
Tranquility: Agree (vs Disagree)	0.27	1.31	0.76	[0.50, 3.42]	.586
Fun: Agree (vs Disagree)	−0.05	0.95	1.05	[0.45, 2.02]	.900
Ease of Use: Agree (vs Disagree)	*-1.86*	*0.15*	*6.67*	*[0.02, 1.06]*	*.058* •
Difficulty: Agree (vs Disagree)	−0.72	0.49	2.04	[0.12, 1.94]	.308
Annoyance: Agree (vs Disagree)	0.23	1.25	0.80	[0.60, 2.61]	.544
Transparency: Agree (vs Disagree)	0.01	0.99	1.01	[0.36, 2.74]	.989
Trust: Agree (vs Disagree)	−0.08	0.92	1.09	[0.35, 2.41]	.869
Age: 18 - 29 (vs Over 29)	−0.07	0.93	1.08	[0.49, 1.77]	.825
Gender: Male (vs Female)	0.52	1.68	0.60	[0.87, 3.24]	.123
Education: >= Bach. (vs No Bachelors)	0.13	1.14	0.88	[0.59, 2.17]	.700
IT/CS Backgr.: Yes (vs No)	*0.68*	*1.97*	*0.51*	*[0.99, 3.93]*	*.054* •
PM Type: Brow/Sys. (vs Third-Party)	***-1.23***	***0.29***	***3.45***	***[0.14, 0.59]***	***.001*** ⋆⋆⋆
Satisfaction: Satisfied (vs Unsatisfied)	*-1.02*	*0.36*	*2.78*	*[0.13, 1.01]*	*.052* •

not realize at the time of switching that I could export my passwords, so I just manually entered each one of them.

The next most mentioned strategies for switching PMs were exporting (20) usernames and passwords from the previous PM, and subsequently importing (15) them into the new PM. For instance, M03 stated that they "*exported my vault in .csv form, stripped off unnecessary data in Google sheets, then uploaded the remaining data into Google Password Manager.*" Similarly, M22 indicated that in "*LastPass, I downloaded the .csv file that contained all my account information and then uploaded it to Bitwarden when I created/setup my account. Then I made sure I nuked that file as best I could.*" Some participants such as M54 used a combination of exporting their credentials and manually entering some of them: "*I did a combination of exporting and manually typing them in. I usually remember my credentials so it wasn't hard for me to just type them in again.*"

Five participants indicated that they did not or were unable to transition for various reasons. For example, M13 could not transition because they forgot the vault password to their previous PM: "*I was not able to transition my passwords because I lost the master password for LastPass.*" M39 indicated that "*given I largely used it at a former job, I didn't have [the] need to transfer many of the credentials. Those that I did need to transfer, I did manually.*" Two participants just started to use their new PM (2) while three mentioned they did not exactly remember how they transitioned.

Easiest parts of the switching process. When asked about the easiest part of switching PMs (**Q24**) in the main survey (n = 54), most participants pointed to exporting data (10) from their previous PM and importing it into their new or current PM (14). For instance, M40 stated that it "*didnt take more than saving a file to my computer and loading that file into Bitwarden to parse*" while M21 added that "*exporting from LastPass and importing into Bitwarden was virtually seamless.*" Four participants appreciated the ability of their new PMs to automatically save their logins as they visited new sites. For example, M01 said that they "*didn't have to do anything. I just visited my usual websites and entered my information. Keychain automatically saves my passwords.*" Other themes described by at least three participants included the limited clicks that participants had to make to transition (3), the ease of learning their new PM (3), and the simplicity or intuitiveness of their new PM's user interface (3). Overall, participants that used export and import functionalities when switching found the switching process easier.

Most challenging parts of the switching process. When asked about the most challenging part of switching PMs (**Q25**) in the main survey (n = 54), most participants described challenges related to moving their passwords to the new PM (14). This ranged from searching for the passwords in the previous PM to difficulty transferring them for example because the process was manual. M17 mentioned "*that the most difficult part of this password transition was finding where firefox stored my passwords*" while M29 was frustrated because of "*resaving all of my passwords manually. It was time consuming.*" M02 complained about "*the sheer number of usernames and passwords that I had to switch over*" while M23 was frustrated about "*manually adding every single password*" to their new PM.

While twelve participants indicated they did not face challenges, seven participants specifically complained about the process being manual while six had challenges exporting their credentials from their previous PM. Four participants struggled to get used to the user interface of their new PM. For instance, M53 had issues *"learning the difference in interface options between LastPass and KeePass. LastPass has a UX design that is more approachable to the general public, while KeePass seems designed more for individuals who are tech-savvy and prefer performance and features over a neater interface."*

Suggestions for improving the switching process. After inquiring about the most challenging parts of the PM switching process, we next asked participants about how the switching process could be made easier (**Q26**) in the main survey (n = 54). While most participants (11) had no suggestions, nine participants suggested improvements to PM's user interfaces. M31 was frustrated about having to click to reveal every password, and suggested that a single button that reveals all passwords in the PM would be helpful: *"I think there should be an option to click a button and it'll show all passwords instead of keeping it hidden. I think it's a bit annoying having to hit the "Show" icon every time I look at my password."* M34 suggested the need for a way to prevent their previous PM from prompting them to save their passwords: *"Knowing a way to turn off the chrome password manager so that it wouldn't still be asking*

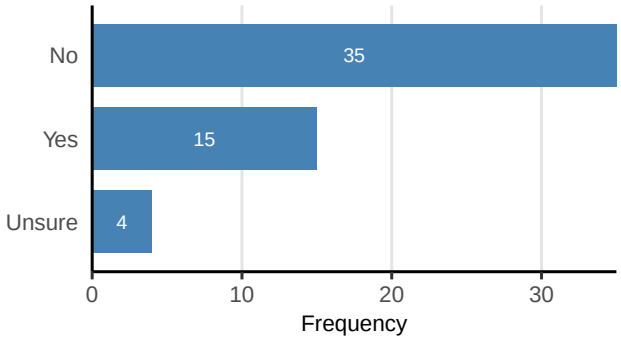

Figure 5: Whether participants looked at any guidance when switching PMs from the main survey (n = 54). Participants could only select one option.

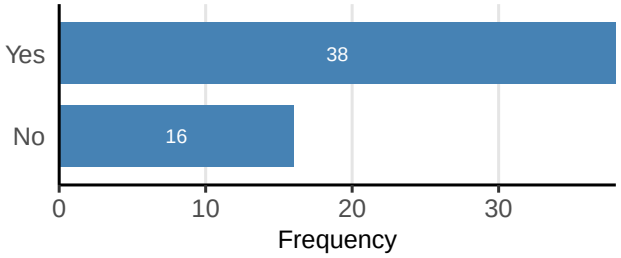

Figure 6: Awareness of the LastPass breach in the main survey (n = 54). Participants could only select one of the responses.

me if I want to save passwords there." M38 suggested the need for *"making Import/Export buttons more visible in settings."*

Eight participants mentioned that an automated way to switch PMs would make the switching process easier, with M19 pointing to the need for *"automated movement of accounts and passwords."* Other suggestions for improving the process described by at least three participants included an export feature (5), an import feature (5), availing guides (4), and making the process easy (3).

Sources of guidance when switching. When asked whether they relied on any guides when switching PMs (**Q16**) in the main survey (n = 54), a majority of participants (35) indicated they did not, with only 15 participants indicating doing so; four participants were unsure (see Figure 5). Out of those that used guides, six indicated the guides were provided by the PMs, particularly the one they were switching to. For instance, M45 indicated that they *"checked articles and the official website for how to correctly transfer the saved passwords. I mainly used the official Bitwarden website as a reference due to them having a high expertise on their own software."*

Five participants used Google to search for help online, with M03 stating they *"entered the search string "how to export from LastPass to Google Password Manager", and choose an article from a computer or Android blog that has step by step instructions."* Other sources of guidance mentioned by at least two participants were reading online articles (2) as well as checking online reviews (2) of the PMs.

Skills required to successfully switch. In the main survey (n = 54), we asked participants to indicate any technical skills required to successfully switch from one PM to another (**Q27**). While 12 participants said none are required as the process is easy, 10 pointed to general computer skills as necessary. For example, M26 said that *"I don't believe the barrier to doing it is that high, I think if you had even a pretty baseline understanding of computers you would be able to get through it fairly quickly."* Other common skills mentioned by participants included data import (9) and export skills (6), file management skills (5), typing skills (5), data download (3), and reading skills (3) to be able to follow guides for switching.

Advice for switching. In the main survey (n = 54), we asked participants to provide any advice they would give to someone considering switching PMs (**Q28**). Eight participants mentioned they would advise those switching to research and find a PM that both fits their needs but is also secure and has not suffered breaches. M16 pointed to the need to *"research which one best suits you and look at reviews"* while M31 added that they *"would tell them to do some research and see if any of the password managers have had data breaches and if so, how did they go about the issue."*

Six participants said they would advise those switching to backup their passwords in some way for example by writing them down or keeping them saved in the previous password manager. For instance, M44 said those switching should *"keep your old passwords saved so you can go back to them incase they don't work on the new platform"* while M05 added that *"if you aren't tech savvy, keep a written log of your passwords somewhere to help you in the event that your process of manually entering the passwords on a new service stalls. It is probably good no matter what to keep them stored in multiple places to ensure they are not lost."*

Other advice suggested by several participants include finding a guide to help with switching (5), first trying the new PM to ensure it suits your needs (4), exporting passwords rather than trying to transfer them manually (3), following instructions from the PMs or other guides (3), and overall finding a good PM that suits your needs and is affordable or free (3).

RQ3 Summary. Overall, we find that most participants used manual mechanisms to switch PMs. However, those that exported their data from their previous PM and imported it into their new PM found the switching process easier. At the same time, most participants indicated not using any guides for switching PMs, suggesting an opportunity for PMs to provide more support to their customers.

5.4 Awareness and Perceptions about Breaches

In this section, we discuss participants' awareness, perceptions, and reactions to the LastPass breach described in Section 2.2, followed by their concerns (and lack thereof) with passwords stored in Lastpass.

Awareness about the LastPass security breach. In the main survey (n = 54), we asked participants whether they were aware about the LastPass breach prior to the survey (**Q32**). Most participants (38) were aware, with only 16 participants unaware (see Figure 6).

LastPass security breach description and perceptions. For the 38 participants that were aware of the LastPass breach in the main survey, we asked them to briefly describe what happened (**Q33**).

The most frequently described theme was access to customer user data (18), specifically by some bad actors or hackers (15), consistent with the alert sent out by LastPass. For instance, M53 stated:

> *"Some of LastPass' files were breached by a third party (this has happened multiple times), including some encrypted files. I don't remember if master password data was also breached but I believe so. The data should have all been secure and encrypted so there was no direct evidence that user passwords/login info had been hacked directly due to this."*

M41 described that user data was accessed, but not not customers' actual passwords: *"I believe that hackers gained access to LastPass user information that was stored in plain text, but that the actual individual login information was not hacked, though I could be wrong."* This was also the case with M45 who believed that "*the breach did not leak out the actual passwords. I don't remember the details, but I think the breach was related to other personal details.*"

M03 anticipated that a bad actor likely hacked an employee's computer and used the obtained logins to access customer data:

> *"A bad actor, possibly in Eastern Europe, Russia, or China, targeted the personal home computer of a senior developer or engineer for LastPass via an unpatched media player, installed a keylogger on that personal computer, and likely recorded the login information for that senior employee's work accounts, which they then used to log into the program's backend and copy everything within."*

M28 described being unsurprised by the breach because breaches can happen to anyone, especially because of specialized hackers:

> *"This has happened to several companies, and it's no surprise. The world wide web is vulnerable to breaches. There are people who specialize in hacking into systems, so I believe that hackers worked hard until they got in."*

M39, on the other hand, was upset at how long it took LastPass to communicate details about the breach:

> *"Credentials used to access secondary services at LastPass were used by malicious actors. The problem wasn't the breach, it was how long they took to respond and inform the public regarding the breach."*

Other common themes that were described by at least three participants included LastPass getting compromised (8), participants being unsure of what particularly happened (7) and passwords getting stolen from LastPass (3) during the breach. For the 16 participants that were unaware about the breach prior to the study, five anticipated that user data had been accessed, with four particularly detailing that the access was likely by a third-party. Three participants further believed that user data had been stolen.

Concerns and reactions to the LastPass breach. After asking participants to describe what happened regarding the LastPass breach, we next asked them about their thoughts on the security of passwords currently stored in LastPass in the main survey (n = 54) as an open-response question (**Q35**). Most participants indicated that these passwords were no longer secure (19) because of the breach, or they had lost trust in LastPass (12). Nine participants anticipated

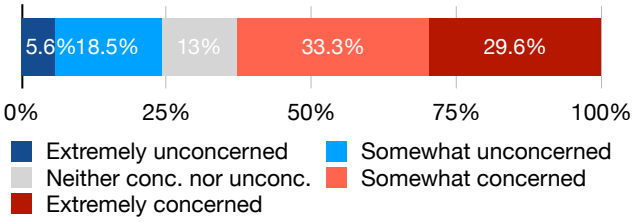

Figure 7: Concern level with passwords currently stored in Lastpass from the main survey (n = 54).

that LastPass had likely improved their security and therefore, passwords stored in LastPass were now secure. At the same time, five participants indicated they would never use LastPass again. For instance, M38 said they *"would not use the service again if they have proven to not properly care for my data."* while M48 added that they *"don't trust LastPass. I advise all my users and friends and family to move to a different platform."* Other themes described by at least three participants included feeling uncertain (4) as well as changing passwords (3), as elaborated by M53:

> *"I am very concerned about the security of passwords within cloud-based password managers like LastPass, after seeing the news and seeing multiple security issues for LastPass since I started using them. While the data is encrypted, there is no guarantee that someone couldn't unencrypt it in the future with more sophisticated technology. I had to change all of my passwords in every account because I no longer trusted LastPass."*

When asked how concerned they were with passwords currently stored in LastPass on a Likert-scale (**Q36**) in the main survey (n = 54), more than half of participants indicated they were somewhat or extremely concerned (see Figure 7). When asked to elaborate, several participants indicated being concerned due to the possibility of other breaches happening in future (7) as well as concerns regarding the previous breach and how it was handled by LastPass (6). Six participants described LastPass as insecure (6). For participants that were unconcerned, most of them attributed this to the fact that they do not or are no longer using LastPass (13), with M29 saying *"that's the whole reason I don't like password managers. They failed to keep customer information secure."* M53 similarly cited the breach as the reason *"why I no longer use it as a password manager."* M31 was not concerned because nothing had happened to their accounts yet, similarly noted in prior work [34]:

> *"Sometimes I would get alerts saying that my passwords were part of a data breach, but even then, I don't bother to change the passwords, and that's because I'm lazy. It'll only concern me if something actually happens to one of my accounts."*

Switching reasons for LastPass PM users. Out of the 26 participants that used LastPass previously as one of their PMs, only 6 explicitly changed PMs because of the security breach, with all six indicating they had lost trust in LastPass. For those that did not switch due to the breach, nine indicated they had already switched before the breach. Other reasons that were mentioned by one participant

included changing jobs, not liking LastPass, discontentment with their subscription fee as well as participants finding a simpler PM.

RQ4 Summary. Overall, we find that most participants in the main study were aware about the LastPass breach prior to the study, with most of them concerned about the security of passwords currently stored in LastPass. The breach particularly seemed to reduce user trust in LastPass, and passwords managers in general, and can further hinder the widespread adoption of PMs.

6 LESSONS AND RECOMMENDATIONS

In this study, we investigate password management as well as why and how users switch from one password manager (PM) to another through two online surveys with PM users, a screener (n = 412) followed by a main survey (n = 54). We find that most users switch PMs for usability reasons, and mostly transition using manual techniques for example copying and pasting logins from their previous to new PM. We additionally find that most participants are aware about the LastPass security breach, with some participants subsequently losing trust in LastPass and PMs generally as a result.

In the rest of this section, we explore other broader themes that we found, and make recommendations to PMs that can overall improve their user experience and boost adoption.

PM's password generation features remain under-utilized. When asked how they create passwords for their important accounts in the main survey, most participants indicated creating the passwords themselves and only storing them in the PMs. Subsequently, a majority of participants said they reuse passwords across accounts. The under-utilization of PMs' password generators [38, 48] seems to directly translate to password reuse across accounts, with some participants complaining that some of the passwords generated by PMs are too complex or sometimes fail to meet password requirements of different websites. There's thus a need to devise mechanisms to make PMs' password generators more usable by end-users to improve password security.

Recommendations: To make password generators more usable, PMs, and particularly browser-based PMs, should make their password generators more customizable; this is currently not the case with most browser-based PMs where users can only disable or enable password suggestions. This could include allowing users to generate passphrases [47] which are easier to enter on devices where the PM is not installed, but are still secure. These settings must also be more easily reachable by users.

Convenience and usability are influential in the adoption and switching of PMs. Our results show that most participants use PMs for convenience, e.g., because PMs save and auto-fill passwords for them, rather than for security purposes. At the same time, usability challenges that still plague PMs frustrate users and force them to seek alternatives. For instance, even though some participants appreciated PM prompts to save passwords, some complained that these prompts are annoying when they are triggered by non-password forms, save their credentials incorrectly, or are inconveniently-placed, making it difficult to interact with the website. This suggests that improving the overall user experience for PMs can directly improve their adoption and use.

Recommendations: Any campaigns fostering the adoption of PMs should focus on their convenience benefits, perhaps more than their security benefits. Additionally, PMs should regularly collect feedback from their users to improve their overall experience. If there are known issues, particularly that are website-related and out of the control of PMs, these should be properly documented and workarounds provided to reduce user frustration. Additionally, PMs, and particularly browser-based PMs, should make it easier for users to access and modify settings, including turning off prompts to save or generate passwords. While Chrome and FireFox PMs have toggles to turn this off, participants seemed unaware about this likely because these toggles are buried deep in the PM settings. As part of the prompts, PMs can additionally ask users if they would still like to be prompted to save their logins, and automatically turn them off if they indicate otherwise. Making the PM settings more reachable (as third-party PM extensions do) could also make it easier for users to quickly access and modify these settings rather navigating to a new (internal) web page as is currently the case.

Breaches reduce trust in PMs, ultimately inhibiting their adoption. While most participants switched from LastPass before the breach for various reasons, e.g., usability and the subscription fee charged, we noted that all the six participants that switched due to the breach lost trust in LastPass. Some participants were particularly displeased and concerned at how LastPass handled the breach and communicated to it's customers, believing that it was neither transparent nor timely. As a result, some participants indicated they do not trust or use PMs anymore. Some participants even mentioned they would tell their friends and family to keep off LastPass. This, coupled with the importance of word-of-mouth propagation in fostering PM use [32], shows that breaches as well as how they are handled can severely inhibit the adoption and usage of PMs.

Recommendations: We encourage PM companies to be more transparent and forthcoming about any security incidents to improve user trust. PMs should particularly provide regular and transparent updates throughout security-related incidents as well as inform their users of steps taken (and the steps users can similarly take) to further protect their accounts and information.

Providing more support and making switching easier will benefit PMs. When asked how they switched PMs, most participants indicated they had done so manually by copying usernames and passwords from their previous PM to their new PM. Most participants further indicated that transitioning manually was the one part of the switching process they found the most challenging. At the same time, a majority of participants indicated they did not use any guides to transition. It is in the best interests of PMs to make the transition process easier as well as offer guidance to users, as these can directly translate to more adoption of their very own PM.

Recommendations: To make it easier for users to transition from another PM, PMs can ask users if "*they are switching from a different password manager*" when they use the PM for the very first time. If users indicate so, the PM can avail instructions on how to export their details from their previous PM and import them into the new PM. Such instructions could also be provided through video tutorials to make them easier for users to follow. Whenever possible, PMs should be ready to offer additional technical support to users should they encounter further challenges when switching.

ACKNOWLEDGMENTS

We thank Elena Korkes and Victoria Hennemann for their assistance with qualitative coding. We thank Lucy Simko, David Balash, Neal Keating, Ruining Yang, and other members of the GWUSEC Lab for their invaluable input and feedback on the survey. Lastly, we are grateful to all the anonymous reviewers for their insightful comments and feedback. This material is based upon work supported by the National Science Foundation under Grant No. 1845300.

REFERENCES

[1] Nora Alkaldi and Karen Renaud. 2016. Why do people adopt, or reject, smartphone password managers?. In *Proc. EuroUSEC*.
[2] Nora Alkaldi and Karen Renaud. 2019. Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs. In *Proc. HICSS*.
[3] Mohammed H Almeshekah, Christopher N Gutierrez, Mikhail J Atallah, and Eugene H Spafford. 2015. ErsatzPasswords: Ending Password Cracking and Detecting Password Leakage. In *Proc. ACSAC*.
[4] Fahad Alodhyani, George Theodorakopoulos, and Philipp Reinecke. 2020. Password Managers—It's All about Trust and Transparency. *Future Internet* 12, 11 (2020), 189.
[5] Sabrina Amft, Sandra Höltervennhoff, Nicolas Huaman, Yasemin Acar, and Sascha Fahl. 2023. "Would You Give the Same Priority to the Bank and a Game? I Do Not!" Exploring Credential Management Strategies and Obstacles during Password Manager Setup. In *Proc. SOUPS*.
[6] J. Craig Anderson. 2013. Identity theft growing, costly to victims. https://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/.
[7] Salvatore Aurigemma, Thomas Mattson, and Lori Leonard. 2017. So much promise, so little use: What is stopping home end-users from using password manager applications?. In *Proc. HICSS*.
[8] Salvatore Aurigemma, Thomas Mattson, and Lori Leonard. 2019. Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications. *AIS Transactions on Replication Research* 5, 3 (2019), 1–21.
[9] Hristo Bojinov, Elie Bursztein, Xavier Boyen, and Dan Boneh. 2010. Kamouflage: Loss-Resistant Password Management. In *Proc. EuroUSEC*.
[10] Joseph Bonneau, Cormac Herley, Paul C van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proc IEEE S&P*.
[11] Alan S Brown, Elisabeth Bracken, Sandy Zoccoli, and King Douglas. 2004. Generating and remembering passwords. *Applied Cognitive Psychology* 18, 6 (2004), 641 – 651.
[12] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. 2015. Cracking-resistant password vaults using natural language encoders. In *Proc IEEE S&P*.
[13] Sunil Chaudhary, Tiina Schafeitel-Tähtinen, Marko Helenius, and Eleni Berki. 2019. Usability and Security in Password Managers: A Quest for User-Centric Properties and Features. *Computer Science Review* 33 (2019), 69–90.
[14] Sunil Chaudhary, Tiina Schafeitel-Tähtinen, Marko Helenius, and Eleni Berki. 2019. Usability and Security in Password Managers: A Quest for User-Centric Properties and Features. *Computer Science Review* 33 (2019), 69–90.
[15] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. 2006. A Usability Study and Critique of Two Password Managers. In *Proc. SOUPS*.
[16] Mark Ciampa. 2013. A Comparison of User Preferences for Browser Password Managers. *Journal of Applied Security Research* 8, 4 (2013), 455–466.
[17] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proc. CHI*.
[18] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The Tangled Web of Password Reuse. In *Proc. NDSS*.
[19] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences* 7, 1 (2017), 12.
[20] Dinei Florêncio and Cormac Herley. 2007. A large-scale study of web password habits. In *Proc. WWW*.
[21] Anuj Gautam, Shan Lalani, and Scott Ruoti. 2022. Improving Password Generation Through the Design of a Password Composition Policy Description Language. In *Proc. SOUPS*.
[22] Maximilian Golla, Benedict Beuscher, and Markus Dürmuth. 2016. On the Security of Cracking-Resistant Password Vaults. In *Proc. CCS*.
[23] Ameya Hanamsagar, Simon S Woo, Chris Kanich, and Jelena Mirkovic. 2018. Leveraging Semantic Transformation to Investigate Password Habits and Their Causes. In *Proc. CHI*.
[24] N. Huaman, S. Amft, M. Oltrogge, Y. Acar, and S. Fahl. 2021. They Would do Better if They Worked Together: The Case of Interaction Problems Between Password Managers and Websites. In *Proc. IEEE S&P*.
[25] Identity Theft Resource Center. 2021. *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends, and Workplaces*. Technical Report. Identity Theft Resource Center. https://www.idtheftcenter.org/event/2021-consumer-aftermath-report/
[26] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Proc. SOUPS*.
[27] Blake Ives, Kenneth R Walsh, and Helmut Schneider. 2004. The domino effect of password reuse. *Commun. ACM* 47, 4 (2004), 75 – 78.
[28] Ari Juels and Thomas Ristenpart. 2014. Honey Encryption: Security Beyond the Brute-Force Bound. In *Proc. EUROCRYPT*.
[29] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. 2014. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. In *Proc. USENIX Security*.
[30] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. 2018. Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. In *Proc. USENIX Security*.
[31] Raymond Maclean and Jacques Ophoff. 2018. Determining Key Factors that Lead to the Adoption of Password Managers. In *Proc. ICONIC*.
[32] Peter Mayer, Collins W. Munyendo, Michelle L. Mazurek, and Adam J. Aviv. 2022. Why Users (Don't) Use Password Managers at a Large Educational Institution. In *Proc. USENIX Security*.
[33] Peter Mayer, Yixin Zou, Byron M. Lowens, Hunter A. Dyer, Khue Le, Florian Schaub, and Adam J. Aviv. 2023. Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches. *ACM Trans. Comput.-Hum. Interact.* (2023).
[34] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J. Aviv. 2021. "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *Proc. USENIX Security*.
[35] Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and Paul C van Oorschot. 2012. Tapas: design, implementation, and usability evaluation of a password manager. In *Proc. ACSAC*.
[36] Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, and Blase Ur. 2023. A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords. In *Proc. USENIX Security*.
[37] Sean Oesch and Scott Ruoti. 2020. That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers. In *Proc. USENIX Security*.
[38] Sean Oesch, Scott Ruoti, James Simmons, and Anuj Gautam. 2022. "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In *Proc. CHI*.
[39] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Proc. SOUPS*.
[40] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2021. Why Older Adults (Don't) Use Password Managers. In *Proc. USENIX Security*.
[41] Johnny Saldaña. 2013. *The coding manual for qualitative researchers* (2nd ed.). SAGE, Los Angeles. OCLC: ocn796279115.
[42] Sunyoung Seiler-Hwang, Patricia Arias-Cabarcos, Andres Marín, Florina Almenares, Daniel Diaz-Sanchez, and Christian Becker. 2019. "I Don't See Why I Would Ever Want to Use It": Analyzing the Usability of Popular Smartphone Password Managers. In *Proc. CCS*.
[43] Frank Stajano, Max Spencer, Graeme Jenkinson, and Quentin Stafford-Fraser. 2015. Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers. In *Proc. PASSWORD*.
[44] Elizabeth Stobert and Robert Biddle. 2018. The Password Life Cycle. *ACM Transactions on Privacy and Security (TOPS)* 21, 3 (2018), 32 pages.
[45] David R. Thomas. 2006. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation* 27, 2 (Jan. 2006), 237–246.
[46] Karim Toubba. 2022. https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/.
[47] Xiaoyuan Wu, Collins W. Munyendo, Eddie Cosic, Genevieve A. Flynn, Olivia Legault, and Adam J. Aviv. 2022. User Perceptions of Five-Word Passwords. In *Proc. ACSAC*.
[48] Samira Zibaei, Amirali Salehi-Abari, and Julie Thorpe. 2023. Dissecting Nudges in Password Managers: Simple Defaults are Powerful. In *Proc. SOUPS*.

APPENDIX

A PRE-SCREENER

Password Manager Description
Please read the following text carefully.

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

and Edge. These browsers can remember passwords for websites, as well as autofill them for you.

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

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

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

P1 Based on this description, do you currently use a password manager? (select all that apply)
☐ I save my passwords in the browser (for example, passwords saved in Google Chrome or Mozilla FireFox).
☐ I use a third-party password manager (for example, LastPass or 1Password).
☐ I use a system-provided password manager (for example, Apple's Keychain).
☐ I do not use a password manager.
Proceed below if they use any form of password manager from above, otherwise end the screener.

P2 What password manager(s) are you currently using? Select all that apply.
☐ LastPass ☐ 1Password ☐ Dashlane ☐ KeePass ☐ EnPass ☐ Apple Keychain ☐ Norton Lifelock Password Manager ☐ Kaspersky Password Manager ☐ Save passwords on Chrome ☐ Save passwords on FireFox ☐ Other: [open]
Ask the following if they select multiple above.

P3 What password manager do you most frequently use?
○ LastPass ○ 1Password ○ Dashlane ○ KeePass ○ EnPass ○ Apple Keychain ○ Norton Lifelock Password Manager ○ Kaspersky Password Manager ○ Save passwords on Chrome ○ Save passwords on FireFox ○ Other: [open]
*For those that select multiple: For the rest of the questions below, we will focus on the password manager you most frequently use, which you indicated to be **current PM***

P4 How satisfied are you overall with your experience using **current PM**? [Extremely dissatisfied, somewhat dissatisfied, neither satisfied nor dissatisfied, somewhat satisfied, extremely satisfied]

P5 What do you like the most about **current PM**? [open]

P6 What do you like the least about **current PM**? [open]

P7 Please indicate your agreement with the following statements regarding **current PM.**[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]
- Using **current PM** makes my accounts less likely to be compromised.
- Using **current PM** means I do not have to worry as much about the safety of my accounts.
- I think that **current PM** is fun to use.
- I think that **current PM** is easy to use.
- I think that **current PM** is difficult to use.
- I think that **current PM** is annoying to use.
- I trust **current PM**.
- I know how **current PM** works.

P8 Have you ever switched from a different password manager to **current PM**?
○ Yes ○ No ○ Unsure

Demographic Questions

D1 Select your age.
○ 18-24 ○ 25-29 ○ 30-34 ○ 35-39 ○ 40-44 ○ 45-49 ○ 50-59 ○ 60-64 ○ 65-70 ○ 71-75 ○ 76-80 ○ 81-85 ○ 86-90 ○ 91-95 ○ 96+ ○ Prefer not to say

D2 With which gender do you most identify?
○ Male ○ Female ○ Non-Binary ○ Prefer to self-describe [open text] ○ Prefer not to say

D3 What is the highest degree or level of school you have completed?
○ Some high school ○ High school ○ Some college ○ Trade, technical, or vocational training ○ Associate's Degree ○ Bachelor's Degree ○ Master's Degree ○ Professional Degree ○ Doctorate ○ Prefer not to say

D4 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 or IT.
○ I do not have an education in, nor do I work in, the field of computer science or IT.
○ Prefer not to say

B MAIN SURVEY

Q1 What password manager are you currently using? (select all that apply)
☐ LastPass ☐ 1Password ☐ Dashlane ☐ KeePass ☐ EnPass ☐ Apple Keychain ☐ Norton Lifelock Password Manager ☐ Kaspersky Password Manager ☐ Save passwords on Chrome ☐ Save passwords on FireFox ☐ Other: [open]
Ask the below follow-up question if they select multiple above.

Q2 You indicated that you use several password managers. Overall, what password manager do you **most frequently use?**
○ LastPass ○ 1Password ○ Dashlane ○ KeePass ○ EnPass ○ Apple Keychain ○ Norton Lifelock PM ○ Kaspersky Password Manager ○ Save passwords on Chrome ○ Save passwords on FireFox ○ Other: [open]

Q3 In the first survey, you indicated that you were using a different password manager(s) prior to switching to **current PM**. What password manager(s) were you previously using before switching to **current PM**? Select all that apply.
☐ LastPass ☐ 1Password ☐ Dashlane ☐ KeePass ☐ EnPass ☐ Apple Keychain ☐ Norton Lifelock Password Manager ☐ Kaspersky Password Manager ☐ Save passwords on Chrome ☐ Save passwords on FireFox ☐ Other: [open]
Ask the below follow-up question if they select multiple above.

Q4 You indicated that you were previously using multiple password managers. Of these password managers you were previously using, which one did you most frequently use overall?
○ LastPass ○ 1Password ○ Dashlane ○ KeePass ○ EnPass ○ Apple Keychain ○ Norton Lifelock PM ○ Kaspersky Password Manager ○ Save passwords on Chrome ○ Save passwords on FireFox ○ Other: [open]
*For those that select multiple: For the rest of the questions below, we will focus on the password manager you most **frequently used previously**, which you indicated to be **previous PM***

Q5 Approximately when did you switch from **previous PM** to **current PM**?
○ Within a week ○ Within a month ○ Within the last three months ○ Within the last six months ○ Within a year ○ Within the last three years ○ More than three years ago ○ Unsure/cannot remember

Q6 What motivated you to switch from **previous PM** to **current PM**? [open]

Q7 How satisfied were you overall with your experience using **previous PM**? [5-point Likert]

Q8 What did you like the most about **previous PM**? Please elaborate. [open]

Q9 What did you like the least about **previous PM**? Please elaborate. [open]

Q10 Indicate your agreement with the following statements regarding the password manager you most frequently used, which you indicated was **previous PM**. [Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]
- Using **previous PM** made my accounts less likely to be compromised.
- Using **previous PM** meant I did not have to worry as much about the safety of my accounts.
- I think that **previous PM** was fun to use.
- I think that **previous PM** was easy to use.
- I think that **previous PM** was difficult to use.
- I think that **previous PM** was annoying to use.
- I trusted **previous PM**.
- I know how **previous PM** works.

You indicated that you switched from **previous PM** to **current PM**. In this section, we will first focus on your previous PM, which you indicated to be **previous PM**.

Q11 When previously using **previous PM**, select the statement that best describes your behavior when creating passwords. When creating or resetting a password for an important account, ...
○ I let **previous PM** create and store the password.
○ I created the password myself, and let **previous PM** store it for me.
○ I created the password myself and recalled it without storing it in **previous PM.**

Q12 How likely are you to recommend **previous PM** to others? [Extremely unlikely, somewhat unlikely, neither likely nor unlikely, somewhat likely, extremely likely].

In this section, we will now focus on your current PM, which you indicated to be **current PM**.

Q13 When using **current PM**, select the statement that best describes your behavior when creating passwords. When creating or resetting a password for an important account, ...
○ I let **current PM** create and store the password.
○ I create the password myself, and let **current PM** store it for me.
○ I create the password myself and recall it without storing it in **current PM.**

Q14 How likely are you to recommend **current PM** to others? [Extremely unlikely, somewhat unlikely, neither likely nor unlikely, somewhat likely, extremely likely].

Password Manager Switching

Q15 When switching from one password manager to another, you can use different techniques to transfer your usernames and passwords to the new password manager. For example, you can manually copy them, manually type them or export them. Please describe how you transitioned from **previous PM** to **current PM**?

Q16 When switching PMs, did you look at any guides or information sources?
○ Yes ○ No ○ Unsure
For those that say yes above, ask below follow up:

Q17 You mentioned that you looked at guides or information sources when switching from **previous PM** to **current PM**. Please describe them. [open]

Q18 When switching PMs, was any guidance provided by **previous PM**?
○ Yes ○ No ○ Unsure

Q19 When switching PMs, was any guidance provided by **current PM**?
For those that say received guidance from previous PM:

Q20 You mentioned that some guidance was provided by **previous PM** during your transition from **previous PM** to **current PM**. Please describe it. [open]

Q21 Please rate your overall satisfaction with the guidance that was provided by **previous PM** [Extremely dissatisfied, somewhat dissatisfied, neither satisfied nor dissatisfied, somewhat satisfied, extremely satisfied]
For those that say received guidance from current PM:

Q22 You mentioned that some guidance was provided by **current PM** during your transition from **previous PM** to **current PM**. Please describe it. [open]

Q23 Please rate your overall satisfaction with the guidance that was provided by **current PM** [Extremely dissatisfied, somewhat dissatisfied, neither satisfied nor dissatisfied, somewhat satisfied, extremely satisfied]

Q24 When switching from **previous PM** to **current PM**, what part of the transition process did you find the **easiest**? Please elaborate. [open]

Q25 When switching from **previous PM** to **current PM**, what part of the transition process did you find the **most challenging**? Please elaborate. [open]

Q26 In your opinion, what is one thing that could have made the **transition easier**? [open]

Q27 What **technical skills**, if any, are required to switch from one password manager to another?

Q28 From your experience, what **advice**, if any would you give to someone switching from one password manager to another?

General Password Manager Usage

Q29 Where did you first hear about password managers?
○ Work ○ Media (Internet, TV, radio, etc) ○ Other People (friends, family, etc, but not at work) ○ School/class ○ I don't know (don't remember, not sure) ○ I first heard about it in this study ○ Other [open]

Q30 What prompted you to start using a password manager in the first place?
☐ Convenience ☐ Memory limitations ☐ Received prompts for example from a browser ☐ To improve the security of my user accounts and passwords ☐ Other [open]

Q31 Do you reuse passwords across any of your accounts?
○ Yes ○ No ○ Unsure

LastPass Breach

Q32 In December last year, the **LastPass** password manager announced that it had been **breached.** Were you aware about this breach prior to this study?
○ Yes ○ No
For participants aware about the breach:

Q33 Briefly describe what you think happened regarding the breach to LastPass. [open]
For participants not aware about the breach:

Q34 Briefly describe what you anticipate happened regarding the breach to LastPass. [open]

Q35 What are your thoughts on the **security of passwords** currently stored in LastPass? [open]

Q36 Overall, how **concerned** are you about passwords stored in LastPass? [Extremely concerned, somewhat concerned, neither concerned nor not concerned, somewhat not concerned, extremely not concerned]

Q37 Please elaborate on why you are **concerned or not** about passwords stored in LastPass. [open]

For participants that indicated they use LastPass:

Q38 Was your decision to switch from LastPass influenced by the breach?
○ Yes ○ No

For participants that switched due to breach:

Q39 You indicated that your decision to switch from Lastpass was influenced by the breach. Please elaborate. [open]

For participants that did not switch due to breach:

Q40 You indicated that your decision to switch from Lastpass was NOT influenced by the breach. Please elaborate. [open]

For participants that indicated using LastPass:

Q41 Knowing the breach, how likely are you to continue using LastPass? [Extremely unlikely, somewhat unlikely, neither likely nor unlikely, somewhat likely, extremely likely].

For non-LastPass users:

Q42 Assuming you were a LastPass user, how likely are you to continue using LastPass now that you are aware of the breach? [Extremely unlikely, somewhat unlikely, neither likely nor unlikely, somewhat likely, extremely likely].

C QUALITATIVE CODES

• easy-to-use (107) **• remember-passwords (91)** **• nothing (86)** *import-simple (1)* **• convenience (68)** *low-importance (1), no-separate-app (1), autofill (1)* **• synchronization (64)** *accessible (1), fast (1)* **• autofill (47)** *fast (1), entered-once (1), remember-passwords (1), multi-device (1)* **• concerned (36)** *repeated-breaches (8), breach (6), security (3), accessibility-of-accounts (2), security-measures-taken (1), companies-not-transparent (1), passwords-vuln (1), important-passwords (1), if-account-breached (1)* **• secure (36)** *needs-password (3), encrypted (2), somewhat-safe (2), unique-passwords (2), personal-info-not-accessible (1), fairly-secure (1), most-likely (1), strong-passwords (1), enough (1)* **• export (34)** *passwords (7), file (6), csv (4), change-format (1), effective (1), remembering-process (1), feature (1), more-readable-format (1), csv (1), method-compatibility (1), pms-compatibility (1)* **• manual (33)** *typed (8), copied (7), entered (7), transferred (5), change-passwords (3), adding-password (2), switching (1), remember-passwords (1), migrated (1)* **• insecure (32)** *saves-non-critical-passwords (2), passwords-saved-on-phone (1)* **• not-secure (31)** *reoccuring-breach (2), passwords-vuln (2), stolen-passwords (2), eventually-exploited (1), companies-not-transparent (1), password-vuln (1), lost-trust (1), repeated-passwords (1), accounts-not-safe (1), monitor-accounts (1), change-passwords (1), user-data (1), open-source-better (1), move-credentials (1), credentials-at-risk (1)* **• not-concerned (27)** *don't-use (15), improved-security (3), changed-passwords (2), no-sensitive-info (2), non-important-accounts (2), sensitive-info (1), no-personal-info (1), nothing-to-do (1), no-financial-info (1), lazy (1), anticipated-breach (1), use-for-work (1), notified-on-leaks (1), other-places-unsafe (1), multiple-safeguards (1), no-access (1), not-private (1)* **• prompts (26)** **• password-generation (25)** *more-secure (1)* **• fails-to-save (24)** **• usability-issues (24)** *phone (4)* **• access-data (23)** *tied-to-user (7), encrypted-files (3), database (3), plaintext (2), secondary-service (1), personal-info (1), view-passwords (1), how-pm-worked (1), user-information (1), servers (1), source-code (1), passwords (1), email (1), username (1)* **• doesn't-work (22)** **• import (22)** *file (2), allowing-csv (1), automated (1), documentation (1), setup (1), automatic (1), improve-process (1), pms-compatibility (1)* **• fails-to-update-changes (22)** *forget-passwords (1)* **• lost-trust (19)** *repeat (2), cloud-based-pms (2), info-not-safe (2), data-breach (1), reoccuring-breach (1), inconsistent-stories (1), skeptical (1), outsourcing-storage (1)* **• hacking-concerns (18)** *passwords–compromise (2), unauthorized-access (1)* **• none (18)** **• usability (17)** *easy (6), multi-device (3), layout (1), no-dark-mode (1), integrated-browser (1), no-multi-device (1), chrome-integration (1)* **• saves-incorrectly (17)** **• easy (15)** **• bad-actor (15)** **• biometrics (15)** *easy-login (4), autofill (3), easy-to-use (1), secure (1)* **• passwords (15)** *search (3), chrome-storing (2), large-amount (2), recollection (2), saving (1), across-accounts (1), transfer (1), incorrect-password (1), reset (1), creating-new-passwords (1), changing (1), difficulty-transferring (1)* **• autofill-fails (15)** **• password-retrieval (15)** **• requires-login (15)** *can't-access-accounts (1)* **• fast (14)** **• automatic (14)** *storage (1), logs (1)* **• importing-data (14)** *quick (2), seamless (1), webvault (1), simple (1)* **• doesn't-sync (13)** **• built-in (12)** **• popups (12)** *non-passwords (3), website-usability-issues (1)* **• no-challenges (12)** **• unauthorized-access (12)** **• security (12)** *breach (6), info-not-safe (2), hacked (1), no-protection-data (1), authentication (1), problems (1)* **• buggy (12)** *password-recovery (1), password-updates (1), poor-navigation (1), clunky (1), flaky-app (1), clunky-integration (1), look-elsewhere (1), search-feature (1), crashes (1), not-reliable (1)* **• password-organization (11)** **• easy-login (11)** *remember-passwords (3)* **• breaches (11)** *require-resets (1), past-incidents (1)* **• documentation (10)** *import-data (3), help-center (3), guide (2), unsure (1), transition (1)* **• exporting-data (10)** *quick (1), seamless (1), downloading (1), correct-file-type (1), tutorial (1)* **• forget-passwords (10)** *loss-of-access (1)* **• limited-to-platform (10)** **• computer-skills (10)** **• data-breach (10)** *compromised (2), lost-trust (2), security-concerns (1)* **• simple (10)** **• improvements-UI (9)** *turn-off-PM (1), automatic-transfer (1), settings (1), export-button (1), sign-in (1), account-recovery (1), transfer-passwords-bulk (1), import-button (1), show-all-passwords-button (1), user-friendly (1)* **• open-source (9)** **• fails-to-popup (9)** **• improved (9)** *after-breach (8), more-secure (1)* **• data-import (9)** **• password-updates (9)** *easy-to-use (1)* **• duplicate-entries (9)** *website-changes (1), different-urls (1)* **• research (9)** *breaches (3), security (2), do-it-once (1)* **• subscription-fee (9)** *high (1), more-expensive (1), started-charging (1), not-free (1)* **• outdated-ui (8)** **• compromised (8)** *development-env (1)* **• slow (8)** *syncing-passwords (1)* **• automated (8)** *transfer (2), passwords-update (1), transfer-passwords (1), temporary-code (1), insecure (1), movements (1)* **• switched-before-breach (8)** **• costly (7)** *limited-income (1)* **• feeling-secure (7)** **• unsure (7)** **• multi-device (6)** **• pm-guide (6)** *expertise (1)* **• saves-non-passwords (6)** **• instructions (6)** *import-data (3), export-data (3)* **• easy-integration (6)** **• backup (6)** *write-down (2), multiple-places (1)* **• annoying (6)** *prompts (2)* **• affordable (6)** **• autosave (6)** *after-inserting-info (2), passwords (1), no-manual-input (1)* **• data-export (6)** **• would-not-use (5)** *more-info (1), failed (1)* **• google (5)** *import (1), export (1), passwords-transfer (1)* **• hard-to-update (5)** **• typing-skills (5)** **• functionality (5)** *feature (1), less-notifications (1)* **• find-guide (5)** *seamless (1), import/export (1)* **• browser-switch (5)** *default (2), not-default (1), worse (1)* **• saved-password (5)** **• don't-remember (5)** *no-transition (1), start-new (1), sites (1), export (1)* **• no-transition (5)** *sign-in (1), lost-password (1), update (1), job (1)* **• file-management (5)** **• too-complex-passwords (5)** **• fails-to-detect-entries (5)** **• breach (5)** *lost-trust (2), raised-questions (1)* **• changed-passwords (4)** **• challenges-for-several-accounts (4)** **• all-passwords-in-one-place (4)** **• save-passwords (4)** **• familiarity (4)** *UI (3), site-use (1)* **• fails-to-update (4)** **• self-hosted (4)** *secure (2)* **• password-management (4)** **• uncertain (4)** *breached-info (1), security (1), eventually-breakable (1), seems-okay (1)* **• free (4)** **• guides (4)** *pms (1), tour-feature (1), videos (1), export (1)* **• don't-use (4)** *breach (1), unusable (1), intrusive (1), clunky (1)* **• try-new-pm (4)** *usability (1), easy-to-use (1), trustworthy (1)* **• limited-features (4)** *requires-subscription (4)* **• follow-instructions (4)** *new-pm (1), don't-delete (1)* **• reliable (4)** *after-breach (1)* **• doesn't-save-usernames (4)** **• youtube (4)** **• third-party (4)** *wanted-passwords (1)* **• saves-old-passwords (4)** **• understanding-pm (3)** *easy (1)* **• check-passwords (3)** **• os--switch (3)** **• stole-passwords (3)** *got-hashes (1), don't-use-lastpass (1)* **• user-interface (3)** *intuitive (2)* **• privacy-concerns (3)** **• integration (3)** **• works (3)** **• data-download (3)** **• aesthetics (3)** *UI (2)* **• use-good-pm (3)** *works (1)* **• inconvenience (3)** *as-Google-PM (1)* **• functional (3)** **• easy-process (3)** **• reading (3)** **• limited-clicks (3)** *complete-task (2), transfer-info (1)* **• guide (3)** *export (3)* **• security-concerns (3)** **• steal (3)** *credit-cards (1)* **• organize (3)** *easy (1)* **• information-risk (3)** *everybody (1)* **• information-lookup (2)** **• not-open-source (2)** **• accessible (2)** **• online-reviews (2)** **• search (2)** *menu (1), guide (1)* **• 2fa (2)** **• transfer-all (2)** **• list (2)** *previous-sites (1), stored-passwords (1)* **• limited (2)** **• useful (2)** **• trust (2)** *in-firefox (1), platform (1)* **• tutorial (2)** *export-passwords (1), screenshots (1)* **• message (2)** *unsure (1), get-csv (1)* **• trust-issues (2)** **• not-automatic (2)** **• hard-to-delete (2)** **• subscription (2)** **• login (2)** **• unpatched-media (2)** **• browser-knowledge (2)** **• app-knowledge (2)** **• account-management (2)** **• strong–password-generation (2)** **• account-creating (2)** **• good-memory (2)** **• straight-forward (2)** **• effective (2)** **• don't-use-pm (2)** *important-accounts (1)* **• vault-password-leaks (2)** *unauthorized-access (1)* **• master-password (2)** **• online-forums (2)** **• saves-others-information (2)** **• concern (2)** *password-recovery (1), just-learned-breach (1)* **• data-exposed (2)** **• passwords–fail-requirements (2)** **• read-documentation (2)** **• login-skills (2)** **• no-issues (2)** **• sync (2)** *work-and-personal (1), info (1)* **• copy-paste (2)** *fast (1)* **• passwords-compromise (2)** **• no-trust (2)** **• compatibility (2)** *used-subsystem (1)* **• N/A (2)** **• online-article (2)** **• requires-subscription (2)** **• entire-process (2)** **• breach-alerts (2)** **• delete-passwords-file (2)** **• no-process (2)** **• reset–fails (2)** **• remember-accounts (2)** **• manual-input (2)** *reentered-passwords (2)* **• expected-safety (2)** **• relieved (2)** *don't-use-lastpass (2)* **• started-using-it (2)** **• passwords-not-accessed (2)** **• data-upload (2)** **• limited (2)** *to-platform (3), features (1), passwords (1)* **• saves-wrong-usernames (2)** **• new-passwords (1)** **• disappointed (1)** **• unfamiliar-features (1)** **• facial-recognition (1)** **• security-adjustments (1)** **• seamless (1)** **• critical-thinking (1)** **• start-over (1)** **• panic (1)** **• already-switched (1)** **• vault-account (1)** *group-accounts (1)* **• stop-using (1)** **• switched (1)** *lost-access (1), due-to-breach (1)* **• random-passwords (1)** **• not-password-vaults (1)** **• navigation-skills (1)** **• one-time-pay (1)** *premium-features (1)* **• customizable (1)** **• hard–to-manage (1)** **• changed-jobs (1)** **• multi-user (1)** *share-with-family (1)* **• don't-use-lastpass (1)** **• incompatibility (1)** **• forget-vault-password (1)** *biometrics (1)* **• many-options (1)** **• loading–faster (1)** *passwords (1)* **• prompts-passwords (1)** **• doesn't-create-passwords (1)** **• outdated (1)** **• usability-issue (1)** *no-multi-device (1)* **• set-aside-day (1)** *do-it-once (1)* **• device-restricted (1)** *chrome (1)* **• OS-knowledge (1)** **• use-program (1)** **• biometric-failure (1)** **• prompts-saving (1)** **• personal-device-contained-user-info (1)** **• backup-difficult (1)** **• use-keychain (1)** **• check-security-privacy-concerns (1)** **• passwords-not-vulnerable (1)** **• surveillance (1)** **• practical (1)** **• no-set-up-time (1)** *nothing-new (1)* **• view-passwords (1)** **• spreadsheet-usage (1)** **• received-email (1)** **• remote-connection (1)** **• IT-person (1)** **• security-issue (1)** **• straight-forward (1)** **• better-than-nothing (1)** **• login-fails (1)** **• tracking (1)** **• password-sharing (1)** **• navigation (1)** **• stripped-data (1)** **• unsurprised (1)** *everyone-vulnerable (1)* **• not-worried (1)** **• remember-vault-password (1)** **• don't-trust-anyone (1)** **• no-AWS (1)** **• decrypting-passwords (1)** **• hard-to-track (1)** **• local (1)** **• update-passwords-often (1)** **• oauth-challenges (1)** **• everything (1)** **• reset-passwords (1)** *one-at-time (1)* **• social-engineering (1)** **• inconsistent (1)** **• customer-support (1)** **• deleted-file (1)** **• account-creation (1)** **• purchase-replacement–tool (1)** **• unable-to-update-passwords (1)** *forgot-login-info (1)* **• system-hog (1)** **• login-info (1)** *not-compromised (1)* **• synchronization-skills (1)** **• customer-service (1)** **• constant-updates (1)** **• already-installed (1)** **• phishing-attack (1)** *employee-opened-email (1)* **• restrictions (1)** **• credit-card-verification (1)** **• no-dark-mode (1)** **• convenient (1)** **• not-everything-will–work (1)** **• easy-to-switch (1)** **• mouse-clicking (1)** **• typing (1)** **• stop-saving-passwords (1)** **• remember-other-details (1)** **• ensure-import-works (1)** **• don't-care (1)** **• delete (1)** *data (1)* **• simpler (1)** **• locked-notes (1)** **• not-influenced (1)** **• prompts-generation (1)** **• dual-support (1)** **• easy-transition (1)** **• stay-up-to-date (1)** *breaches (1)* **• encode-passwords (1)** **• fail-to-update-changes (1)** **• response-time (1)** *actual-issue (1)* **• intuitive (1)** **• no-breach (1)** *import (1), export (1)* **• customize-passwords (1)** **• application (1)** **• not-consistent (1)** **• bad-memory (1)** **• communicated (1)** **• insecure-passwords (1)** **• information-sold (1)** **• maintenance (1)** *not-everything-working (1)* **• secure-passwords-file (1)** **• stole-username (1)** **• collects-data (1)** **• reddit (1)** **• no-password-synchronization (1)** **• cancellation-process (1)** **• breached (1)** **• portable (1)** **• new-accounts (1)** **• use-cheap-pm (1)** **• credit-monitoring (1)** **• not-accessible (1)** **• choosing-pm (1)** *availability (1)* **• lost-info (1)** *sensitive-personal-info (1)* **• easy–to-update (1)** **• use-new-pm (1)** **• wrong-updates (1)** **• availability (1)** **• use-open-source (1)** **• time-consuming (1)** **• fails-to-popup (1)** **• notebook-more-secure (1)** **• internal-breach (1)** **• avoid-switching (1)** **• gather-data (1)** **• more-efficient (1)** **• forgot-password (1)** **• ownership (1)** **• lost-merit (1)** *reoccuring-breach (1)* **• reputation (1)** **• write-down (1)** *passwords (1)* **• paid-service (1)** **• used-tools (1)** *transferred (1)* **• make-process-easy (1)** *not-manual (1)* **• uninformed (1)** *breach (1)* **• lawsuit (1)** *potential-fiscal-payback (1)* **• not-using (1)** *PM (1)* **• loss–customers (1)** **• take-time (1)** *transition-bit-by-bit (1)* **• not-impacted (1)** *breach (1)* **• self-hosting (1)** **• password-vuln (1)** **• fee-structure (1)** **• popup (1)** **• authenticator-upload (1)** **• money (1)** **• strong-passwords (1)** **• removal (1)** *dual-use (1)* **• ransomware (1)** **• viewing-passwords (1)** *prior-to-transferring (1)* **• data-entry (1)** **• phone-skills (1)** **• help-section (1)** **• compatible (1)** **• safety (1)** **• compatibility-issue (1)** *operations-systems (1)* **• efficiency (1)** **• lack-security (1)** **• use-multiple-sites (1)** **• disliked-service (1)** **• passwords-leaked (1)** **• password-vault (1)** **• security-notifications (1)** **• less-features (1)** **• distracting (1)** **• sign-in (1)** *apple-account (1)* **• no-ads (1)** **• data-leaks (1)** **• saves-without-consent (1)** **• syncing (1)** *multiple-devices (1)* **• inconvenience (1)** **• data-deletion (1)** **• stopped-using (1)** **• familiarity-with-system (1)** **• sync-without-upload (1)** **• ensure-passwords-correct (1)** **• usernames (1)** *large-amount (1)* **• fills-wrong-password (1)** **• unsure-about-password-leak (1)** **• reassuring-users (1)** *do-better (1)* **• only-on-first-time (1)** **• password-not-accessed (1)** **• predicted-breach (1)** **• no-auto-fill (1)** **• keylogger (1)** *store-login-info (1)* **• security-superior (1)** *apple (1)* **• difficult-to-learn (1)** **• not-transparent (1)** **• quick (1)** *easy (1)* **• authentication-codes (1)** *not-reset-passwords (1)* **• breach (1)** **• unaccessible-passwords (1)** **• selling-data (1)** **• didn't-have-to-do-anything (1)** **• prompting (1)** *not-relevant-passwords (1)* **• password-storing-process (1)** *similar (1)* **• overstated-practices (1)** **• just-as-safe-other-pms (1)** **• not-challenging (1)** **• deleted-prev-pm (1)** **• not-shareable (1)** **• did-not-use (1)** **• apple-universal (1)** **• fraud (1)** **• standard-process (1)** **• job (1)** **• dark-web (1)** *personal-info (1)* **• browser (1)** *restricted (1)* **• not-managed (1)** **• excel-knowledge (1)** **• bad-press (1)** **• not-complex (1)** **• challenges-updating-apps (1)** **• vuln-knowledge (1)** **• process-perfect (1)** **• hardware-specific (1)** **• vault-password-accessed (1)** **• save-file (1)** *csv (1)*