Why people (don't) use password managers effectively

Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University
spearman@cmu.edu, shikunz@cs.cmu.edu, {lbauer, lorrie, nicolasc}@cmu.edu

Abstract

Security experts often recommend using password-management tools that both store passwords and generate random passwords. However, research indicates that only a small fraction of users use password managers with password generators. Past studies have explored factors in the adoption of password managers using surveys and online store reviews. Here we describe a semi-structured interview study with 30 participants that allows us to provide a more comprehensive picture of the mindsets underlying adoption and effective use of password managers and password-generation features. Our participants include users who use no password-specific tools at all, those who use password managers built into browsers or operating systems, and those who use separately installed password managers. Furthermore, past field data has indicated that users of built-in, browser-based password managers more often use weak and reused passwords than users of separate password managers that have password generation available by default. Our interviews suggest that users of built-in password managers may be driven more by convenience, while users of separately installed tools appear more driven by security. We advocate tailored designs for these two mentalities and provide actionable suggestions to induce effective password manager usage.

1 Introduction

Despite years of searching for viable alternatives, text passwords remain as ubiquitous as they are challenging and frustrating for most internet users. Experts often recommend password managers that combine secure password storage and retrieval with random password generation. These are seen as tools that can improve account security while also improving the usability and convenience of text password authentication [40]. However, use of separately installed password managers still seems to be relatively uncommon. Previous studies have suggested that many users are not certain what password managers are, how to use them, and/or whether they are trustworthy [1, 40].

We describe a 30-participant interview study with people who do not use password managers at all, people who use password managers built into their browsers (e.g., Chrome) or operating systems (e.g., Apple Keychain), and people who employ separately installed password-manager applications. Our findings emphasize tradeoffs between convenience and security in password management and password-manager adoption, and we confirm and contextualize multiple barriers to adoption and effective usage that have been described in previous work [1]. We also highlight factors that we do not believe have been discussed previously, including confusion about the source of browser password-saving prompts and about the meaning of "remember me" options.

Furthermore, previous work has indicated that users of separately installed password managers are more likely to use unique, strong, randomly generated passwords, while users of built-in password managers may be more prone to weak passwords and password reuse. Lyastani et al. discussed that these patterns may result partially from separately installed password managers more often having integrated generators [26]. We present evidence of differences in initial motivations that may also contribute to these reuse patterns. We also provide actionable suggestions to target the three aforementioned groups of participants and induce effective password-manager usage.

2 Related Work

We summarize prior work on users' password habits and management choices as background for our work. We also

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.

describe studies that have explored adoption of password managers, as well as problems with password managers that might hinder their effective use.

2.1 Password Habits and Management

Studies exploring people's current password habits and burdens [15, 31, 40] provide crucial context in understanding users' password-management choices. The typical user has been estimated to have between 16 and 26 password-protected accounts in active use [11, 31, 44], and recent reports indicate that the average workplace password-manager user may have hundreds of accounts [16]. Password reuse can have serious consequences for users and organizations affected by data breaches [7, 22, 28, 30, 34, 43]. Experts thus recommend using unique, strong passwords for all accounts [21] or at least for high-value accounts [42].

However, users often struggle to remember passwords, especially infrequently used passwords [13, 40], passwords created under certain types of website requirements [36], and randomly generated passwords [45]. Users cope with these demands in part by frequently reusing passwords across multiple accounts [9, 26, 31, 44]. Along with memorability challenges, users' inaccurate perceptions of password strength and difficulty entering long or complex passwords on mobile devices also lead them to create weak passwords [27, 42]. All of these factors make a strong case for password managers.

2.2 Password-Manager Adoption

Security experts often recommend password managers with storage and random-generation features to help users employ strong and unique passwords without incurring memorability issues [5, 19, 20]. However, previous studies have showed password managers (particularly stand-alone applications) suffer from low adoption rates [38, 40], especially among non-experts [21, 41]. Using in-depth semi-structured interviews, we explore possible reasons for low password-manager adoption rates, as well as non-expert users' understandings and opinions regarding approaches to password management.

In 2014, Stobert and Biddle conducted 27 semi-structured interviews to examine the "life cycle" of password use. They found the rationing of effort to be a central theme in users' password-management choices. Almost all of the participants in this study reported using password managers built into web browsers, but none were using separately installed password managers [39]. Our study uses a similar interview approach to explore themes including users' strategies for creating and managing their passwords, with the intuition that the password ecosystem may have become more complex for some users since 2014. Furthermore, we intentionally sought out users and non-users of password managers in order to examine what factors drive them to adopt or not adopt these tools.

Alkaldi and Renaud conducted a web survey as well as analyzed reviews for password-manager apps in the Google Play Store and broadly listed many observed reasons for adoption and non-adoption [1]. Fagan et al. surveyed 248 people on MTurk to probe their reasons for using or not using password managers as well as their emotions associated with the usage of password managers. Similarly to the work by Alkaldi and Renaud, this survey asked participants, in an open-ended question, why they chose [not] to use a password manager. This work also provides a number of broad reasons including "security concerns," "lack of need," and "lack of motivation/time." They found that password-manager users tend to regard "convenience" and "usefulness" as their main reasons for adoption, and "non-users" are more likely to feel suspicious compared to "users" [10]. Similarly, Aurigemma et al. conducted a survey with 283 undergraduate students who reported they did not adopt password managers because they lacked time for installation, the sense of urgency, or the awareness of how password managers worked [3]. Alkaldi and Renaud also conducted another study to test an Android application to recommend password managers to users and found that such an intervention may be most effective when it appeals to users' autonomy (sense of control) and relatedness (sense of community with others) [2]. Our study complements these studies with interviews to present a more comprehensive picture of why and how people arrive at their decisions of using or not using password managers.

2.3 Problems with Password Managers

In 2006, Chiasson et al. studied two password managers and identified several usability issues caused by: i) users' incorrect or incomplete mental models of the tool, and ii) users' feelings that they did not need password managers and unwillingness to hand over control [6]. In 2011, Karole et al. evaluated the usability of password managers running on a website, on a mobile device, or on a USB device. They found that non-technical users preferred to manage passwords on their mobile devices rather than relinquish control to a web-based password manager [23].

Besides the aforementioned usability issues, prior work has highlighted some security vulnerabilities in password managers, although experts generally still consider password managers a net positive [12, 18]. Li et al. identified various vulnerabilities associated with five popular web-based password managers [25]. Silver et al. revealed risks of the auto-fill functionality provided by many popular password managers [37]. Research has also indicated problems with local data security. Gray et al. revealed that unencrypted password data could be found in temporary folders [17]. Belekno et al. [4] and Gasti et al. [14] described risks that exist when attackers possess physical access to users' devices or password databases.

In 2018, Lyastani et al. collected *in-situ* password data of MTurkers through a Chrome plug-in. They found that

Chrome's autofill seemed to encourage password reuse, while users of LastPass' integrated generator tended to have stronger and less-reused passwords [26]. Our study provides more insight about the mindsets of these types of users, as well as those of users who do not use any password tools.

3 Methodology

We conducted 30 semi-structured interviews to probe participants' current password behaviors as well as their attitudes, beliefs, and understandings surrounding password creation and composition, account security, and password management and storage.

3.1 Recruitment

We recruited participants from Pittsburgh, PA using both online outreach (posts on Craigslist, Reddit, and Facebook) and offline strategies such as posting flyers on community bulletin boards. We used purposive sampling to ensure that we interviewed participants who used a variety of password-management strategies, including non-technological approaches (e.g., writing passwords in a notebook), computer-based approaches that did not involve password-specific software (e.g., saving passwords in an Excel spreadsheet), password managers built into web browsers, password managers built into operating systems (e.g., Apple Keychain), and separately installed password managers. We stopped recruiting when our sample included multiple participants from each of the above categories. We also sought diversity in age, occupation, and level of technical knowledge.

Potential participants were asked to take a short screening survey to confirm eligibility (age 18 or older, able to speak English), availability, estimated number of internet accounts, types of devices used (laptop, desktop, smartphone, tablet, other), primary operating system(s) for those devices, password-management strategies, past experiences with compromised accounts or data breaches, and basic demographics.

3.2 Interviews

This research was approved by our university's institutional review board. Participants completed a consent form, were given the opportunity to ask the researcher questions before beginning, and were instructed that they could stop the interview at any time or decline to answer any question. The interview script is shown in Appendix B.

Participants were interviewed in person on our institution's campus. One primary researcher was present for all 30 interviews. A second researcher assisted in some interviews. Each interview lasted approximately one hour. At the end of the interview, each participant filled out a brief demographic survey. Participants received a $30 Amazon.com gift card.

With participants' consent, all interviews were recorded, and the recordings were then transcribed by a commercial transcription service. Participants were asked not to share actual passwords or other identifying information, but when participants did mention details that seemed likely to be sensitive or identifying, the recordings were trimmed of those details before being sent to the transcription service.

3.3 Analysis

Interview transcripts were analyzed using inductive coding. An initial codebook was created based on the interview script and early interviews, and two researchers collaborated iteratively to improve the codebook throughout the coding process.

Five of the 30 interviews were coded by both researchers to ensure inter-rater reliability. The average Cohen's kappa, a commonly-used statistic reflecting agreement among coders, was 0.84, which denotes a very high level of agreement [24]. All coding discrepancies in these five interviews were discussed and reconciled. The remaining interviews were coded independently (10 by one researcher and 15 by the other); however, the researchers met regularly throughout the process to discuss any perceived ambiguities in the coding of particular data points as well as any necessary changes or additions to the codebook. These methods were deemed sufficient given that the results reported are qualitative and exploratory.

The final codebook contained 309 total codes across 59 categories. Most categories reflected a particular question or topic from the interview script and the types of responses observed to that question: for example, one category of codes called "current password management" included codes such as "physical notebook" and "browser password manager." A "miscellaneous" category also captured certain high-level themes that were observed repeatedly, e.g., "device sharing."

3.4 Demographics

We interviewed 19 users who identified as female and 11 who identified as male. Four were 18–24 years of age, nine were 25–34, eight were 35–44, five were 45–54, three were 55–64, and one was between 65 and 75. Most users were highly educated: 21 had bachelor's degrees, and nine of those also had graduate degrees.

Nine users worked in technical fields. We sought to interview a more representative sample, but we encountered difficulty in recruiting users of separately installed password managers when we excluded those with technical backgrounds. Only two participants self-identified as security professionals.

3.5 Limitations

We emphasize that this study is qualitative and based on a purposive sample, and we are not making any quantitative comparisons or claims. Our population sample skews female and

young, and most of our participants had bachelor's degrees or higher. We also had a disproportionately high percentage of participants with technical backgrounds, largely because we found it difficult to recruit users of separately installed password managers who did not have technical backgrounds. We do not claim any generalizable statistical findings from this study: our goal is to describe some of the user types to consider when designing and marketing password managers, as well as some of the barriers to adoption and effective use.

Due to our screening survey and purposive sampling methods, participants likely came to the interview believing that we were security researchers interested in password-management tools. This could raise concerns about priming and the Hawthorne effect, i.e., that participants might indicate more affinity for password managers than they actually had. Nonetheless, many participants still told us about habits that they knew were not considered secure and about reasons that they did not like or did not want to use password managers.

We also acknowledge that users may not have been able or willing to self-report their password habits accurately in all cases. However, in complement to existing in-situ data, these self-reports offer crucial insights regarding the mindsets underlying users' observed behavior.

4 Results

Many of the users interviewed had complex password strategies, including multiple password-storage methods. However, we have categorized interviewees based on whether their primary approaches to remembering passwords depend on non-password-specific methods, built-in password managers, or separately installed password managers. Here we describe how these groups characterized their current password habits and their attitudes towards password-management options.

4.1 Password-Management Approaches

Approaches Not Involving Password-Specific Tools The first group of participants that we will discuss used approaches that did not involve any type of tool designed specifically for password management as their primary method. This includes memorizing passwords, writing passwords (or hints to passwords) on paper, sending oneself emails or voicemails containing passwords, listing passwords in unencrypted computer files (e.g., a Microsoft Word file), or listing passwords in note-taking applications (e.g., iPhone Notes app). Some participants also relied heavily on the ability to reset forgotten passwords. Nine interviewees were in this group.

Some of these participants had used password managers incidentally or in the past. P27, for example, reported that he was able to log into a few apps on his Android smartphone with his fingerprint, suggesting he was likely using Google Smart Lock to a limited degree. However, his primary strategy was to memorize his passwords. P28 also had some passwords that were saved in the browser on an infrequently-used home computer, but she reported that these were outdated and that she did not save passwords when prompted anymore.

Built-In Password Managers The second group of participants discussed below primarily used password managers built into browsers (e.g., Apple Safari, Google Chrome, and Mozilla Firefox) or operating systems (e.g., macOS Keychain Access & iCloud Keychain, or Google Smart Lock for Android and ChromeOS) to store and autofill some or all of their passwords. The distinguishing feature of these tools versus other password-management tools discussed below is that they are present in the browser or the operating system as standard features. To access these tools, users may need to install browsers that are not built into their operating systems, but they do not need to install additional password-specific applications or extensions. Twelve belong in this group.

In many cases, browser-based and operating-system-based tools from the same company are integrated with each other: for example, passwords saved in Safari may be viewed in Keychain Access on macOS and may be set up to sync to the cloud and to iOS devices using iCloud Keychain (all Apple products). For this reason, we discuss all of these built-in tools together rather than distinguishing browser-based tools from operating-system-based tools.

Separately Installed Password Managers The third group of participants that we will discuss are those who used some type of separately installed password manager, i.e., tools that are not built into browsers or operating systems and must be installed as separate applications and/or browser extensions. We interviewed seven users in this group: four users of 1Password, two users of LastPass, and one user of KeePass.

Other Approaches Two participants were difficult to place in the aforementioned categories. P29, who described his approach as "security by obscurity," reported using a combination of memory, mnemonics, and browser password storage to handle passwords on a routine basis, but he mainly stored his password list using an application called Cardfile that he described as a "Windows 3.1 executable." He updated this file manually on a home machine running Windows XP. P21 created his own encrypted file using PGP to store his passwords, and accessed them through SSH when at work.

4.2 Current Password Habits

Account Numbers When asked how many password-protected accounts they had, almost all participants (except for five users of separately-installed password managers) gave answers under 100. Most of the participants who do not use password managers gave an answer under 50, and two reported having more than 50 but under 100 accounts. For users

of built-in password managers, estimates most commonly ranged between 15 and 50 accounts. For users of separately installed password managers, the five with technical jobs all reported having well over 100 password-protected accounts, with one reporting having over 1000 accounts. The remaining two users reported having 20-50 accounts.

Password Reuse Of participants who do not use password-management tools, seven indicated multiple risky password habits, including heavy reuse of passwords and few or no unique passwords. However, one user reported that none of her passwords were reused exactly but that she did reuse substrings when creating passwords (although always in different positions in the passwords). Another user reported that most of his passwords were unique but also reported that his strategy for creating passwords was to use words related to "kids," "names," cities, or states, and then add numbers, which suggests that his passwords may have been highly guessable.

Only one participant who primarily relied on built-in password managers specifically reported efforts to have unique passwords for all important accounts. About half of the other built-in password-manager users indicated heavy reuse of one password for all of their accounts. The rest employed various strategies to decrease the extent of their password reuse: some applied a tier system, using a unique password for accounts of similar importance, and some tried to have unique passwords for important accounts but still engaged in insecure practices like reusing parts of their passwords or using memorable personal information in their passwords.

Of the seven participants who use separately installed password managers, all but one reported switching to password manager use gradually, with only one participant (P23) reporting an effort to change all passwords to randomly generated, unique passwords at the start of using a password manager. P23 reported that this took at least five hours over the course of about three days to migrate the 40 accounts that he had at the time, which was three to four years prior to the interview. (At the time of the interview, he estimated that he had about 300 accounts.) Another participant (P19) did not commit to changing all of his passwords at the beginning. After one of his reused passwords was phished, he updated hundreds of his passwords to be unique and randomly generated.

Password Generators Only one of the users who relied primarily on built-in password managers described using password-generation features. P10 reported using Safari's password-generation tool to create random passwords for important accounts. She used Apple's Keychain functionality to record and fill these passwords. (She described reusing a weaker password across some low-value accounts.)

She indicated a recent account breach as the impetus for this strategy: previously, she had been reusing many of her passwords, and then an attacker gained access to a department store account as well as her email. She described this as a traumatic experience that caused an immediate desire to change her habits:

> All of my information was just taken. It was awful, so I'm having to get a new debit card for everything, having to get new credit cards... That's when I realized that I needed to reevaluate. That's when I changed every single password that I had to random digits. I didn't even think twice. I was like, "Something needs to change, and it has to change on my end."

At the time of these interviews, Safari did offer a password generator, but the six other participants who used Safari on some of their devices did not report use of this feature. Google Chrome began to roll out Chrome 69, which included a new password-generation feature, in fall 2018 [8, 33]. Some of our interviews were conducted after the release of Chrome 69, but no Chrome users mentioned awareness or use of the feature.

All seven users of separately-installed password managers reported using randomly generated passwords when creating new accounts, and most of these participants used unique passwords for newly-created accounts (with the exception of P22, whose strategy is described in more detail below). P30 reported using websites to generate random passwords before realizing that LastPass had that ability.

P22's strategy was distinct from that of the other participants. First, he did not use the password generator built into 1Password: he instead preferred to use other generators such as one offered by Symantec, which he reported was simply a matter of "habit." Second, he did not use the generated passwords in their original form, but instead made changes of his own by adding characters in the middle and/or removing some characters before saving the passwords in order to make them "more secure" and "more random."

Additionally, P22 reported that he reused passwords in tiers rather than storing unique passwords for accounts. For example, he reported that he might use the same password for all social media accounts. He did this out of worry that he might not have access to his password manager in certain situations or if borrowing someone else's device.

Master Passwords The seven participants who use separately installed password managers employed a number of different approaches to deal with their master passwords. All but one of those seven (P20) reported using a unique password as their master password. P20 reported that her master password was one of her three heavily reused passwords. Some participants (P18, P23) reported using passphrases as their master passwords, like "a quote from a movie" (P23) or "a sentence that doesn't make sense" (P18). Some (P17, P19, P22, P30) indicated that their master password was randomly generated. P17, P19, and P22 used 1Password, which prompts users to memorize a randomly generated master password when creating an account. P30, who used LastPass, reported

using a website to generate a random master password, but was unable to memorize it. She kept written copies at home, at work and saved it in a draft inside her email account. P20 and P30, who engaged in unsafe practices regarding their master password, did not have technology-related degrees or technology-related jobs.

4.3 Experiences of Participants Not Using Password Managers

Nine participants were not using any password-specific technology or tools to help them manage their passwords. Some participants without password managers were satisfied with their password-management approaches, but others were concerned about password security or found their current approaches inconvenient.

Satisfaction with Current Method Some participants who were not using password-specific tools liked specific aspects of their current password-management methods, which may inform efforts to target password-management tools to people who currently do not use such tools.

P11 and P27 noted that password reuse made it easy for them to remember their passwords. P11 noted that this was due to always using a default password. P27 noted, "it's easy because I've been using the same variations for a while... It's like my phone number. I know it without thinking about it."

P4 liked keeping a copy of her passwords outside of her browser because she felt that passwords stored in a browser password manager might be lost—e.g., if the IT department at her workplace had to wipe a computer during troubleshooting.

Some participants liked having control over how their passwords were organized. P4 kept them in alphabetical order with notes about the account they belonged to, while P7 kept them grouped by type of account.

P12 liked keeping his passwords in a list in a note on his phone because he could bring this list with him anywhere. He mentioned not being aware of how else he could have access to his passwords on the go.

Dissatisfaction with Current Method Some participants in this group did like aspects of their current method of storing passwords. However, five participants were dissatisfied with their current password-management methods, and several participants described negative aspects of their current methods, including recall difficulty, disorganization, access problems, and potential security risks.

Some participants emphasized that it was difficult to recall their passwords. P28 talked about having to reset passwords "constantly" due to forgetting them. As mentioned above, P27 said that it was generally easy to remember passwords that he had reused for a long time, but he also encountered difficulties when trying to remember what password variation he had used for a particular websites' password requirements:

> It can be hard because I don't remember if a website wanted me to have a capital letter or if they wanted me to have a symbol or if they wanted at least 12 characters.

While some participants liked how they organized their password lists in paper notes or in files, P26 felt like her system of using her memory as well as writing a few passwords down was "disorganized":

> I put a lot of energy into trying to remember what's what. I'm like, "I could be doing something else with that energy."

P4 described problems with accessing accounts when away from where her password list file was stored. She kept a Microsoft Word file on her computer and also kept a printed copy, but she did not carry a copy with her on paper or on her phone. She felt that carrying passwords with her was risky.

> I could [keep the list on my phone]. And I could email it to myself too but... I feel like you're putting more risk when you do all those things. I mean, what's the point of having passwords if you're gonna carry them on your body and say, "Hey, this is my password." You know. But yeah, I can't always access them, to be honest.

Some participants who stored passwords in files or digital notes expressed concern that an unauthorized user of one of their devices might be able to access these password lists. P4, who kept passwords in a Microsoft Word file, said, "It's on the computer, which I know is really bad. But I don't name that 'passwords' on the computer. Just in case somebody got on my computer."

P12, who stored passwords in a note that was saved only on his iPhone, was concerned about what this would mean if his phone was stolen or used by someone without permission: "I know it's dumb, but I save them in my phone in my notes, so if someone has my phone, I'm through, right?"

4.4 Barriers to Adoption Among Participants Not Using Password Managers

Some users who were not using password-management tools were simply unaware that they existed. Additional barriers to adoption expressed by this group included security concerns, believing they did not have much to protect, concerns about the single point of failure, or past negative experiences with password managers.

Awareness Some users in this group did not believe they were using the best password-management methods, but they also were not sure if better options existed. P4, for example, said there could be a better way, but she was not aware of one, suggesting that sheer awareness of password-management

tools is the primary adoption barrier for some users. Similarly, P14 wished for "an easier way to remember passwords, like a universal-type system."

Security Six out of the nine participants expressed various concerns about the security of password tools.

Some expressed concern or lack of knowledge about the security of password managers. P12 noted that he would need to learn more about their security. P11 wondered if password managers were "really safe and secure" and described generally preferring "pen and paper" due to being "leery of technology." P11 wanted to know where and how password managers stored passwords, as did P27.

Some participants had considered using browser password features but were uncertain about their security. P26 described declining browser prompts to save passwords because "it feels insecure." P28 had stored passwords in Chrome in the past and said it felt easy, but she stopped because she was not sure whether Chrome stored passwords securely.

P11 also described confusion about who or what was prompting her to store passwords in her browser:

> I don't know if it's Google that's asking me, I don't know if it's the website that's asking me... that would be one reason [to not save passwords].

Some participants were reluctant to use password managers due to concerns about specific types of attackers, including external attackers (i.e., "hackers"), employees at password-manager companies, and other users (authorized or unauthorized) of their devices. P14 worried about important accounts being hacked if their passwords were saved:

> I'm afraid that if I use it, I might be sorry in the end. I might have a hacker get into my system. You know? Some people have nothing to do and they'll just hack into people's computers for no reason. This is just kind of like insecurity.... I use it [Chrome's password manager] for certain accounts... but I don't think I'd use it for my email or my bank...

P27 expressed concerns that employees at a company offering a password manager might be able to decrypt and access his passwords. P27 was also concerned about other users of his device accessing his accounts, as were P4 and P11.

Not Enough to Protect Three participants felt that they did not have enough accounts or that their accounts were not valuable enough to require a secure password-management tool. P5 and P27 felt that they were able to remember their passwords without help.

> My life on the Internet is not that complicated with my 15 passwords that I can more or less remember and my little book. But if it were to get anymore complicated than that if I were to have dozens of accounts, then yes, I would.... I would think that there's a far superior way to deal with passwords if you were using a huge number of them. (P5)

P5 and P12 felt that their accounts were not sufficiently high-value to require extra security like that offered by a password manager. P5 said that she might use one if some accounts were protecting more important financial information. P12, who mentioned he used prepaid credit cards for online purchases instead of cards connected to bank accounts, said he might consider using a password manager if he had bank accounts or medical records to protect.

Some participants had trouble conceptualizing the mechanisms of "hacking" or the statistical risk of their own accounts being compromised. P7, for example, when discussing his use of a website from which 340 million records were exposed, believed that the probability of his own information being exposed was "one in 340 million" and thus was not very concerned: "I don't care... I'll take that risk anytime. I'm more likely to walk out of here and get run over by a car, right?"

Single Point of Failure Some participants worried about storing all of their passwords in one place. P27 was concerned about security: "If somebody found out the way that they encrypt it, they would be able to get access to all my passwords at once instead of one of my passwords." He also worried that it would be difficult to create new passwords if all of his passwords needed to be changed. P11 and P26 were afraid of losing access to all of their passwords due to a forgotten master password or other problem.

Past Negative Experiences Three participants in this group had negative experiences with password managers before. They were unable to reliably store their passwords using those tools. P4 reported that Google Chrome had sometimes saved her passwords incorrectly, such as with a lowercase letter rather than uppercase. She also recalled losing passwords stored in her phone after clearing the browser cache. Similarly, P14 said that she had tried to use Chrome's password manager in the past but that "it mostly doesn't work out." She said it saved her personal information, such as her address, but that it did not save her passwords: "Even though it says it's going to save it, it doesn't.... I wish it would save more."

P28 had experienced trouble with password managers in the past because she changed her passwords frequently: she described cases in which the browser would fill in the old password and cause failed logins. P28 had also tried briefly to adopt LastPass, but she found master password creation to be a "hurdle": "the last thing I would want is to have a database with all your passwords with a dumb [master] password."

4.5 Experiences of Users of Built-In Password Managers

Of 12 participants who were using a password manager built into a browser or operating system, half (six) reported that they were not satisfied with their current password-management choices. P3 said, "I know there should be a better way." Two participants were uncertain and expressed wishes for an easier or safer way to manage passwords.

Participants generally reported adopting built-in password managers due to seeing prompts or for reasons of convenience, and the aspects of these tools that they liked included convenience-focused features such as autofill. These participants did not report choosing these tools for reasons of security. In many cases, they believed that their password habits were risky—probably correctly, since most of them reported significant password reuse—but did not feel motivated to change those habits and were not aware of features such as password generators that would assist them in doing so.

Likes Almost all participants emphasized liking autofill. P16 reported that it saved time, and P24 enjoyed the convenience of not having "to always type in a password."

P25, who was more familiar with Chrome's features than other users, liked that Chrome allowed her to sync passwords across devices and protect her passwords with multi-factor authentication.

In addition to any comments about password-management tools, half of the participants in this group mentioned that they liked reusing passwords because it allowed them to remember their passwords easily. P3, for example, said:

> It's a no-brainer. I don't have to think about it, I just automatically do it. I'm 68 years old and I don't want to have to remember more than I have to.

Dislikes Four participants (P3, P6, P15, and P24) expressed concerns over other people having access to passwords that they saved using built-in tools. P6, for example, was worried that her child's friends, who she said borrowed her computer sometimes while visiting her house, might make online purchases using her accounts.

One other complaint is the accessibility of passwords on devices that the passwords were not saved to (P2, P6).

> Auto-fill is awesome. I'm starting to rely on that more and more. It's just if you don't have that device... and you're somewhere else when you need it, that's the only downfall I can see. (P2)

Ten out of the 12 participants did not know or believe that their password manager allowed them to view a list of all passwords, although Chrome, Firefox, and Safari do offer this. Four participants (P2, P6, P9, P13) emphasized that they would like the ability to view all of their saved passwords.

P15 pointed out that sometimes the built-in tools did not update her passwords when she changed them.

Factors in Adopting Built-In Password Managers No participants mentioned security or unique passwords or randomly generated passwords as a reason for adopting a built-in password manager. Users in this group all focused on prompts, convenience, or memory limitations as adoption factors.

Nine out of 12 participants in the group remembered receiving prompts from the tool offering to save passwords for them. Seven quickly accepted these prompts, and these users gave no other particular reason for their adoption of the tool. Two participants (P1 and P25) were slower to accept those prompts. P1 mentioned that she finally decided one day to click "yes" when she was feeling "lazy." P25 said that she was skeptical about letting Chrome save her passwords but that she felt more comfortable after hearing that her friends liked Chrome's password manager and found it to be convenient.

Six participants emphasized convenience as a reason for using the built-in tool, emphasizing benefits such as "faster" log-ins. P2 mentioned that forced password changes made it hard for him to remember all of his passwords on his own.

4.6 Barriers to Effective Use Among Users of Built-In Password Managers

Users of built-in password managers often adopted them for reasons of convenience or due to seeing prompts. Accordingly, they often did not use them in effective or secure ways because they (perhaps incorrectly) believed themselves to be at low risk or because they did not have sufficient knowledge.

Risk Assessment Like many of the participants who were not using password-management tools, the 11 participants who stored reused passwords in their built-in password managers were often reluctant to change their habits because of a lack of personal experience with account compromise, a perception that they were at low risk of account compromise, or a belief that an account compromise would not have important negative effects.

Eight of the 11 participants who stored reused passwords in their built-in password managers acknowledged that their password habits put them at some risk. However, P1, P8, and P25 said they were not likely to change their behavior since they had not experienced negative consequences so far.

> Yes, it's a bad idea to have all the passwords like to be very similar, but I think that because I haven't been personally affected by someone... hacking me or changing or grabbing my info... I'm less inclined to change the way I manage my passwords. (P1)

P10, the only built-in password manager user who was using randomly generated passwords, reported that she also

had not believed herself to be at risk of account compromise until she experienced it first-hand:

> Not really, because I hadn't really experienced anything like [being hacked]. It was just...a complete eye-opener. I was like, "Nobody's ever going to hack anything, nothing." Completely naïve.

Another two participants (P3 and P9) did acknowledge risk in their behavior but also felt that their accounts were not of much value. Both of them were aware of password managers, and one had even used a separately installed password manager previously. P3 explained that she only shopped online for "tiny things" and that her wife, who handled most of their finances, had more reason to be concerned about passwords.

P9 claimed that she did not have much to lose: "[T]hey can have my bank account; there's not that much money." P9 was one of a few participants who mentioned that they were more careful with other people's information than their own: she described having better password practices when she was working in a university job where she was responsible for research data on her computer.

Lack of Awareness or Knowledge As we find in participants who do not use password managers, lack of knowledge remains an obstacle for built-in password manager users. Four out of 12 participants were not aware of the term at all, and only one (P16) expressed awareness of separately installed password managers.

Furthermore, as discussed in Section 4.2, only one built-in password manager user used or was even aware of the password generation feature included in their password manager.

A lack of information also caused some of these participants to be reluctant to consider separately installed tools. After the interviewer offered a description of available password management options, three participants (P2, P3, and P13) expressed concerns about password managers from unfamiliar companies. P2 said that he might use a tool offered by a known company like Google but that he would be "leery" of a "new-name company":

> Any kind of third party scares me a little bit. I don't know who or what is doing that part of it, and what information is shared out there.

4.7 Experiences of Users of Separately Installed Password Managers

Five separately installed password-manager users (P17, P18, P19, P22, and P23) reported that they were satisfied with their password managers, but the two users without technical backgrounds (P20 and P30) had less positive perceptions. P20 referred to her password manager as "a pain in the ass" but was not convinced a better solution would ever exist.

> There's not going to be a better solution, I'm going to not store them occasionally, and I'm going to have to call and get someone to reset them... That's just the price that we pay to keep those things.... I'm in public health, so we think about prevention instead of treatment, and this is the kind of thing where you're preventing things that are happening, but you're not seeing any rewards for it. So if I don't get hacked, I don't have a party because I don't get hacked. Whereas if I get hacked... I'm assuming that's a really negative experience.

Likes P18 and P23 appreciated no longer needing to memorize passwords. P17 and P30 also referred to generally liking that their passwords were stored or saved. A few participants also mentioned that they used their password managers to store information other than passwords. P22 found the ability to store SSH keys particularly useful.

P19, P23, and P30 liked being able to generate random passwords. P19 specifically liked having passwords that were not vulnerable to dictionary attacks and that would likely be slow for an attacker to crack. P30 also specifically liked that the password manager helped her use unique passwords.

P18 (a KeePass user) and P22 (a 1Password user) specifically liked having a desktop client. P23 liked the ability to sync across devices. P20 appreciated the portability of this system, or the ability to have passwords available "on the go."

P19 mentioned the ability to fill passwords without typing as an important feature, but he also specifically liked 1Password's implementation: "It doesn't pick random domains to fill in for a phishing website or something like that." [1]

Dislikes P17 said, "From a user experience standpoint, [1Password] is a mess," noting that it often did not save usernames or passwords correctly. She also reported that 1Password would sometimes fill a password without filling the corresponding email or username and would try to submit these incomplete credentials.

P30 said, "the [LastPass] app sucks," also citing issues with the browser extension not logging into websites correctly. P20 also encountered conflicts between Google Chrome's password manager and the LastPass browser extension: since she had saved some passwords in Chrome in the past, Chrome would still prompt her about filling or saving passwords.

P23 cited the difficulty of entering long, randomly generated passwords into certain devices that were not compatible with the password manager, such as gaming consoles or Roku streaming devices. P17 also mentioned that she would prefer to have shorter, easier-to-type passwords for certain

[1] 1Password's password filling functionality is different from most password managers in that it requires user instruction to trigger the filling of a password. 1Password prefers not to refer to this as "autofill" and has made this choice for security reasons [32].

frequently-entered passwords, entry on mobile devices, or cases where the password manager was unavailable:

> I recently had to factory reset my phone, and I had to log into my Google account. And, if I hadn't had that password in my brain, then I would have to like go to my laptop, then open up 1Password, and then read this like 20 character string, and then type it... it's always so annoying.

P23 mentioned that 1Password's generator did not offer enough control to fit some websites' password requirements.

P18, a KeePass user, reported that it was "annoying" to have to sync his password database manually. He also mentioned KeePass's lack of cloud storage, and he noted that it was not easy to access his passwords from his Android phone. (At the time of writing, KeePass is available natively as a Windows client or portable application. To run KeePass on other operating systems such as macOS, Linux, or Android requires using an unofficial ported version [35].)

P20 and P30 feared forgetting their master passwords. P20 said, "I don't know if you can reset it if you forget it.... and there's something scary about that."

Adoption Motivations P20 and P30 cited memory limitations as a primary motivator. P30 had encountered memory difficulties after attempting to use unique passwords.

P18, P19, P20, P23, and P30 described a broad desire for increased security as an important motivator. P30's password-security concerns were heightened due to volunteer work in which she was responsible for other people's data. P22 also cited a specific desire to avoid typing in passwords manually (implying concerns about keyloggers) and a belief in password managers' use of "modern cryptography in encryption."

Information Sources P17, P18, and P19 gained awareness of password managers from working in IT or technology. P17's company encouraged password-manager use and paid for employees' subscriptions to premium versions of popular password managers, and P17 chose 1Password because IT staff at her company recommended it.

P20 specifically remembered hearing a story about password managers on NPR. P23 listed a number of possible places where he might have first heard about password managers, including Reddit and Hacker News.

5 Discussion

Our findings emphasize tradeoffs between convenience and security in password management and in password-manager adoption. We confirm and contextualize barriers to adoption and effective usage of password managers that have been covered in past work, while introducing additional factors. We also provide actionable suggestions to induce effective password-manager usage targeting three groups of users.

5.1 Security vs. Convenience

Tradeoffs and Effort Rationing A consistent theme that emerged from password-manager users and non-users alike is the tradeoff between security and convenience. Many of our participants reported making compromises about security in order to ration their efforts—even participants who were relatively concerned about security and who had fairly secure practices overall. Our findings echoed Stobert's work on password life cycles, which reported that "effort rationing" was a primary motivator of various password-related habits [40]. Multiple participants mentioned following recommended secure practices for higher-stakes accounts (e.g., financial), while employing reused and/or weak passwords for lower-value accounts. Many also mentioned reusing passwords in tiers to ration efforts.

Furthermore, our study extended this line of reasoning to users of separately installed password managers, who were not present in Stobert et al.'s study. Password managers were sometimes described as solutions that saved memory effort and/or time, but in other cases, they were described by our participants as tools that required additional effort. When these tools do not function as intended, we see users ration their efforts by circumventing these inconveniences and resorting to other methods, which are often less secure. Users of separately installed tools would choose not to randomly generate passwords but reuse old weak passwords when user-interface problems made saving logins difficult, or would email passwords to themselves when syncing was not available. Users of built-in tools would resort to recording passwords on paper or in text files if they could not trust their browsers to save passwords reliably. We believe that there is a need for better user-experience design and thorough usability testing, especially long-term user studies for corner cases. We also observed that users without technical backgrounds may encounter more problems in their use of separately installed password managers, calling for tailored design and usability testing targeting non-expert users.

Motivations Lyastani et al. observed lower password strength and more reuse among users of browser password managers than among users of separately installed tools. The authors suggested that browser password managers, by not integrating generators with normal password creation workflows, potentially exacerbated password reuse [26]. Our results suggest that users of built-in password managers and users of separately installed password managers often have fundamentally different motivations and that differences between password-manager interfaces are not the sole cause of the reuse patterns Lyastani et al. observed. The majority of users of built-in password managers began saving passwords due to prompts or convenience, while users of separately installed tools emphasized security concerns, limitations in remembering unique passwords, and features such as generators

and strong encryption.

However, findings from our interviews do confirm Lyastani et al.'s suggestion that having a generator integrated into the workflow for password creation is beneficial. Many users of separately installed password managers found the generator convenient, while the majority of users of built-in password managers were not aware of the feature. It seems constructive to continue adding password generation features to existing browser password tools, as Apple (and, more recently, Google) have done. Furthermore, given how many users of built-in password managers adopted those tools due to prompts, we suspect that similar prompts towards password generation might be effective. We suggest that future work investigate what types of nudges are more likely to lead to password generator adoption (or other ways to improve password habits) among these more convenience-focused users.

5.2 Factors Driving Adoption

Our study provided additional evidence supporting some of Alkaldi and Renaud's findings about the adoption of separately installed password managers [1]. In particular, we found evidence of the importance of: subjective norms and social influence (supported by our findings of workplace influences on adoption of these tools), time-saving and memory benefits, past experience with security breaches, and perceptions of increased security.

Some of our findings, however, added complexity to Alkaldi and Renaud's results around adoption factors. Some of our users of separately installed tools, like theirs, reported that syncing was useful and desirable, but others found it not secure and/or not useful, implying that password-manager makers might want to continue to offer both cloud-based options with syncing and locally stored options that do not sync automatically. Furthermore, given their different backgrounds and needs, some participants found password managers effort-saving and easy to use, while others found them frustrating and unreliable, emphasizing that password managers must be designed to be usable for non-experts.

Our results also lend nuance to Fagan et al.'s findings that convenience and usefulness, not security, were the primary reasons for password-manager use [10]. Fagan et al. did not distinguish between users of built-in and separately installed password managers. Our results suggest that convenience and usefulness are indeed paramount for many users of built-in password managers, but that security is often a primary motivator for users of separately installed password managers.

5.3 Barriers to Adoption and Effective Use

Our work confirms and contextualizes many factors discussed by Alkaldi and Renaud as leading to rejection of separately-installed password managers [1], including lack of awareness, not enough passwords or important data, and concerns about security. Participants not using password managers and participants using built-in tools reported common themes like risk assessment and lack of awareness or knowledge.

We found that certain themes from Alkaldi and Renaud's work were especially salient in the discussion of password generators in our findings. In particular, participants who discussed not wanting to use randomly generated passwords often did so because they believed being able to "master" and memorize their passwords was important. P26 indicated that not knowing her passwords would feel like giving up control. P25 emphasized the importance of being able to access her information at all times and asked, "What's the point of creating a password if you can't remember it yourself?"

We also found some specific barriers that we do not believe have been discussed in other work. First, we found gaps in some participants' underlying understanding of websites, browsers, and password saving that precluded making informed decisions about using password managers. Some participants who had received prompts about browser password-saving features were unsure where the prompts were coming from: the browser, the website, or the computer. Participants were also sometimes uncertain where passwords would be stored or whether employees of the company making the password manager could see their passwords. Password managers should help people understand where their passwords are stored and what security measures are taken to protect their passwords in order to help them make informed choices.

Some participants also expressed confusion about password managers because they recalled checking "Remember me" options on login pages and not having their passwords saved. Multiple participants were confused about whether this option (which might normally either create a persistent login with a cookie or cause a username to be prefilled for subsequent page visits) was part of the browser password manager. These confusions lead users to lose trust in the reliability of those browser password managers, which propels them to resort to other insecure methods as mentioned in Section 5.1.

A few participants echoed concerns about having "all eggs in one basket," i.e., a single point of failure, which also appeared in Alkaldi and Renaud's survey responses. Some users of separately installed password managers also acknowledged this risk, but they felt that security benefits such as strong and unique passwords outweighed those concerns. Clear, accessible information about how password managers store and protect passwords may offer non-expert users a more accurate understanding of password managers' risks and benefits. Password managers that offer multi-factor authentication might also increase confidence for some of these users.

Targeting Non-Users Some people who were not using any tools to manage passwords were simply unaware of the existence of such tools. Some were uncertain about the security of those tools to protect from external attackers, thieves or others with unauthorized access to their devices, or other

(authorized) users of their devices. We suggest that further research might explore how advertising, education, or browser prompts could target those who are not currently using password tools, who may often be individuals who have less experience or expertise with technology. Accessible information should be offered that emphasizes not only security against remote attacks but also features that allow the user to control whether passwords are accessible to others with physical access to the device.

Furthermore, some participants using their own notes emphasized that they liked being able to sort passwords alphabetically or by category. Many separately installed password managers have robust sorting and retrieval capabilities for passwords and other types of information, and this may be feature that could be emphasized to target users for whom organization is a primary concern.

Multiple participants mentioned website guidelines on account creation pages were their main source of password knowledge, so we suggest that these guidelines could offer advice beyond password composition, including nudges to use password generators and password-management tools.

Targeting Users of Built-In Password Managers Given that prompts to save passwords seemed to be extremely effective for many of the users of built-in password managers that we interviewed, password-generation prompts might also be effective to nudge these users to adopt safer password practices. Chrome 69, released during the course of this interview study, introduced password generation prompts for signed-in Google users [8]. However, none of our participants mentioned awareness or use of this feature. At present (summer 2019), Chrome prompts users to generate passwords by default as long as they are signed in and have turned on password syncing, which may nudge more users to use randomly generated passwords.

We did encounter one user who was using Safari's password generator and was mostly satisfied, although she encountered problems when Safari's generator did not meet password requirements. Built-in generators will likely need to offer better compatibility with website requirements to increase usability and adoption, either by offering options to adjust length or character classes manually or by automatically conforming to website requirements.

Users of built-in password managers in our study generally did not know that there was a way to view their passwords after saving them. Chrome's latest UI does seem to make this more obvious by providing a link to passwords.google.com after a password is saved, which may improve usability.

With improved password generation tools, built-in password managers could be convenient *and* secure options for users who prefer not to install specialized tools. However, some interviewees were using multiple operating systems and/or browsers and could not rely on a single ecosystem like Apple's or Google's for password storage, and these users might adopt separately installed tools if they had sufficient information and confidence in the usability of those tools.

Targeting Users of Separately Installed Password Managers Current users of separately installed tools, as well as some participants who had tried and failed to use those tools, often portrayed the setup process as daunting. Many current users did not update all of their accounts to have randomly generated passwords at the time of adoption, but continued to use many reused and/or weak passwords, changing them gradually over time. Some password managers offer tools that attempt to replace weak passwords automatically, but none of our participants mentioned awareness or use of such features. Some password managers, including 1Password, intentionally do not offer such features [29], but if users are thus retaining large numbers of weak or reused passwords, password-manager makers may need to offer a feature to assist with improving existing passwords at the time of adoption.

Participants who were open to using separately installed password managers did not specifically report being deterred by cost. However, when we inquired regarding cost, most participants who were not currently using separately installed password managers were unwilling to pay for password management. These participants might be more likely to try built-in password managers or password managers with free versions, such as LastPass. Some said they might be willing to pay only if the tool was "very secure" or very usable, or if it offered special features such as identity theft protection. Most who were willing to pay for password management indicated that they would pay five dollars per month or less.

6 Conclusion

Our analysis of 30 interviews with non-users of password managers, users of built-in password managers, and users of separately installed password managers, confirms convenience, usability, and security concerns observed in past studies of password manager adoption. We highlight barriers not previously identified, such as confusion about the source of password prompts or the meaning of "remember me" options.

We find that users of built-in password managers are often driven by convenience, whereas users of separately installed password managers prioritize security, which may explain past findings showing higher levels of password reuse among users of built-in password managers. We call for tailored designs for these two mentalities. Future work should focus on ways to serve users whose primary task is not security and nudge them to use password generators without sacrificing convenience. Our results regarding user-interface frustrations also call for better usability testing and design for password managers, including more focus on non-expert users, as well as long-term field studies to reveal edge cases in which password managers may not function as intended.

Acknowledgments

This research was supported in part by the North Atlantic Treaty Organization (NATO) through Carnegie Mellon CyLab. We would like to thank Chelse Swoopes and Soraya Alli for their assistance with the study design and the interviews.

References

[1] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? In *Proceedings of the 1st European Workshop on Usable Security (EuroUSEC '16)*, 2016.

[2] Nora Alkaldi, Karen Renaud, and Lewis Mackenzie. Encouraging password manager adoption by meeting adopter self-determination needs. In *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS '19)*, 2019.

[3] Salvatore Aurigemma, Thomas Mattson, and Lori N. K. Leonard. So much promise, so little use: What is stopping home end-users from using password manager applications? In *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS '17)*, 2017.

[4] Andrey Belenko and Dmitry Sklyarov. "Secure password managers" and "military-grade encryption" on smartphones: Oh, really? Technical Report MSU-CSE-06-2, Elcomsoft Co. Ltd., https://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf, 2012.

[5] Andrew Chaikivsky. Everything you need to know about password managers. *Consumer Reports*, https://www.consumerreports.org/digital-security/everything-you-need-to-know-about-password-managers, February 2017.

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

[7] Catalin Cimpanu. Crooks reused passwords on the dark web, so Dutch police hijacked their accounts. *BleepingComputer*, https://www.bleepingcomputer.com/news/security/crooks-reused-passwords-on-the-dark-web-so-dutch-police-hijacked-their-accounts, July 2017.

[8] Catalin Cimpanu. Chrome 69 released with new UI and random password generator. *ZDNet*, https://www.zdnet.com/article/chrome-69-released-with-new-ui-and-random-password-generator, September 2018.

[9] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The tangled web of password reuse. In *Proceedings of the 2014 Network and Distributed System Security Symposium (NDSS '14)*, 2014.

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

[11] Dinei Florêncio and Cormac Herley. A large-scale study of password habits. In *Proceedings of the International World Wide Web Conference (WWW)*, May 2007.

[12] Geoffrey Fowler. Password managers have a security flaw. but you should still use one. *The Washington Post*, https://www.washingtonpost.com/technology/2019/02/19/password-managers-have-security-flaw-you-should-still-use-one, February 2019.

[13] Xianyi Gao, Yulong Yang, Can Liu, Christos Mitropoulos, Janne Lindqvist, and Antti Oulasvirta. Forgetting of passwords: Ecological theory and data. In *Proceedings of the 27th USENIX Security Symposium*, August 2018.

[14] Paolo Gasti and Kasper B. Rasmussen. On the security of password manager database formats. In *Proceedings of the 17th European Symposium on Research in Computer Security (ESORICS '12)*, 2012.

[15] Shirley Gaw and Edward W. Felten. Password management strategies for online accounts. In *Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS '06)*, 2006.

[16] Amber Gott. Lastpass reveals 8 truths about passwords in the new password exposé. *The LastPass Blog*, https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html, November 2017.

[17] Joshua Gray, Virginia N. L. Franqueira, and Yijun Yu. Forensically-sound analysis of security risks of using local password managers. In *24th IEEE International Requirements Engineering Conference*, September 2016.

[18] Alex Hern. Do we really want to keep all our digital eggs in one basket? *The Guardian*, https://www.theguardian.com/technology/2015/jun/17/do-we-really-want-to-keep-all-our-digital-eggs-in-one-basket, June 2015.

[19] Troy Hunt. The only secure password is the one you can't remember. *troyhunt.com*, https://www.troyhunt.com/only-secure-password-is-one-you-cant, March 2011.

[20] Troy Hunt. Passwords evolved: Authentication guidance for the modern era. *troyhunt.com*, https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era, July 2017.

[21] I. Ion, R. Reeder, and S. Consolvo. "...No One Can Hack My Mind": Comparing expert and non-expert security practices. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'15)*, July 2015.

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

[23] Ambarish Karole, Nitesh Saxena, and Nicolas Christin. A comparative usability evaluation of traditional password managers. In Kyung-Hyune Rhee and DaeHun Nyang, editors, *Proceedings of the 13th International Conference on Information Security and Cryptology (ICISC '10)*, Seoul, Korea, 2010.

[24] J. Richard Landis and Gary G. Koch. The measurement of observer agreement for categorical data. *Biometrics*, 33(1):159–174, 1977.

[25] Zhiwei Li, Warren He, Devdatta Akhawa, and Dawn Song. The emperor's new password manager: Security analysis of web-based password managers. In *Proceedings of the 23rd USENIX Security Symposium*, August 2014.

[26] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. Better managed than memorized? Studying the impact of managers on password strength and reuse. In *Proceedings of the 27th USENIX Security Symposium*, 2018.

[27] William Melicher, Michelle L. Mazurek, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Usability and security of text passwords on mobile devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*, 2016.

[28] ThreatMetrix Digital Identity Network. Cybercrime report 2017: A year in review. *ThreatMetrix,* https://www.threatmetrix.com/info/2017-cybercrime-year-in-review, January 2018.

[29] Lars Olsson. Automatic password changing. *1Password Forum,* https://discussions.agilebits.com/discussion/87083/automatic-password-changing, March 2018.

[30] Danny Palmer. This sneaky botnet shows why you really, really shouldn't use the same password for everything. *ZDNet,* https://www.zdnet.com/article/this-sneaky-botnet-shows-why-you-really-really-shouldnt-use-the-same-password-for-everything, May 2016.

[31] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*, 2017.

[32] Jamie Phelps. Does 1Password autofill input fields? *1Password Forum,* https://discussions.agilebits.com/discussion/62706/does-1password-autofill-input-fields, April 2016.

[33] Ellie Powers and Chris Beckmann. Chrome's turning 10, here's what's new. *Google Blog,* https://www.blog.google/products/chrome/chromes-turning-10-heres-whats-new, September 2018.

[34] Steve Ragan. Mozilla's bug tracking portal compromised, reused passwords to blame. *CSO,* https://www.csoonline.com/article/2980758/data-breach/mozillas-bug-tracking-portal-compromised-reused-passwords-to-blame.html, September 2015.

[35] Dominik Reichl. Setup - KeePass. *KeePass Password Safe* (official website), https://keepass.info/help/v2/setup.html, 2019.

[36] Richard Shay, Lorrie Faith Cranor, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, and Nicolas Christin. Can long passwords be secure and usable? In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*, 2014.

[37] David Silver, Suman Jana, Dan Boneh, Eric Chen, and Collin Jackson. Password managers: Attacks and defenses. In *Proceedings of the 23rd USENIX Security Symposium*, 2014.

[38] Aaron Smith. Americans and cybersecurity. Pew Research Center, http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security, January 2017.

[39] Elizabeth Stobert and Robert Biddle. The password life cycle: User behaviour in managing passwords. In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS'14)*, July 2014.

[40] Elizabeth Stobert and Robert Biddle. A password manager that doesn't remember passwords. In *Proceedings of the 2014 New Security Paradigms Workshop (NSPW)*, 2014.

[41] Elizabeth Stobert and Robert Biddle. Expert password management. In Frank Stajano, Stig F. Mjølsnes, Graeme Jenkinson, and Per Thorsheim, editors, *Technology and Practice of Passwords*, volume 9551, pages 3–20. Springer International Publishing, 2016.

[42] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "I Added '!' at the End to Make It Secure": Observing password creation in the lab. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'15)*, 2015.

[43] Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. The next domino to fall: Empirical analysis of user passwords across online services. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18)*, 2018.

[44] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding password choices: How frequently entered passwords are re-used across websites. In *Proceedings of the 12th USENIX Conference on Usable Privacy and Security (SOUPS '16)*, 2016.

[45] Jeff Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. Password memorability and security: Empirical results. *IEEE Security and Privacy*, 2(5):25–31, September 2004.

A Appendix: Open Data

The codebook, a more detailed demographic summary, and the (anonymized) dataset for this paper are available at https://osf.io/6u7m8/.

B Appendix: Interview Script

B.1 General Questions about Passwords

1. What types of online accounts do you have? (e.g. social media, bank accounts, shopping sites, etc.)
2. What level of protection do you think they each need? (Follow up, if necessary): Are there some accounts you want to protect more than others?
3. To the best of your knowledge, approximately how many online accounts do you have that use passwords?
4. How many of these do you access on a daily basis?
5. On which device(s) do you access these online accounts? (Follow-up below for each category the person has.)
   (a) For phones/tablets: what type(s)? (iPhone, Android, etc.)
   (b) For computers: what operating system(s)? (Windows, Mac, Linux, ChromeOS, etc.)
   (c) Public, work or personal device?
   (d) For each device: what web browser do you use most often on your [device]?
6. How many times do you manually type in passwords on a daily basis?
   (a) Which types of accounts?
   (b) On which device(s)?
7. How many of your accounts are always logged in?
   (a) Which types of accounts?
   (b) On which device(s)?
8. Do you have any passwords that get auto-filled for you?
   (a) Which types of accounts?
   (b) On which devices?
   (c) Do you know how your passwords are auto-filled?
9. Are your passwords different for each account?
   (a) (If yes) Are your passwords similar to one another?
   (b) (if reuse exists): How many of your accounts share the same password? How many of your accounts have unique passwords?
10. How do you create a password for a new account?
    (a) How does this password compare to other passwords? (i.e. is it similar?)
    (b) What if your password does not meet the character/length requirements. How would you change your password to meet those requirements?
    (c) Is this process different for some types of accounts? Which ones? What do you do?
11. How do you keep track of your passwords now? Do you use more than one method?
12. Are you satisfied with your current method(s) of managing your passwords?
    (a) What do you find easy about it?
    (b) What do you find difficult about it?
13. Has anyone ever logged into any of your accounts without your permission?
    (a) (if yes) Was this done by someone you didn't know?

(b) (if yes) What did you do? Follow up, if applicable:
   i. Did you change the compromised password?
   ii. How did you choose the new password?
   iii. How does the new password compare to your existing passwords?
   iv. Did you change the passwords to your other accounts that share the same password?

(c) (if no) What would you do if someone did?
   i. Would you change the compromised password?
   ii. (If yes) How would you choose the new password?)
   iii. How would you choose it?

14. To your knowledge, have any of your accounts ever been subject to a password data breach?

(a) (if yes)
   i. How did you find out about it?
   ii. What did you do?
   iii. After the breach, did you change the way you manage your passwords?
   iv. Did that account share a password with any of your other accounts?
   v. If so, did you change any of those passwords?

(b) (if no) What would you do if it was?

B.2 General Questions about Password Managers

1. Have you ever heard of password managers? Where did you hear about them?

2. Do you use a password manager?

3. What, to your knowledge, is the purpose of a password manager? (If they respond to something along the lines of "it manages passwords") What else do you think they're used for?

4. *Read description of password managers to participant*

   Password managers are tools that can securely handle passwords for you. They can remember your passwords, generate new ones, and even sync them across devices. There are various types of password managers with different features, but for the purpose of this interview, we will consider three of them.

   One type of password manager is built into the web browser, such as Google Chrome, Mozilla Firefox, Safari, Internet Explorer, and Microsoft 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. 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 can remember passwords in and out of your browser. It can also be used with iCloud to sync passwords across Apple devices.

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

5. Based on our description, which of these categories of password managers do you currently use, if any?

6. Have you used any [other] password manager tools in the past?

7. (If they have used PM, now or in the past) When did you start using a password manager? Why did you start using it?

8. (if stopped use): When did you stop using the password manager and why?

9. (If they use any and haven't already named them) Can you name the password management tools that you use? (Or if they can't name them, ask them to describe them / indicate how they use them so that you can try to discern what they mean)

B.3 Experience Using Password Managers

1. Why did you choose [PM]?

2. How has your experience been using a password manager?

3. What functions did you like / find helpful?

4. What functions did you dislike / find unhelpful?

5. Is all functionality of your password manager available for free, or does this tool have a paid version?

   (a) (If paid version exists) Do you use the paid or free version? Why?

   (b) (if uses free version) Would you ever pay for a password manager? How much? What features would it have?

6. Do you use your password manager on all of your devices, including [list of tools they already told you about in the first section]?

   (a) (if no)

i. Which devices do you use it on?
ii. Why do you use it on those?
iii. Why not use it on the others?
iv. How do you keep track of passwords on the device(s) that you don't use your PM on?

7. (For each device that the user uses PM on): Did you have to install an application to your device, or install an extension to your browser, or both?
   (a) (if no) How do you access your password manager? (possible answers include logging into a website, or USB drive)
8. Does your password manager offer the option of syncing passwords between devices?
   (a) (If this option exists) Do you use it? Why or why not?
9. Do you use your password manager for all the accounts you access through your web browser?
   (a) If not, how do you decide which accounts to use it for?
   (b) How do you keep track of passwords that are not stored in this PM?
10. Do you use your password manager for any accounts outside of your web browser? Examples of this would include an email client like Outlook on your computer or a social media app such as Facebook on your phone.
   (a) Do you use it for all of the accounts outside of your web browser(s)?
   (b) (if no to a) How do you decide which accounts to use it for?
11. Do you have to provide a master password or other authentication to access the passwords stored in your password manager?
   (a) (If yes) What type of password or authentication is required?
      i. (if master password):
         A. How did you create your master password?
         B. Is your master password similar to your other passwords?
         C. Is it difficult to remember your master password?
         D. (if yes) How do you remember it?
   (b) (If yes) How often do you have to provide it?
   (c) Have you ever modified the default settings to change how often you have to provide this?
12. Do you feel like your passwords are safe and secure when stored in this PM tool?
13. Do you know how this tool protects the security of your passwords? *(Unless they say they have no idea, ask them to elaborate on how they think it works)*
14. Does your password manager have a password generation tool?
   (a) (if yes to 14) Have you ever used the password generation tool?
      i. (if yes to a):
         A. Do you use the generation tool for newly created accounts?
         B. Have you used the tool to generate a new password for an existing account?
         C. (if yes to B) Does your password manager have an automatic password replacement feature that changes passwords for you without you having to actually visit the website yourself? Do you use it? Why or why not?
         D. Approximately how many of your passwords are now created by the password generation functionality?
         E. Do you ever change the settings from the defaults when generating a password?
         F. Was there an instance where the generated password did not meet the website's password requirements? (If yes) What did you do about it?
         G. Overall, how has your experience been using the password generation tool?
15. Does your password manager have a dashboard or tool that examines the security of your passwords?
   (a) (If yes): How often do you use it?
   (b) Have you changed any of your passwords after looking at this information?
16. Has your password manager ever informed you of a data breach? (If yes) What did you do?
17. Has your password manager ever prompted you to change your password? (if yes) Under what situation? What did you do?
18. Are there any additional services or features that you would want in your password manager?

B.4 Why not Using PMs? (If answer "no" to Using Password Managers)

1. Can you tell us why you aren't using a password manager? *(Follow up by probing what it would take for them to use a password manager.)*
2. Many third-party password managers require a monthly fee to use their services. Would you be willing to pay for such a service?
   (a) If yes, how much?
   (b) If no, why not? (*If participant says there are free third-party PMs available, then ask:* Would you be willing to pay for additional features that are not included in the free version? How much would you be willing to pay?)

B.5 Perceptions of Password Managers' Functions

We talked about different types of password managers a few minutes ago, including third-party password managers, password managers built into web browsers, and password managers built into operating systems.

1. Do you think some types of password manager tools are safer to use than others? (Why?)
2. Do you think some types of password manager tools are more convenient than others? (Why?)
3. How do you think password manager tools compare to other methods of managing passwords, such as writing them down on paper or saving them in a file on your computer? (Why?)
4. How do you think password managers store passwords?
   (a) Do you think password managers store your passwords locally on your device or on a server (in the cloud)?
      i. Do you think one is more secure than the other? (If so, which one? Why?)
      ii. Do you have a preference? Why or why not?
   (b) How do you think password managers sync your accounts across devices?
      i. Would you want this function? Why?
      ii. Do you think this impacts your password security? If so, how?
   (c) What do you think the password data looks like when stored on your computer?
      i. If your password is "password2018!", does your password manager store it as "password2018!"?
      ii. Is there a difference when stored in the cloud?
5. Do you think password managers affect the security of your accounts? Why or why not?
6. Do you trust password managers to always store or not forget your passwords? Why or why not?
7. Do you trust password managers to protect your passwords from attackers? Why or why not?
8. Have you ever received advice or training on how to create or manage passwords?
   (a) (if yes) What guidelines have you been taught? Where?
   (b) (if yes) Do you use these guidelines? Why or why not?
9. (non-PM user): Would you consider using a password manager in the future? Why or why not?
10. (If "No" or "I don't know" to data breach question in Part B.1, Q. 13: Earlier you mentioned that you were never impacted by a data breach, or that you weren't sure if you were. Would you like the opportunity to verify this? We can use a website called HaveIBeenPwned to check whether your accounts were compromised in a public data breach.
    (a) *Explain to participant:* The website asks for your email address and checks if any accounts tied to it were compromised. Note, however, that the website cannot check information on every data breach. It checks those that are known to the public.
    (b) *If participant agrees, inform participant:* For privacy reasons, we recommend that you access the website on your own device. This way, we won't see your email address, nor will we know which of your accounts, if any, were impacted by a breach.
    (c) *Instruct the participant to try any other email address they may use often.*
    (d) Were any of your accounts compromised?
    (e) (if yes)
       i. How many?
       ii. What types of accounts? (Provide categories to choose from: social media, bank, shopping, other)
       iii. How do you feel about this information?
       iv. (follow up, if necessary) Will you do anything with this information?

C Appendix: Codebook

Code categories are shown in bold type, with the list of codes in that category following. For a more detailed version with code descriptions, see https://osf.io/6u7m8/.

- **Account type:** shopping, banking, utilities, email, social media, healthcare, work, school, other
- **Account number:** less than 10, 10-15, 16-20, 21-30, 31-50, 51-100, more than 100
- **Account importance:** all accounts important, financial accounts, accounts with PII, work accounts, Facebook, email, other
- **Accounts accessed daily**: accounts accessed daily *(single code to used only identify snippet where participant gave estimate of this number)*
- **Password composition:** use passwords of equal strength, stronger passwords for more important accounts, disposable/weaker passwords for unimportant accounts, unique passwords for all accounts, unique passwords for important accounts, use shared substrings, use randomly generated, use passphrase, use words related to website type, use 2FA for more important accounts
- **Devices and browsers used:** iPhone/Safari, iPhone/Chrome, iPhone/Firefox, iPhone/other, iPad/Safari, iPad/Chrome, iPad/Firefox, Windows/Chrome, Windows/Firefox, Windows/Edge, Windows/IE, Mac/Safari, Mac/Chrome, Mac/Firefox, Android/Chrome, Android/Firefox, Android/other, Linux/Chrome, Linux/Firefox, Linux/other
- **Passwords typed daily:** 0, 1-2, 5, other number
- **Passwords saved:** never, unimportant accounts,
- **Exceptions to password reuse:** set by someone else, need to share, use old password, forced change, password requirements, other
- **Exceptions to password reuse: method of remembering exception password:** write down, other
- **Action when password is rejected due to password creation requirement:** add required characters, regenerate new password, remove forbidden characters, other
- **Password creation process:** same password for all accounts, use generator, one password per "tier" of accounts, use memorable personal info, other
- **Current password management:** synced file, guessing variations / resetting, physical notes, local file, memory, third-party PM, keychain, browser, fingerprint, not sure, other
- **Password management: satisfied?:** satisfied, not satisfied, not sure
- **Password management likes (non-PM methods):** always accessible locally, easy to remember, other
- **Password management dislikes (non-PM methods):** potential to lose, hard to remember, other
- **Had compromised account:** yes, no, I don't know
- **Compromised account action:** major/total change to compromised password, minimal change to compromised password, contact support, change passwords for accounts with same email, stronger password, other
- **Had data breach:** yes, no, I don't know
- **Data breach action:** change password, contact support, change passwords for accounts with same email, other
- **Aware of password managers?:** aware, not aware
- **Not use PM reason:** not many accounts, not aware of PMs, not much to protect, security concerns, master password concerns, past negative experience, other
- **Heard of PM from:** work, media, other people, I don't know, other
- **PM definition:** store/organize passwords, unique passwords, generate random passwords, no need to memorize, improve security, autofill, I don't know, other
- **Use PM time:** less than 1 year, about 1 year, multiple years
- **Use PM device:** all, non-shared, computers only *not phones, tablets, etc.*
- **Start using PM reason:** convenience, memory limitations, receive prompts, security, other
- **PM like function:** autofill, generate strong passwords, no memorizing, syncing, unique passwords, view passwords, desktop client, other
- **PM dislike reason:** incompatible device, saved unwanted passwords, cannot view passwords, generates passwords with unacceptable symbols, other
- **PM feature request:** PM feature request *(single code used to tag all snippets referring to features that participants wished PMs had)*
- **PM switch strategy:** gradually, change all at start
- **Use PM to store info other than website passwords:** use PM for application passwords, use PM for other info (e.g. credit cards)
- **Master password unique:** yes, no
- **Master password composition:** random, passphrase, other
- **Uses 2FA in combination with master password**: yes *(single code only used for participants who reported using this combination)*
- **Pays for PM (if using) or willing to pay (if not using a PM)?:** yes (currently pays or would pay), no (does not pay / would not pay), depends
- **Function that would convince them to pay for PM**: 2FA *(single code, no other specific functions mentioned)*
- **Not pay for PM reason:** already using free version, other
- **Pay for PM price:** $5 or less per month, depends, other
- **PM dashboard:** has used, has not used, not available in their PM (as self-reported)
- **Exceptions, PM users: certain passwords not stored in PM:** infrequently used, habit, multiple accounts, personal info, shared computer, email, financial, old account
- **PM generator:** not aware, aware / does not use, aware

/ does not use now / would not unless something "bad" happened, uses, not available for their PM (as self-reported)
- **Choosing PM reason:** compatibility, cost/value, features, convenience, other
- **PM security (beliefs about most secure type):** OS most, third-party most, browser most, third-party least, browser least, depends, no difference, I don't know
- **PM security belief reason:** not sure, connected to internet → less secure, trusts known names (e.g., Google), distrusts third parties, password storage method (e.g., "browser not secure because it stores passwords in plaintext"), trusts specialized/password-specific tools, distrusts browser code, other
- **PM convenience (opinions about most convenient type):** third-party least, browser most, OS most, third-party most, no difference, I don't know
- **PM convenience belief reason:** no extra setup step, no extra cost, not sure, other
- **PM or other methods safer?:** PM, other, neither/unclear/depends
- **Beliefs on where PMs store passwords: locally or cloud?:** locally, cloud, both, depends, I don't know
- **More secure: locally or cloud?:** locally safer, cloud safer, equal, I don't know
- **PM stores passwords: format?:** "in code," encryption, plaintext, I don't know
- **PM stores passwords: format: different in cloud?:** no difference, difference, I don't know
- **PM effect on security:** no effect, positive effect, negative effect, I don't know
- **Trust PM to remember passwords?:** sometimes, yes, no
- **Trust PM to protect from attackers?:** not sure, yes, no
- **Password advice sources:** website guidelines, people, work, other
- **HaveIBeenPwned:** used previously, no pwnage found, breach found, declined
- **Uses syncing?:** currently syncs, does not currently sync
- **Syncing perceptions?:** useful, not useful secure, not secure
- **Miscellaneous themes:** acknowledges risks, uses 2FA for all accounts, dormant accounts, time-saving, does not log out of accounts, social media: no customer support, conflates hacking and data breach, stores work passwords in PM, work passwords similar to personal, uses PM at work, logs out of banking accounts, likes having constant/mobile access to passwords, access problems, control, attackers target bigger entities than me, inertia b/c no past bad experiences, confusion about "remember me", specifically trusts Google, specifically trusts Apple, specifically trusts another company, tradeoffs, frustration with security questions, account sharing, knowledge gap, device sharing, habit, self-imposed password changes, kept reused passwords after breach, avoids creating new accounts, multiple accounts on same website, bank will reimburse, switching too much work, browser not safe, threat model: physical access, negative past PM experience, required password changes at work, all eggs in one basket