"It Basically Started Using Me:" An Observational Study of Password Manager Usage

Sean Oesch
The University of Tennessee
Knoxville, TN, USA
toesch1@vols.utk.edu

Anuj Gautam
The University of Tennessee
Knoxville, TN, USA
agautam1@vols.utk.edu

Scott Ruoti
The University of Tennessee
Knoxville, TN, USA
ruoti@utk.edu

ABSTRACT

There is limited information regarding how users employ password managers in the wild and why they use them in that manner. To address this knowledge gap, we conduct observational interviews with 32 password manager users. Using grounded theory, we identify four theories describing the processes and rationale behind participants' usage of password managers. We find that many users simultaneously use both a browser-based and a third-party manager, using each as a backup for the other, with this new paradigm having intriguing usability and security implications. Users also eschew generated passwords because these passwords are challenging to enter and remember when the manager is unavailable, necessitating new generators that create easy-to-enter and remember passwords. Additionally, the credential audits provided by most managers overwhelm users, limiting their utility and indicating a need for more proactive and streamlined notification systems. We also discuss mobile usage, adoption and promotion, and other related topics.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing → User studies**.

KEYWORDS

password manager, observational study, grounded theory

ACM Reference Format:
Sean Oesch, Anuj Gautam, and Scott Ruoti. 2021. "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In *CHI '22: ACM Conference on Human Factors in Computing Systems, April 30–May 06, 20122, New Orleans, LA.* ACM, New York, NY, USA, 23 pages.

1 INTRODUCTION

Weak and reused passwords are a consistent problem for authentication security. Password managers attempt to alleviate these issues by helping users generate, store, and fill strong and unique passwords. These benefits have led many security experts and news outlets to actively promote the adoption of password managers.

However, the effectiveness of password managers is limited if users fail to fully leverage the manager's rich feature set or use the manager in unexpected ways. For example, prior research has found that users often eschew the manager's password generator, continuing to self-select and reuse passwords [22, 28]. To help identify similar issues, additional research is needed to investigate how users leverage their managers in practice, exploring both underutilized functionality and unexpected usage patterns. Furthermore, even when user behavior is known—as with password reuse—it is unclear why they behave that way, making it difficult to improve the design of managers to address impediments and correct usage.

To help illuminate these knowledge gaps, we conduct observational interviews wherein users both demonstrate how they use their password managers and explain why they use them in that manner. This includes having users demonstrate and explain how they configured their password manager, create accounts (including credential selection/generation), log into accounts, and update accounts. The interviews also explore topics related to the initial adoption process, promotion of the manager to others, sharing passwords, and using the health check functionality built into most modern managers. Participants for these interviews include 28 password manager users recruited from Amazon's Mechanical Turk and four users from a convenience sample of highly technical users.

Data from the interviews was analyzed using grounded theory [11]. The main findings from these interviews include,

(1) Many participants (n=21; 66%) simultaneously use multiple password managers. Most commonly (n=13; 41%), this involves using the password manager built into their browser and an external manager (e.g., LastPass or KeyPass). The adoption of multiple managers often occurs without forethought as participants click through the browser manager's frequent pop-ups, which are seen even if the user has already adopted an external manager. This is best described by one participant who stated that "it basically started using me." However, this usage does not remain incidental, as participants leverage multiple managers as a backup solution for each other, addressing concerns related to losing passwords and syncing passwords between devices.

    This result expands upon past work by Stobert and Biddle [34] that showed that highly-technical users leverage multiple managers. Our results demonstrate that multiple manager use is common regardless of technical expertise. Our results also help provide additional details for the rationale behind multiple manager usage and describe its role in users' password management strategies.

CHI '22, April 30–May 06, 20122, New Orleans, LA

(2) Participants need to enter credentials on devices that do not have the user's password manager installed. Due to the difficulty of entering generated passwords on such devices and the fear that they may need to enter the generated password when they do not have a way to look it up (i.e., they are away from their phone or desktop), many participants eschew generated passwords. While previous work has identified the limited use of generated passwords [22, 28], our work helps explain the reasoning behind this behavior and establishes the need for passwords managers to better support the cross-device credential entry use case.
(3) Participants rarely leverage the credential audit tools (i.e., password health checks) available in external managers. While they are interested in having their credentials audited, they feel overwhelmed by the sheer volume of warnings produced by these tools and do not know how to prioritize those warnings or best address them. In contrast, they are highly appreciative of the credential compromise warnings provided by Chrome's built-in manager. These warnings are generated automatically (i.e., users are not required to run a health check manually), occur rarely, and clearly indicate what the user needs to do.
(4) Usage of mobile password managers is minimal, regardless of usage on desktop. This is caused by (1) inconsistent autofill and autosave functionality, (2) issues syncing between desktop and phone password managers, (3) apps and websites that stay logged in near-permanently on mobile, and (4) preference for SSO. Even if users use a mobile password manager, they often do not use password manager features such as autofill and autosave.
(5) Adoption of managers primarily arises from (a) a requirement to use a manager at work, (b) to simplify the credential entry process, or (c) improve the quality of the passwords they use. When choosing which manager to adopt, users rely on recommendations from friends, colleagues, and trusted online sources. While participants overwhelmingly love their managers, most (n=26; 81%) do not promote manager usage outside of their immediate family, and even among those who do, success is rather limited. These results serve to triangulate similar results from past interview studies [13, 28, 30] and also provide additional empirical evidence regarding challenges to the adoption of password managers discussed in research focused on this issue [1, 2, 5, 6, 23].

We also include a discussion of less central issues: how participants (a) share passwords with other individuals, (b) encounter inconsistencies with autofill and autosave functionality, (c) use the manager's autolock functionality, (d) rely on default settings, (e) desire increased adoption of single sign-on (SSO), and (f) changed their usage of their password managers due to COVID-19.

1.1 The Big Takeaways

Our research has important implications for how the research community should think about password managers. First, our results demonstrate that multiple manager usage is common among both technical [34] and non-technical users. This indicates a critical need for research exploring the usability and security implications of multiple manager usage—for example, how continued usage of browser-based managers, which are less secure than external managers [26], limits the security benefits of adopting an external manager.

Second, our results help explain why users eschew password generators, a troubling trend identified in prior empirical research [22, 28]. Our results show that this avoidance is primarily attributable to concerns about entering generated passwords on devices where the password manager was unavailable to autofill or lookup the credential. As such, there is a practical need for more research exploring how password can be generated that are easy-to-enter on devices without keyboards [15, 16] and/or which are user-memorable [8], especially as the existing research on these issues does not address the wide range of devices and situations where users could use generated passwords.

Third, users do not use credential audit tools, finding their results to be confusing and overwhelming. Research is needed to identify what designs can improve the utility of credential audits. Based on participants' responses, a good start would be to explore making these tools more proactive and streamlined in the notifications they provide, helping users address issues incrementally instead of asking them to fix everything at once.

Fourth, many users avoid mobile managers due to concerns about their usability. This is in line with prior results from a lab study of mobile manager usability [31]. Taken in conjunction with results on the poor security of mobile password managers [4, 25], this demonstrates a need to rethink mobile password managers and find a way that they can be made both usable and secure.

2 BACKGROUND

In this section, we first provide background on password managers. Next, we described related work.

2.1 Password Managers

Password managers serve to help users (1) generate random, unique credentials for each service they authenticate to, (2) store the user's credentials (both generated and user entered), and (3) fill those credentials for the user. These features provide several tangible benefits for users:

- They reduce the cognitive burden of remembering usernames and passwords. Ideally, this allows users to have unique passwords for every service they authenticate to, addressing the problem of password reuse.
- They help users generate strong passwords resistant to online and offline guessing attacks.
- They help users audit their credentials, identifying compromised or weak passwords.

There are three primary classes of password manager implementations: built into the browser, integrated into the browser using an extension, and a separate app not integrated with the browser. In this paper, we refer to the latter two as external managers—i.e., not built into the browser—and the former as browser-based.

2.2 Related Work

Below we discuss related work, categorizing it based on the main findings of our research.

2.2.1 Multiple Manager Usage. Stobert and Biddle [34] conducted semi-structured interviews of 15 expert users about their password management usage. These participants were predominantly male (87%) and young (average age of 29). Their findings showed that these expert participants utilized more secure behaviors for important accounts versus non-important accounts. Additionally, most of their participants used multiple managers. Pearman et al. [28] also mention that in their interviews with users, some participants used multiple strategies for storing passwords. However, it is unclear whether this refers to multiple manager usage or whether it refers to using a password manager and recording passwords outside of a password manager. Either way, other than mentioning that this usage pattern exists, there is no further discussion of the phenomenon.

Our study confirms and expands upon past results, demonstrating that multiple manager usage is common for all users, regardless of technical background. Furthermore, our results help provide necessary context regarding multiple manager usage, describing the rationale and workflows underlying such usage. For example, we find that one key reason users employ multiple managers is for fear that one of the managers will fail to store a generated credential, whereas using multiple managers increases the likelihood that at least one will have stored the desired credential. Also, in line with Stobert and Biddle's results, we find that most users utilize more secure behaviors for important accounts versus non-important accounts, confirming that this behavior is not limited to only technical users.

2.2.2 Why Users Avoid Generated Passwords. Lyastani et al. [22] used an instrumented password manager to collect telemetry data regarding password manager usage. They found that participants were using their managers to store and autofill credentials for a wide variety of websites. However, they also found that stored passwords were weaker than expected, resulting from the fact that participants largely eschewed the password generator in favor of passwords the participants had created themselves. In a series of interviews with password manager users, Pearman et al. [28] also observed that users tend to avoid the password generator. However, neither paper identified the underlying reason that users eschew generated passwords.

In our work, we also find that users avoid generating passwords but build upon prior research by identifying why they do so. Our results show that this avoidance is primarily attributable to concerns about entering generated passwords on devices where the password manager was unavailable to autofill or lookup the credential. This can include worrying about the inconvenience of entering a complex password on a device with a constrained input device (e.g., a smart TV or IoT device). It can also include fears that they will not be able to remember a generated password when needed if they are not next to their phone or primary desktop.

Concerns about the annoyance of entering generated passwords on mobile phones form the basis of research by Greene et al. [15, 16] that permutes generated passwords to make them easier to enter. Similarly, there is a body of literature looking at the ability to generate memorable cryptographically-strong passwords, starting with work by Bonneau and Schechter [8]. Our results suggest an urgent need for more research in these veins.

2.2.3 Credential Audit Tools. In 2021, Simmons et al. [33] systematized password manager users cases, identifying credential audits as an important feature offered by password managers. They also conducted cognitive walkthroughs of eight different password managers. However, they do not discuss any results related to the usability of credential audits. In line with claims by Simmons et al., we do not find any evidence that there are other evaluations of credential audit tools in the literature. As such, our work serves as the first set of results regarding the usability and utility of credential audit tools, finding that while such tools have promise—such as automated compromise warnings from Google Chrome—they are largely underutilized due to usability issues.

2.2.4 Mobile Manager Usability. Seiler-Hwang et al. [31] conducted a laboratory user study exploring the usability of four smartphone password managers. In this study, novice participants installed and used several password managers to register, update, and autofill credentials. Their results found significant usability issues through the tested tools, particularly regarding poor integration of the manager with apps and browsers. Overall, users rated the password managers as having barely acceptable usability.

In our study, participants also share their frustrations with mobile password managers. We confirm Seiler Hwang et al.'s results, showing that in the field, poor integration between managers, apps, and browsers remains a significant usability hurdle for mobile password managers. Moreover, our results show that these usability issues are sufficient to cause many users to ignore using mobile managers altogether.

2.2.5 Adoption. Fagan et al. [13] surveyed users and non-user of password managers to understand why and why not, respectively, users chose to adopt a password manager. They found that adopters were generally motivated by security, whereas non-adopters were motivated by security concerns. In line with Fagan et al.'s work, Pearman et al. [28] conducted semi-structured with users and non-users of password managers, finding that users of browser-based managers were motivated primarily by convenience. They also found that users of external managers (e.g., LastPass or KeyPass) were driven by security. For users of browser-based managers, Pearman et al. hypothesized but did not find direct evidence that their focus on convenience may explain why some users do not generate and continue to reuse passwords. More recently, Ray et al. [30] replicated Pearman et al.'s protocol with adults over the age of 60, finding that older adults are more likely to adopt a manager if the recommendation comes from a family member and have more concerns with storing passwords in the cloud and syncing than younger adults.

Aurigemma et al. [5] analyzed the adoption of password managers among home end-users and found a lack of trust and threat apathy as the main hurdles to adoption. Similarly, Alkaldi et al. [1] studied password manager adoption among smartphone users and found that lack of awareness and trust were key issues. There is work exploring how the unified theory of acceptance and

use of technology (ATAUT2) and protection motivation theory (PMT) models may explain adoption, or lack thereof for password managers [6, 23]. Looking through the lens of these models helps explain explaining why lack of trust, threat apathy, and lack of awareness prevent adoption—for example, threat apathy impacts the threat-appraisal process in PMT, indicating that users will be unlikely to adopt the technology unless there is nearly no cost to do so (and even then they may not), which is not true of password managers. Alkaldi et al. [2] also looked at password managers through the lens of self-determination theory, showing that when all self-determination factors (autonomy, relatedness, competence) were satisfied, users were most likely to adopt password managers.

In our study, we examined participants who had already adopted passwords, finding that the three most common reasons for adoption were (1) requirements to use a password manager at work, (2) that the manager makes their life easier, and (3) that the manager allows them to increase the security of their online credentials. We also explored whether these participants promoted their manager to others and asked participants what caused their promotion efforts to fail. One common reason was the difficulty for the person being told about the password manager to understand how it would benefit their lives. We believe this issue is somewhat different from the lack of awareness described by Aurigemma et al. [5] and Alkaldi et al. [1], as even after being made aware of the manager, people still struggled to identify how the manager would benefit their day-to-day life from a utility, usability, and security perspective. We expect that the threat apathy described by Aurigemma et al. [5] partially explains the lack of understanding of how a password manager improves security. We also found that promotion was most likely to succeed among family, with family members able to help each other overcome the lack of trust [1, 5] and misunderstanding of the threat-appraisal process and response efficacy, increase adoption as predicted by PMT [6, 23].

2.2.6 Other Usability Studies. Huaman et al. [18] investigated interaction problems between password managers and websites by analyzing online feedback in user reviews and GitHub issues, then empirically confirming these issues using 15 desktop password managers. They found that password managers do a poor job of implementing authentication features and following modern standards (e.g., autocomplete) and that websites often do not implement well-structured authentication forms.

Chaudhary et al. [9] conducted a systematic literature review, selecting 32 final articles on password managers that focused on usability and security, to summarize known issues with managers and identify the best-known mitigations for those issues. They found that there are still issues related to users' trusting managers and lacking the appropriate mental model to use them, as well as technical issues with autofill, master password creation, and browser integration.

In our work, we find that the issues identified by these three works are a common source of frustration for users. More specifically, we found browser integration issues in a similar category, though not identical, to those mentioned in Chaudhary's survey [9]. For example, when the username and password fields are on separate pages, managers often fail to autofill properly, and that the password manager icon often overlaps with other website elements displayed inside credential fields.

There are also several works analyzing user preferences between manager types. Karole et al. [20] conducted a 20 participant study comparing user preferences for an online manager (LastPass), a phone manager (KeePassMobile), and a USB manager (Roboform2Go). They found that non-technical people preferred the phone manager and that technical people were inclined towards the USB manager. Ciampa et al. [10] compared user preferences for LastPass vs. SuperGenPass, a bookmarklet-based manager, finding a tendency to prefer the bookmarklet based manager. In our work, we did not directly evaluate user preference for different manager types, though we did find that some users were unaware that their manager offered cross-platform functionality.

2.2.7 Security Evaluations. There is a substantial body of research on the technical aspects of password manager security [21, 25, 26, 32, 35]. In general, this body of work finds that improvements are needed across all types of password managers. Still, browser-based password managers faired especially poorly, leading Oesch and Ruoti [26] to conclude that users should be steered away from this type of manager. Past research has also shown that on mobile devices, it is not safe to use the clipboard to transmit passwords between mobile managers and apps [7, 14]

In our work, we find that browser-based manager usage is common, even among users of external managers. Similarly, many users copy and paste the password from their mobile managers. In both cases, prior research demonstrates that these behaviors are risky. In light of our findings, more research is needed to help steer users from these behaviors.

3 METHODOLOGY

To understand user password manager behavior and the rationale behind that behavior, we conducted IRB-approved observational interviews. In these interviews, participants demonstrate and explain how they configure their password manager, create accounts (including credential selection/generation), log into accounts, and update accounts. The interviews also explore topics related to the initial adoption process, promotion of the manager to others, sharing passwords, and using the health check functionality built into most modern managers. Participants for these interviews include 28 password manager users recruited from Amazon's Mechanical Turk (MTurk) and four users from a convenience sample of highly technical users.

This section provides an overview of our interview process, interview guide, recruitment strategy, participant demographics, analysis methods, and limitations for our study. All study instruments can be found in Appendices A–E.

3.1 Interview Process

We conducted two rounds of interviews. In the first round (January 6–13, 2021), we interviewed four participants drawn from a convenience sample of highly technical users at a local research institute. In the second round (February 16–March 4, 2021), we interviewed 28 participants gathered from MTurk, with participants receiving $27 USD in compensation. On average,

interviews lasted 35–40 minutes, not including the initial overview and verifying that the participant had everything configured properly for the interview to flow smoothly (e.g. able to share their desktop and mobile screen via Zoom). All participants were active users of a password manager, with preference given to users of external password managers.

We conducted interviews online using Zoom.[1] Remote interviews were necessary due to institutional restrictions for conducting in-person research due to the COVID-19 pandemic.

We designed the interview to observe participants using their password managers on their own devices. Whenever possible, we asked participants to demonstrate specific behaviors during or before questions regarding those behaviors. We recorded all audio from the interview and video of the participants' screens during the portion of the interview where they were demonstrating how they used their password managers. Before starting the interview, we ensured that participants could share their screens from both their desktop and mobile device. We also had participants log out of their password manager on all relevant devices to avoid recording sensitive information. Once we ensured that the participant was comfortable with the sharing process, we began recording.

3.2 Interview Guide

The interview itself was semi-structured, and for continuity, a single researcher conducted all 32 interviews. The interviewer had an interview guide containing an ordered list of topics and questions designed to spark discussion and ensure users demonstrated all desired actions.

First, we asked questions related to general usage, such as how participants protected their password manager accounts, how they created their master password, and whether they used 2FA. We also asked how they chose this password manager, whether they ever recommended it to others, and if others adopted it based on their recommendation. Then we asked if they ever saved passwords anywhere other than their primary password manager, such as in the browser or on a notepad.

Second, we had participants log in to their password manager with a temporary account that we provided and show us if there were any settings they would change when configuring their manager on a new device. We then had them create an account on Reddit and eBay, walking us through how they would typically create an account. We chose these two sites as they represent different potential security risks, and we were curious whether users used different strategies for selecting passwords on social vs. financial websites. During account creation, we asked participants if they had issues when creating or saving accounts and about their password creation strategies.

Third, we had participants log back into those same two accounts, asking questions about how they utilize autofill. Once participants had logged in, we had them update their passwords for both accounts. We then asked them questions about their password updating habits.

[1]We used Zoom in an attempt to achieve a geographically and demographically diverse set of participants. Due to difficulties in recruiting, our results are not as demographically diverse as we tried to achieve (discussed in §3.4). Still, respondents did come from across the United States, providing more demographic diversity than we would have gotten from in-person interviews.

Fourth, we asked participants about their password creation and storage habits for different types of websites, their use of the autolock feature of their manager, and whether they filled passwords into apps on their desktop. These questions often led to fruitful discussions around important versus nonimportant accounts, device privacy, and edge cases for autofill.

Fifth, we asked participants how they usually go about sharing passwords and, if they were not already aware of it, demonstrated the password sharing feature of their password manager. We also asked how participants would typically check if their passwords had been compromised in a data breach and demonstrated the health check feature of their manager if they were unaware. Both questions led to extended discussions around password sharing and auditing behaviors. We then asked participants if there were any additional features they used that we had not yet mentioned (e.g., secure notes)

At this point, we had participants stop sharing their desktop screens and pivot to their mobile devices. Regardless of whether they used their password manager on their mobile device, we began with an open-ended question about how password management was different on their mobile device than on their desktop. We then asked them whether they created accounts on their phone, how they logged into websites and apps on their phone, and if they created/generated passwords on their phone.

If they used any password manager, including the one built into their phone's OS, on their mobile device, we had them share their mobile screen and demonstrate those behaviors they regularly practiced. Depending on their answers to prior questions, we had them log in to Reddit using the account we just created to help us understand how they sync between devices and how they utilize autofill on mobile. We also had them create, log out of, and log back into an account in the Memrise app if they used a manager for apps.

Finally, we had them stop sharing their mobile screen and wrapped up with a few closing questions. The first question was open-ended and provided participants an opportunity to share anything else they felt we would find helpful. We then asked what feature they would add or things they would change about their manager and closed by thanking participants for their time and explaining compensation.

3.3 Addressing Potential Risks

Because we did observe participants using their devices, we took several steps to protect their privacy. First, we reminded them at the beginning of the interview that we would be recording them on their own devices and allowed them to opt-out. Second, we had users log out of their password managers before we started recording and then had them log in to a temporary account that we provided. Third, we had users disable their video feed before recording just in case it exposed any private information. Fourth, when we uploaded the interviews for transcription, we only uploaded the audio in case the video contained private information.

3.4 Recruitment

To validate the utility of the interview guide, we started by conducting pilot interviews with a convenience sample of highly technical password manager users from a local research institute.

We gathered these participants via email invitation and administered a consent form, in which they were made aware that their data may be used in future publications. As this portion of the interviews was already IRB approved and the study methodology had no significant differences from the main studies, we decided to include data from these responses in our results, labeled as P1–P4. The behaviors of these pilot participants did not differ significantly from that of the non-pilot participants with highly technical jobs (e.g., engineer, IT professional).

The remainder of our participants were recruited using MTurk (see Section 4 for a discussion of the implications of using MTurk). To identify potential interview candidates, we first conducted an (IRB-approved) screening survey. This survey collected demographic data, asked respondents which password manager they used, including password manager-related questions from the Security Behavior Intentions Scale (SeBIS) [12], and select questions from Masur's online privacy concerns scale [24]. We included these two scales to help us better understand users and to look for potential correlations between user responses and behaviors. However, after completing the interviews, we did not observe any meaningful correlations between these scales and participants' responses and do not discuss the results from these scales in this paper.

Respondents were required to live in the United States,[2] be over the age of 18, and to actively use a password manager. Initially, we also limited respondents to Master Workers. However, after receiving only 101 responses from January 25–28, of which only 18 indicated a willingness to participate in our interviews, we opened the screening survey to non-Master Workers as well. Ultimately, we closed the survey on January 30 after receiving 1026 responses. Completing the survey took an average of 3–5 minutes, and participants received 1$ USD in compensation for completing the screening survey.

Next, we invited select respondents from the first survey to sign up for an interview time and answer additional questions from SeBIS. Initially, we invited respondents to participate in the interview based on gender and age to have a demographically representative sample. Unfortunately, due to a low response rate for interview signups and a high incidence of missed interview appointments, we ended up dropping this demographically targeted approach and instead invited nearly all respondents who had indicated willingness to participate in an interview. Ultimately, we ended up inviting 456 respondents to participate in our interviews, with 28 participants completing an interview labeled as R1–R28.

We stopped at 28 participants due to reaching saturation—i.e., in the last five interviews, we did not uncover any new findings not already illuminated in earlier interviews. While there may be some minor issues related to password management, saturation is a good metric for establishing that major issues have been discovered [17]. On average, interviews took 35-40 minutes, and participants received 26$ USD in compensation ($1 for signing up for an interview, $25 for completing the interview).

[2]We chose to focus on users from the United States to avoid confounding factors related to culture.

3.5 Participant Demographics

Our interview participants skewed male (n=22; 69%) with all but four participants between the ages of 18–44 (n=28; 88%). Most participants identified as Caucasian or White (n=23; 72%), with a smaller number identifying as Black or African American (n=4; 13%), Asian (n=4; 13%), and as Hispanic or Latino (n=1; 3%). Our participants had a range of educational experience: high school or GED (n=2; 6%), some college (n=5; 16%), Associate's (n=2; 6%), Bachelor's (n=11; 34%), Master's (n=8; 25%), Professional (n=3; 9%), or a Ph.D. (n=1; 3%). Following an approach similar to that of Tan et al. [36], we considered participants technical if they reported that people asked them for computer-related advice and that they knew a programming language, finding that half of our participants were technical by this measure (n=17; 53%).

Participants used a wide range of primary password managers: LastPass (n=11; 34%), Dashlane (n=3; 9%), KeePass (n=3; 9%), 1Password (n=2; 6%), RoboForm (n=1; 3%), Bitwarden (n=1; 3%), Chrome (n=9; 28%), and iCloud Keychain (n=2; 6%). The majority of participants used multiple managers simultaneously (n=21; 66%), with a plurality of participants using both an external and browser-based manager (n=13; 41%) and a smaller number using some other pattern such as having different managers on their desktop and mobile devices (n=9; 28%). About a third of participants used only a single manager (n=11; 34%). Most used a password manager on their mobile device (n=25; 78%), though as we discovered, this usage was often quite limited. Appendix F gives a list of participants their managers.

3.6 Analysis

To prepare our data for analysis, we first used an online transcription service to transcribe the audio recordings from the interviews. The (sanitized) interview transcripts, along with other artifacts from our analysis, are available at https://userlab.utk.edu/publications/oesch2022observational.

Our analysis follows a four-stage grounded theory [11] approach during our analysis (open coding, axial coding, selective coding, and theory generation). In the initial phase, three researchers reviewed each transcript phrase-by-phrase and assigned codes, revisiting the video and recordings as needed. We assigned codes primarily using open coding , though we also generated some in situ codes. After completing coding, we had a total of 572 unique codes. In the axial coding phase, we used the constant comparative method to group codes into concepts. In the third stage, we grouped concepts into related categories, drawing and labeling connections between concepts and categories. We refer to this collection of concepts and their relationships as a concept map.

Finally, we used these categories and the connections between them, the concept maps, and our research notes and observations to generate theories about how people use their password managers. Here "theory" is a term of art that in this context can be thought of as a description of the process and reasoning behind participants' password manager usage. In our analysis, we identify four such theories and discuss these in Section 5. We also identify other interesting findings not covered by these theories in Section 6.

4 LIMITATIONS

We selected participants from MTurk and conducted interviews via Zoom because we conducted our interviews during the COVID 19 pandemic and wanted to be sensitive to peoples' safety and university regulations. We also chose participants only from the United States to avoid the conflation of cultural factors. It is possible that people from other cultures use these managers differently. Additionally, MTurk users who live in the United States tend to be younger, better educated, more tech-savvy, and more privacy-conscious than the general population [19]. Future work could replicate this study with different populations and use more quantitative, large-scale approaches to explore specific observed phenomena.

We also selected only individuals who actively use a password manager, and a majority of our participants used either Chrome or LastPass. As a result, we did not collect any data on individuals who gave up on using a manager after trying it (survivor bias) and cannot generalize our results to all managers. There may be specific populations (the elderly, for example) who tend to give up on managers and do not fit the data presented in our study.

Because interviewees may desire to appear knowledgeable to the interviewer, they may have reported security practices different than their normal behaviors [3]. Likewise, direct observation may alter participant's behavior [29]. While we designed our study to limit the impact of these issues, they may have still impacted the results.

The fact that participants used fake accounts rather than their own may have also influenced our results, though it is difficult to say in what way. On the one hand, because we chose websites that would present the user with certain workflows / challenges, we were able to observe specific phenomena and to make the experiment consistent across users. On the other hand, we may have missed issues users face with their daily accounts.

In addition, we offered to demonstrate several features to participants (password sharing, password auditing) if they were unaware of said features. It is possible that demonstrationg these capabilities biased participants' attitudes towards them.

5 CORE THEORIES

Our analysis identifies four theories describing the processes and rationale behind participants' usage of password managers. Connections between the concept maps for each theory are explained in the caption for that concept map.

5.1 Adoption of Multiple Managers

In our studies, most participants use multiple managers in tandem. Figure 1 shows the concept map for multiple manager usage, highlighting the causes and resultant behaviors. While previous work has shown that experts use multiple managers [34], our results show that this behavior is common (n=21; 66%) among all users regardless of technical expertise.

Most commonly (n=13; 41%), multiple manager usage involved a browser-based manager (e.g., Chrome) in addition to an external manager (e.g., LastPass or KeePass). We also observed other multiple usage patterns, such as using a different manager on their desktop and phone (n=3; 9%). While this was a common occurrence in our interviews, to our knowledge, this has not been discussed in prior research, revealing an interesting new usage scenario for password managers to design around.

The most extreme case of multiple manager usage in our interviews was R7, who used Safari at home, Chrome at work, and aWallet on their phone. They used Safari because it synced passwords between their devices, Chrome because it was on their work PC, and aWallet for their most sensitive accounts and accounts that they needed to access when not near their desktop computers.

Several participants (n=3; 9%) did avoid using multiple managers, either because they believed it was insecure to store passwords in multiple locations or because they felt the browser manager was less secure than their external manager.

5.1.1 Browser and External Managers. As mentioned above, the most common form of multiple managers usage was using a browser-based manager in conjunction with an external manager. This behavior was motivated by three key factors. First, participants feared losing passwords stored in their external manager and use the browser's manager as a failsafe. As described by R9,

> *I do have [passwords] in Chrome as well, only because I have this horrible phobia that I'm going to, like LastPass or something like, oh, no, something's gonna blow up. Like, I'm going to forget the password and not be able to sign in. Something's gonna happen. And I kind of want to just have a backup. Oh, I just I'm paranoid like that."*

The second factor is that participants adopted the browser manager due to habituated click-through of dialogs presented by the browser. R13 described this second factor, saying,

> *"I guess when I said I would click on and save it (in browser manager). It's sort of just out of habit of clicking a popup. I'm kind of always like, just get the pop up out of here."*

As noted by R13 adoption of the browser-based manager was often unintentional and was a consequence of clicking through autosave dialogs generated by the browsers. Note, these dialogs are shown to users even after installing an external manager that integrates with the browser.

The third factor is that participants used both managers, hoping that if one failed to autofill a given website, the other would be able to. Still, while some participants (n=4; 13%) found having two managers added value, others (n=6; 19%) noted that sometimes multiple managers interfered with each other, leading to usability issues. For ,example, R12 stated that,

> *"Yeah, if it autofills, it's kind of like first come, first serve. If [Chrome] gets in there and autofills it before I have the chance to tell LastPass. It does cause some problems. So when I've updated a password somewhere out there in [Chrome] and now [Chrome] is out of sync with LastPass."*

5.1.2 Other Patterns. We also found that some participants (n=6; 19%) used different managers on their phone and desktop devices. Most commonly, this involved using an external manager on desktop and a built-in manager on mobile, with the

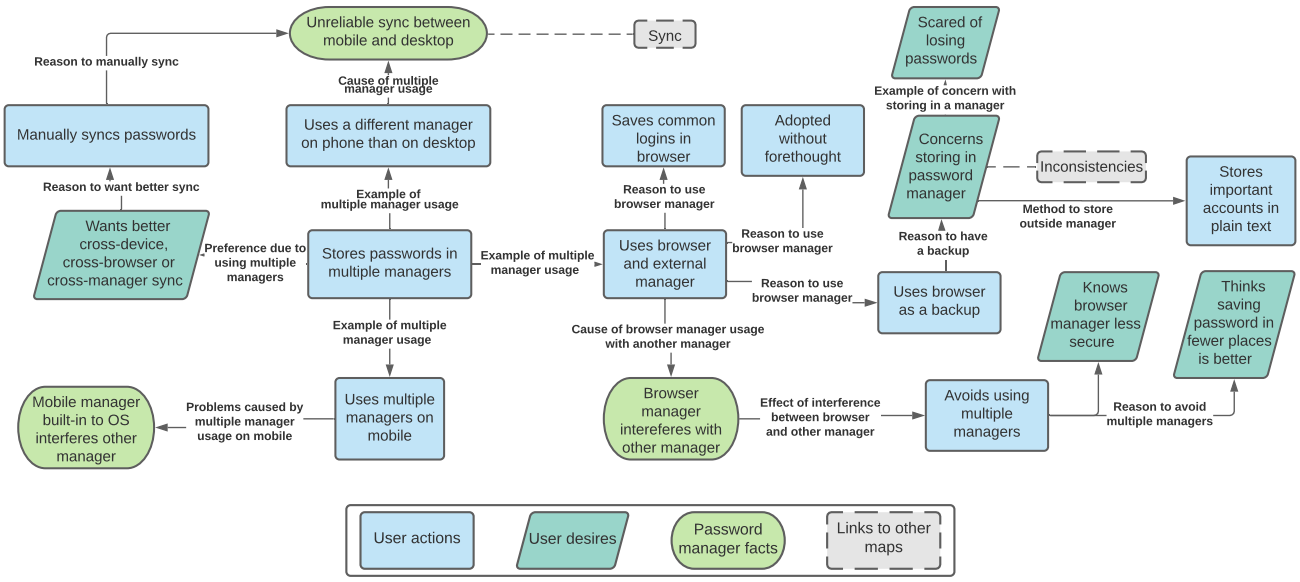

Figure 1: Concept map for multiple manager usage. Half of the participants used multiple managers due to issues syncing between devices, fear of not having their main manager available, and simply because the manager built-in to the OS or browser was persistently available. Only a few participants specifically avoided multiple manager usage, generally due to concerns about saving their passwords in too many places. This map connects to the concept map for syncing because issues syncing between devices resulted in multiple manager usage. It is also connected to the concept map for inconsistencies because inconsistent manager behavior caused users to distrust their manager, which resulted in using a second manager to backup their passwords out of fear of losing them.

built-in manager being adopted due to habituated click-through of autofill dialogs, as was the case on mobile. As described by R12,

> *"I do but not intentionally. Chrome picks [passwords] up sometimes and I don't stop it is what it boils down to."*

One potential explanation for the lack of external manager usage on mobile devices is the overall limited usage of password management on mobile devices, even when managers are installed. This is described later in this section. One consequence of this fragmented manager usage was that passwords were often out-of-sync between the multiple managers, causing passwords to only be available on the desktop or mobile device, but not both. These frustrations with syncing led R17 to state that if they change any one thing with their password managers that they *"would want to make it so that like, Apple and Chrome could marry one another, like, oh my goodness, you know, like so passwords can transfer easily."*

We also note that some participants also stored credentials outside of a password manager, such as writing them in a physical notebook or storing them in a digital text file.

5.2 Password Entry and Reuse

Our interviews found that participants need to enter credentials on devices without a password manager. This includes devices where it is impossible to install a password manager—e.g., a Smart TV—or for which they did not want to install a password manager—e.g., using a work computer or a mobile device. Figure 2 provides the concept map for cross-device entry. Even though this was an important issue for participants, to our knowledge, there is minimal prior research exploring cross-device entry for password managers.[3] Similarly, password managers largely lack the functionality to make this task easier.

This need for cross-device entry and lack of support for this use case had an unexpected consequence—it caused many participants to eschew generated passwords. While an unwillingness to use password generation has been observed before [22, 28], we were able to ask participants the reasons behind their avoidance of generated passwords. There are two primary reasons for this behavior, (1) participants find generated passwords to be extremely difficult to enter when not autofilled by the password manager, and (2) participants worry that they would not have their password manager available to lookup the generated password, thus locking them out of their accounts. For example, when asked if they ever intended to use the password generator, R4 stated,

> *"[I] would not. And the reason for that is that the password generator will give you like a bunch of gibberish letters. There's no way you could ever remember it. So let's say if you're outside and you're on your mobile, and you want to, you know, go to the website that you haven't been to on the phone, chances*

[3] Greene et al.'s work [15, 16] is a notable exception to research on cross-device entry, though it is limited to entry on mobile devices.

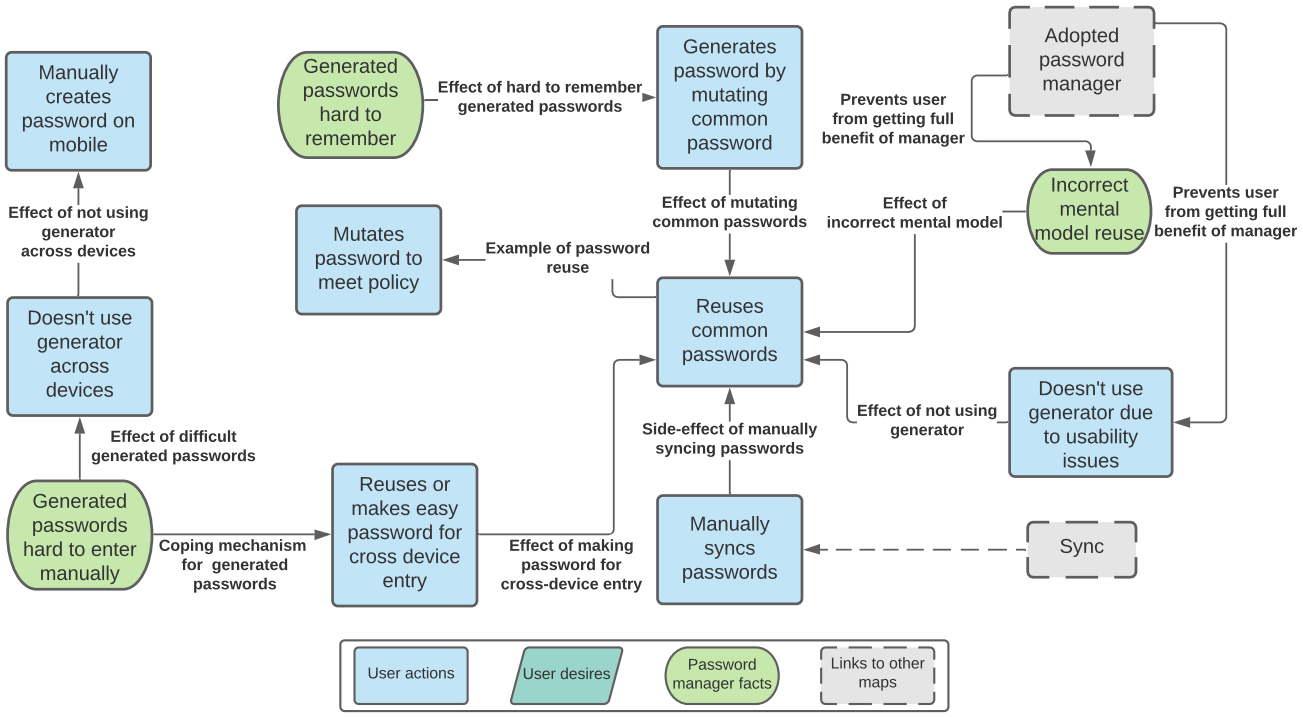

Figure 2: Concept map for password entry and reuse. Password reuse was still fairly common (n=8; 25%) even though all participants used a manager. We found that most reuse was due to usability issues with cross-device entry rather than a poor mental model of reuse. Participants felt generated passwords are difficult to remember and enter manually on other devices, so they reused common passwords instead. This map was connected to the sync concept map because when participants had to manually sync their passwords between devices, they tended to reuse passwords to make them easier to enter on the second device. The connections with the adoption concept map exist because even though these users adopted a manager, they still had an incorrect mental model of why password reuse is bad.

> *are like good luck remembering that password, you would never log in."*

Similarly, R21 shared,

> *"Like I'm very, very set in my ways in which passwords I use. So if they have too many, you know, special characters or numbers, I feel like not going to use that. So just in case the Chrome password manager craps out on me, it'll be easier for me to remember."*

In contrast, when participants were not worried about cross-device entry, we found that they were likely to use generated passwords liberally. As they trusted the manager to store and fill their credentials, they enjoyed the simplicity of no longer needing to pick and remember passwords themselves. As described by R10,

> *"Years and years ago, um, you know, I tried to use a system or like, I'd use the same base password and kind of modify it, depending on the site. You know, currently using keychain, I just let it generate the password and hit OK… It just works well between my phone and my iPad and my computer where I don't have to worry about syncing them or anything like that. It just kind of natively does the work for me."*

Even when participants frequently generated passwords, it was not unusual for them to continue having a small handful of passwords that they self-selected and memorized. These were for accounts they felt they might need to commonly authenticate to on other devices (e.g., Netflix) or where they felt the credentials were too sensitive to store in a cloud-synced manager.

Importantly, even when participants memorize their passwords, they still like the convenience of having the password manager autofill those credentials. This observation highlights the importance of both ease-of-use and autofill for password manager adoption.

When participants do select their password managers, we find that they primarily use strategies already well covered in the literature, such as reusing passwords for less critical websites or picking a strong secret, then permuting it for individual websites [22, 27]. Unique to our study, we found that some participants leveraged the password manager to allow them to act as human-password generators. In this case, they would examine physical items and activities occurring in their vicinity and use this ephemeral data to select the password. For example, a participant may look out their window, see a dog being walked, notice that the date is June 06, and that it is currently in the

afternoon, with a resulting password of `dogwalker66@noon`. The manager was necessary, as it would not be possible for the user to remember this generated password later.

5.3 Overwhelming Credential Audits

While some users only cared about convenience and did not update passwords even if their accounts were breached, most users would update passwords for breached accounts and found breach notifications helpful. However, health check results were often overwhelming when first checked because users had so many weak/reused passwords. The result was that most users simply avoided health checks. Users who self-audited accounts were the most likely to use or want to use health checks in their current form.

Participants preferred the account compromise notifications provided by Chrome's built-in manager to those of external managers. These notifications trigger automatically whenever a stored credential is detected in a leaked password data set. Critically, they do not require the user to do anything to receive the notification. Participants found these notifications timely and actionable—i.e., they knew what they needed to do it and when they needed to do it.

In contrast, participants were not a fan of the credential audit services provided by many external managers (often referred to as a health check). These credential audit services differ from the automatic notifications provided by Chrome in several ways. First, they require users to start the audit process manually. Second, they simultaneously audit all of the user's credentials. Third, they identify potential problems with all of a user's credentials but do not identify how significant the problem is or how to address it.

Participants' dislike of these credential audit services stems from the fact that these audits overwhelmed them with the sheer number of issues detected. This led most participants to ignore these health checks entirely, though many indicated they hoped to find time to address all the issues identified by the credential audit. This was demonstrated in R12's response regarding his impression of the health check tool in his manager:

> *"It's a very cool feature. However, it's, you know, the duplicate password thing, like, there's a bunch of passwords I've never changed because they don't have any financial implications for me. And so it just comes up every time. And so it's kind of become background noise for me, that when I click in, it pops up and says, 'Hey, you have a duplicate password here.' And then I go, oh, yeah, I gotta change that. And that's been about, I don't know, four or five years? I don't know. No, I don't remember how long anyways, it's a lot, you know, it's just white noise at this point, I just kind of dismiss it immediately. And there's an option to turn it off permanently. But I don't want that because someday I'm actually gonna take care of it."*

As the health audits were not generally effective in getting participants to update weak, reused, or compromised credentials, we asked participants under what circumstances they did update their credentials. Responses fell into one of three categories: (1) responding to a breach notification, (2) periodically for important accounts (but only essential accounts), or (3) never unless forced to by the website. The first two categories were mentioned in a response by R26:

> *"I would say maybe once or twice a year. I should probably do it more often, but…I would say typically the high priority ones, and then if there's something that just prompts me to change it for the other ones, I might do it as well, you know, you just read that, you know, there was a compromise of you know, 20,000 accounts. For example, I might just decided to change it as well, even if it's not too hypercritical."*

R12 described how their behavior fits into category three when asked how often they update passwords:

> *"I'm not proud of it, but about never. Yeah. things require me to basically, which a lot of important places do require me to banks and credit cards and things like that. But even they may be only required once a year, you know? Where probably should be frequent than that."*

5.4 Limited Mobile Usage

Participants rarely used mobile password managers, even if they were installed on their mobile devices. The reasons for this are far-ranging. First, the mobile experience is inconsistent, especially regarding autofill and autosave functionality, which is in line with findings from lab studies conducted by Seiler-Hwang et al. [31]. For example, R11 shared,

> *"My biggest annoyance with the Google and the Android OS password system is its inconsistency. It's just it sometimes works, and sometimes it doesn't. Sometimes it does what you expect it to do, and other times it doesn't."*

Similarly, when asked how they would retrieve their password after creating an account on mobile, R25 responded,

> *"I don't. That's the problem. Yeah, I don't because right now, Facebook, I know my password. So I can log in if I wanted to. But like say I didn't know the password. I would have to just go back to the app or go onto my computer or reset it or something like I just wouldn't be able to."*

Second, many participants had issues syncing credentials between their desktop and mobile systems. This was a bi-directional problem, with credentials saved on mobile not showing up in the desktop client and vice versa. This was especially problematic when participants used multiple managers. For those participants concerned about security, syncing issues led some to use easy-to-remember passwords when creating accounts on their mobile device, then updating those credentials to stronger passwords once they got home and could save those credentials in their desktop manager.

Third, participants rarely need to authenticate on their mobile devices. This can occur because of generally limited usage of mobile devices, websites, and apps. For example, R21 stated,

> *"And I started doing it on that to some degree, but there's only like, probably less than ten websites where I have*

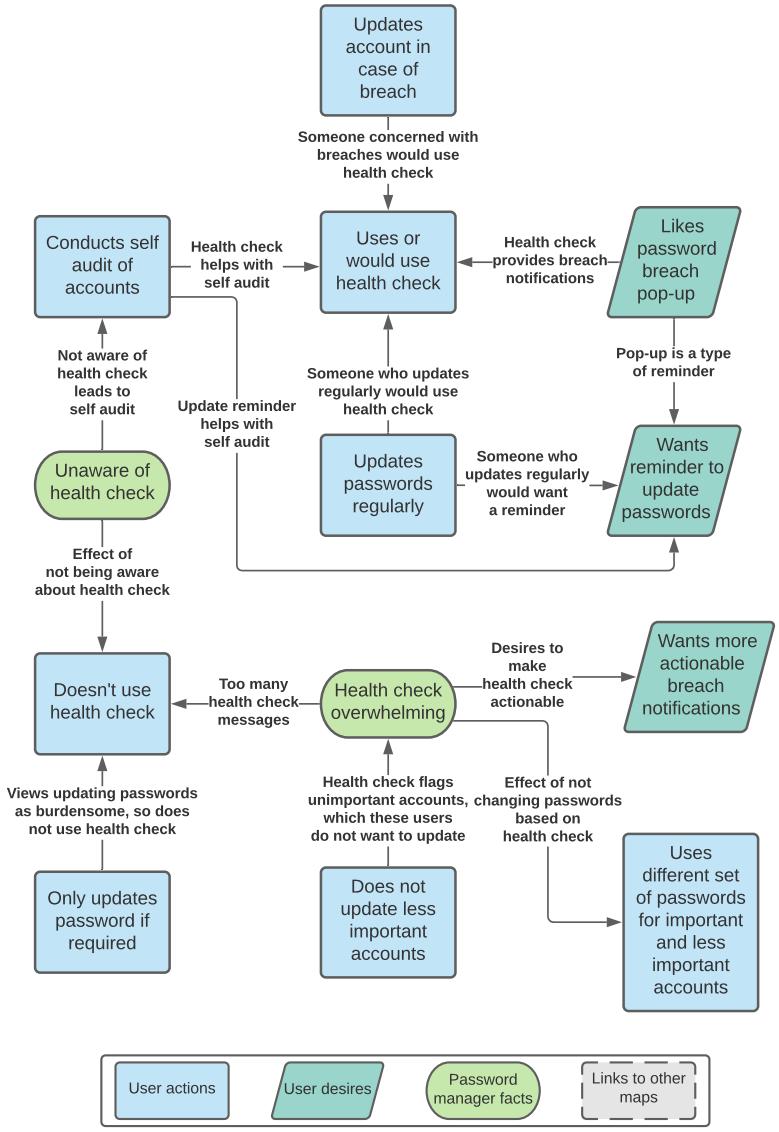

Figure 3: Concept map for account auditing and health check.

> *my password saved on my phone. Like, my laptop has a lot more."*

It also occurs because many websites and apps remain logged in nearly indefinitely after initial login. As shared by R19,

> *"I don't log into sites nearly as often on my phone. When I first set up the phone, I used it to actually authenticate into Reddit and authenticate into other things. But those remain logged in throughout the lifetime of the app as long as you're not, you know, logging out of it."*

Even when participants do use a mobile password manager, they often only use it as a credential store, copying and pasting credentials from the vault. As described by R1,

> *"But in the sense I only use it as like a reference book. If I had a book with me, with all my passwords in it, I would look one up. That is what I use it for."*

This usage pattern is concerning as past research has demonstrated that copy and pasting credentials are fraught with security vulnerabilities [7, 14]. As such, more work is needed to understand how mobile managers can be modified to better support users' needs and increase correct usage.

6 ADDITIONAL TOPICS

In addition to the core theories identified in our analysis, we explored other interesting topics with participants. In this section, we share additional results from our studies.

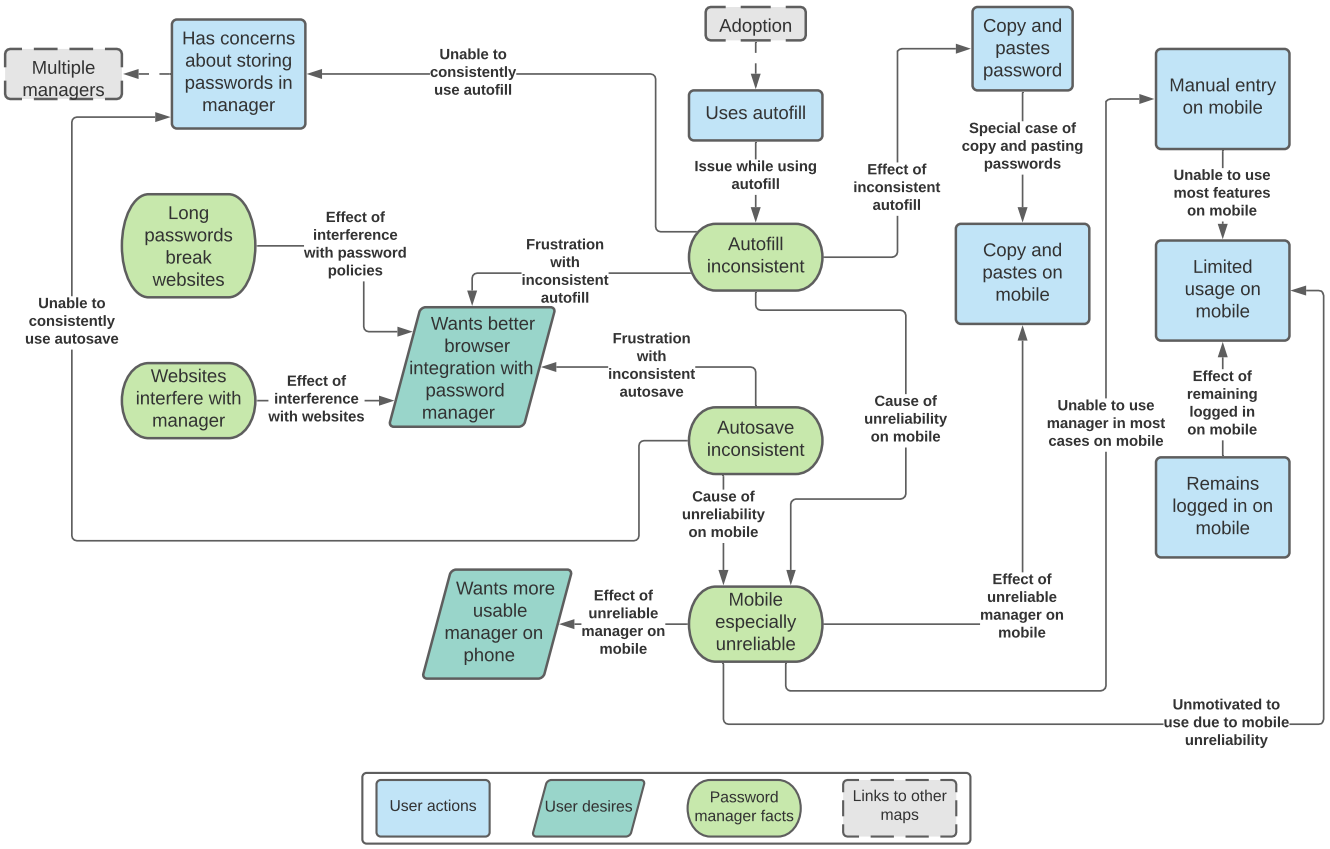

Figure 4: Concept map for limited manager usage on mobile devices. Users generally did not mind inconsistencies in autofill and autosave on the desktop, though they did want their manager to integrate better with their browser for a variety of reasons. However, mobile managers were especially unreliable, to the point that users often resorted to manual password entry and copy and paste. Given that many users remained logged in on mobile anyways, some users simply avoided the mobile manager altogether. This map links to the multiple manager usage map because concerns with mobile managers led to multiple manager usage. It links to the adoption map because the adoption of a mobile manager precedes the usage of autofill.

6.1 Adopting a manager

Participants generally adopted a password manager for one of three reasons: (1) requirements to use a password manager at work, (2) it makes their life easier, or (3) it allows them to increase the security of their online credentials. For example, R16 shared about their adoption reason:

> *"Actually, I didn't pick it. My job started forcing it. And then I just got used to it. I might as well just put it on my phone."*

When selecting which manager to adopt, external recommendation was the most common (n=8; 25%) reason given for manager selection. These often came from friends or other trusted online sources. For example, R26 stated the following about their chosen password manager:

> *"That was actually pretty much the first one that kind of popped up. You know, when I was looking for a password manager (online). I did speak with friends, and there is one friend that was using it and had just a good personal experience with it."*

In other cases, participants started using the built-in managers because they just clicked through the autosave and autofill dialogs presented by the built-in manager and discovered that they liked the manager. For example, R25 shared how the browser's built-in manager just started using them:

> *"It basically started using me. It just would ask me if I want to save my password. And then I would, and I guess I just thought that was standard. And then it would start telling me, like, I have 23 compromised passwords. And then I realize that this is like a whole system here."*

In some cases, adoption of the browser-based manager ended with the user only using the built-in manager, but in other cases, it led to the user eventually adopting an external manager.

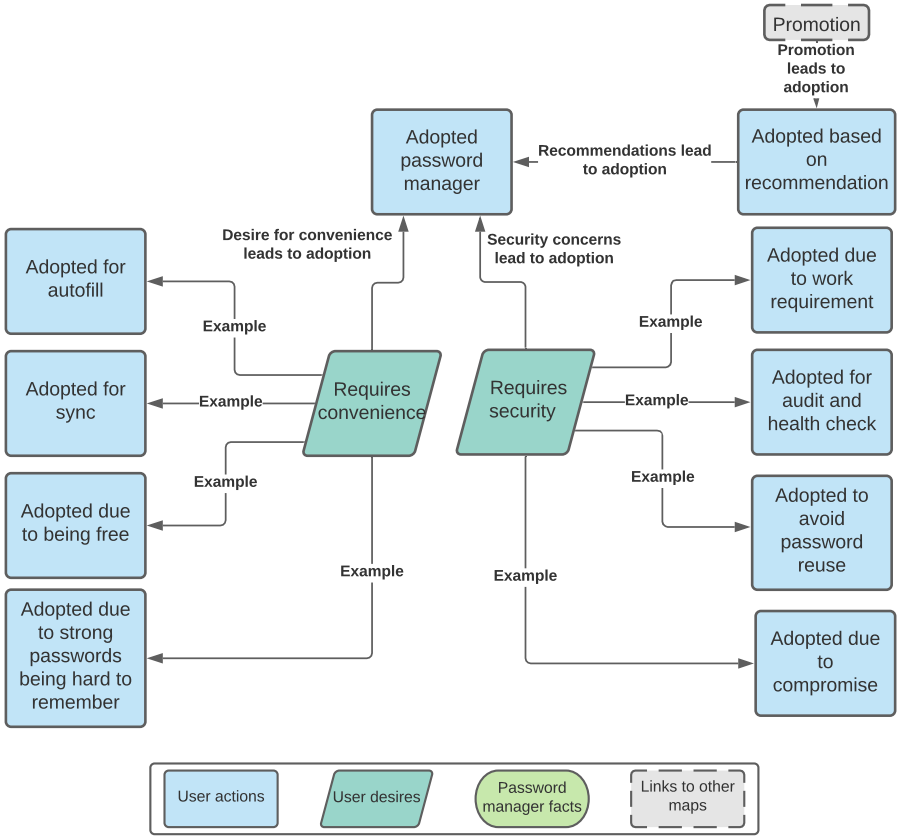

Figure 5: Concept map for adoption. Participants who adopted managers on their own generally did so either for the sake of convenience or to keep their accounts more secure. When participants adopted a manager based on a recommendation, it most often came from a friend or family member or a requirement to adopt a manager at work. This map connects to the promotion map because promotion may lead to adoption.

6.2 Promoting a manager to others

While participants overwhelmingly loved their passwords managers, they were somewhat unlikely to promote password manager usage to others. Even when they did promote the tool to others, it was often done in an off-handed manner, and they had limited success in getting others to adopt a manager. One reason for the lack of success was that other people did not have a correct mental model for how password managers improve convenience and security, and participants were unable to help them establish correct mental models. Regarding convenience, R23 shared their difficulty convincing others to use a manager:

> *"No one understands its utility or they just can't wrap their mind around how they would use a password manager because they're always trying to think, well I have to remember all these different passwords. No, you don't. You remember one password. Yeah, that's why I think I have no converts."*

Participants were most successful at getting others to adopt a manager when those individuals were family members or close friends. In these cases, convenience was usually the key selling point. For example, R10 describes how they got their mother to use a password manager:

> *"Yeah, so my mother, [who] uses either myself or my sister as technical support. She's not gonna remember a complex password by any means. And her default is to use her cat's name as a password. In this day and age, she just simply cannot do that for banking or brokerage accounts or anything like that. It's just, you can't do it. So we showed her how to use keychain herself. And it pretty much takes care of anything you have to do for you, especially if you're using it on your phone, and you could use face ID or whatever; like, you know, once you know how to use it, there's no work involved, and she's willing to do it. Whereas, for something more complicated, she wouldn't be willing to."*

One potential explanation for success among families is that there is a high level of trust in these situations, helping overcome adoption hurdles related to a lack of trust in password managers [1, 5]. Additionally, family members were willing to spend the time to help each other build correct mental models

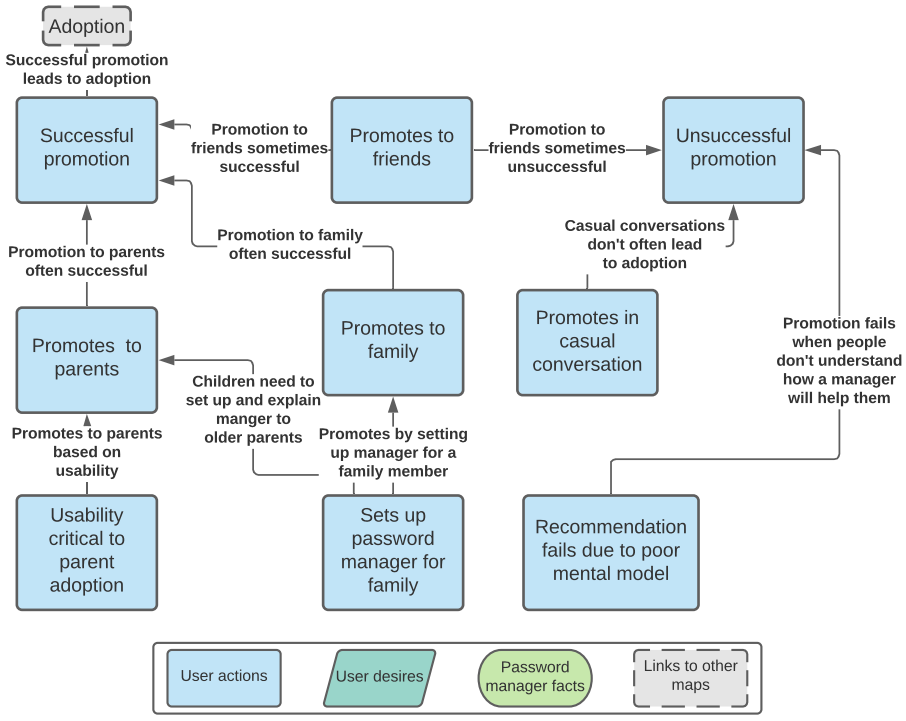

Figure 6: Concept map for promotion. Participants were most successful at promoting managers to immediate family members, parents, or close friends. Promotion in casual conversations was unsuccessful, and several participants (n=2; 6%) mentioned that promotion failed due to inaccurate mental models of how managers work.

related to threats and the efficacy of password managers, which according to the protection motivation theory (PMT) could explain why these interactions were more likely to induce adoption [6, 23].

6.3 Password Sharing

Participants indicated that they rarely needed to share passwords. However, when presented with examples of commonly shared accounts (e.g., video streaming services), they noted that they did share credentials with others. Still, this was not seen as a security-critical issue, and most participants felt comfortable sharing these credentials by phone or email.

Participants were nearly universally unaware of password sharing features present in managers. When made aware of this feature, most participants indicated that while it sounded cool, it would not be helpful because they did not have any acquaintances who also used their password manager. In contrast, several participants (n=3; 9%) mentioned that this feature would be most helpful in work settings where all users had the same manager.

R12 had attempted to share a password using LastPass but found the feature difficult to use:

> *"I did this (password sharing) with a friend. He was sharing with me using LastPass. And I figured with LastPass, everything would be pretty normal. But no, it came through and wanted, like, oh, I had to accept it. And then he got a notification. And then there's some temporary password that just doesn't give me his actual password. It does some sort of encryption… It's kind of like those blue boxes, right? You know the door locks for your house where you, you can authorize somebody to come in at one time, and then you delete it, right? That is the same thing. Except for, like, I said it didn't work. And then he shared it with me for a minute. And it popped in and out of six times. And every time I tried to use it, it would not work. And so he just ended up texting the password to me."*

In addition, several of the users who were aware of the password sharing feature did not know another person who used the same manager with whom they needed to share a password:

> Doesn't know anyone who has a password manager—P3: *"Most people are too lazy to set up a password manager. So I'll just send an email or something."*
> R26: *"Most of the people that have been in the scenario that you mentioned (need to share password), I don't believe are dashlane users. So it's probably a feature I've heard of, but I don't think it's a feature I've ever actually used. But I would."*

6.4 Inconsistencies Autofill and Autosave

In roughly half of the interviews, we observed managers failing to identify login forms and save new or modified credentials. Similar issues have been identified in laboratory settings [18, 31], and our results demonstrate that they frequently occur in the wild.

Participants indicated that these are common, not isolated, issues. For example, R14 notes that when websites split their login dialog across two screens—i.e., only being shown the password entry field after submitting a username—consistently causes autofill and autosave to fail. While participants were aware of these inconsistencies, they also indicated that they were not problematic enough to discourage their use of password managers, finding that the manager's convenience more than made up for these inconsistencies. Still, we believe that these issues should be addressed as the lack of participants' annoyance may be nothing more than survivor bias in our results.

To cope with these inconsistencies, particularly regarding autosave, many users save their credentials in multiple locations. This includes using multiple managers as well as writing them down physically or digitally. As shared by P1,

> *"I'll use the password generator, and I'll copy it from there into a notepad because I've had issues where the generated password doesn't go where I expect it to go. Or I even like lost it entirely. So I'll paste it over into Notepad, get my account created, make sure everything's sorted out in LastPass that the password and LastPass and the password I have in my notepad that I've copied and pasted over, make sure they match. And then I'll close the notepad if they do or fix any problems if there's a problem."*

6.5 Attitudes Towards Autolock

While autolock is a standard feature in external password managers, several participants (n=4; 13%) felt that having their manager periodically lock itself would be extremely annoying. For example, R14 indicated,

> *"That is a hindrance to somebody like me that works online all the time. I can't stand it, say, for example, I get up and go to the bathroom or get a drink or something. And then oh, my computer has gone to sleep. So I have to log in again? I'm sorry, I just don't have time for that. If I'm here, you know, it should be on."*

Even security conscience participants were unlikely to leverage time lockouts for their vault. The reasoning behind this was that they were not worried about the physical safety of their devices and thus believed autolock was not adding a meaningful layer of security, only inconvenience. For example, R11 expressed,

> R11: *"I use it at work, I don't use it at home. I used to use it at work much more often when I was in the office. Now that I'm at home, I still use it. But it's definitely not as prevalent. Because it is a good feature. It is good to have in case someone is walking by and they can see a password. But because I'm in my own house, and no one comes and sees me where I work in my home office. I don't need to worry about that security as much. But in a crowded office, where I would normally be working. It's very helpful."*

6.6 Ubiquitous Default Settings

In our study, only a single participant indicated that they updated settings for their password manager. This indicates that having safe defaults here is extremely important, as users are unlikely to fix any issues.

Similarly, most participants did not change the settings used by the password generator (if they used it at all). For the participants who updated password generation settings, there was no clear reasoning behind the settings they picked, other than understanding that having more characters is more secure. While this is true, it has a limited impact after a certain point. Based on our observations, password managers need to do better at assisting users to select appropriate password generation settings.

6.7 Desire for Single Sign-On

Even though participants could rely on their password managers to store and fill their credentials, they still preferred it when websites used single sign-on (SSO). The reasoning behind this preference was that they did not like creating new accounts for websites, regardless of whether those accounts were managed for them by the password manager. Additionally, participants preferred it when they did not need to store too many passwords in their manager. This may be connected to the fact that participants often memorized their passwords, even when they were also stored in the manager.

6.8 Impacts from COVID-19

A handful of participants (n=3; 9%) indicated that the COVID-19 pandemic had altered their password manager usage. R28 indicated that while they had previously used Face ID to access their mobile password manager, this was often not an option when they were wearing a mask. This caused them to drop back to typing their master password, which was not an enjoyable experience using the mobile keyboard. Several participants (n=3; 9%) indicated that they generally used their mobile phones less due to being at home with their desktop computers, further limiting their use of their mobile managers. Finally, R11 indicated that password sharing features would have been advantageous during COVID:

> *"Definitely—because emails can be intercepted. And depending on how high and the count [of passwords] I'm trying to share with them [is], it would be easier that way. Back before the pandemic hit, I would just write it down on a post-it note, show them, and then throw the post-it note in a confidential bin. We can't do that anymore. Because everyone's in a different part of the state."*

7 IMPROVING MANAGER USABILITY

Throughout our interviews, we identified usability issues in password managers. In this section, we make recommendations on how managers can address those concerns.

7.1 Multiple Manager Usage

Multiple manager usage has both security and usability implications. Regarding security, prior research has shown that browser-based managers are often vulnerable to a range of attacks [26]. While in many cases they may be better than using no manager at all, they are not better than using an external manager. However, our results demonstrate that even after adopting an external manager, built-in managers continue to function and store user credentials, either intentionally or because users click through autosave dialogs, putting credentials at unnecessary risk. As such, we believe that built-in managers either need to improve their security to be in line with external managers, or they need to automatically disable themselves when an external manager is installed. Regarding usability, multiple managers frequently interfere with each other's operation, lead to out-of-sync credentials, and may impede the full functionality of the managers.

To help reduce multiple manager usage, we recommend the following practices:

(1) During setup, external managers should walk users through exporting credentials out of their browser manager and then disabling the browser manager. While the ability to complete these tasks already exists, our study clarifies that users are not aware of how to complete these tasks or the need to do so.
(2) Improve the consistency of autosave and credential syncing operations. Problems with these two features caused users to adopt secondary managers as a fail-safe. Managers could also add features that help them be their own fail-safe—for example, storing previously generated passwords along with the website that was activated when they were generated in case the autosave process fails. Managers could then suggest credentials when users log in to a website that does not have linked credentials. Similarly, managers could provide better awareness regarding the sync status of credentials and help users proactively handle potential issues such as a device that has not synced for a long time.
(3) Provide credential storage backup features to help alleviate users' fears of losing credentials. These backups should include both digital and physical backups, as some users may only trust physical backups.

7.2 Generate Usable Passwords

Users avoid generating passwords because they are challenging to enter and remember when the manager is unavailable. Clearly, there is a need for more research into cross-device entry. This includes work exploring how often cross-device entry occurs, what devices and contexts it occurs in, and what input limitations are present for those devices. This information could help inform generation of easy-to-enter credentials [15, 16]. Additionally, more work is needed on generating memorable passwords [8] so that users can memorize more than a single generated password, especially within the time and effort constraints of password manager users. It would also be worthwhile to explore generating passwords based on simple dictionary words.

7.3 Seamless and Targeted Credential Audits

Credential audits, while helpful, are not the main reason users adopt or use password managers [1, 5, 13, 28]. As such, users are unlikely to search for audit tools proactively. Similarly, if these tools present users with too many issues, users are likely to ignore them and focus on the core features of the password managers.

To address these issues, we suggest the following changes. First, audits should execute automatically and then proactively prompt users with results from these audits (e.g., by showing a pop-up window). Second, notifications from the audits should be short and immediately actionable. Suppose there are many issues identified in the audit. In that case, users should initially only be shown the most critical issues, focusing on accounts users are likely to view as high value. Over time, the remaining issues can be surfaced to users, focusing on giving users an actionable amount of tasks.

7.4 Limited Usage of Advanced Features

Simmons et al. [33] systematized password manager use cases, splitting them into three categories: essential, recommended, and extended use cases. Essential use cases are supported by all browsers and include use cases such as setting up the manager, saving credentials, autofilling credentials, and generating passwords. In our study, participants described using all of these essential use cases, providing evidence for the taxonomy produced by Simmons et al.

Where managers distinguish themselves is in the set of use cases they implement from Simmons et al.'s list of recommended and extended use cases. Such use cases included the ability to audit credentials, recover access if the master password is lost, and to group credentials into identities. Managers are also differentiated by how they choose to implement these features. For example, whether the credential audit identifies old passwords, weak passwords, and/or compromised passwords.

In our study, users did not discuss using any of these advanced features that distinguish the different password managers. While perhaps not surprising, this is unfortunate, as these features can significantly improve password managers' utility, usability, and security. One potential way to address this issue is for password managers to make users aware of these advanced features more proactively. There is also a need for research into these features to ensure that they will be sufficiently usable to be adopted when users finally do discover them.

8 CONCLUSION AND FUTURE WORK

In this paper, we conducted observational interviews with password manager users. Our results confirm and expand prior findings of multiple manager usage [28, 34], finding that it is common among users regardless of technical background and that it serves a critical function within participants' usage of password managers. Our work also helps explain why prior studies found that users eschew password generation [22, 28], showing that this avoidance is primarily attributable to concerns about entering generated passwords on devices where the password manager was unavailable to autofill or lookup the credential. We report the first results regarding the utility and usability of credential audit checks, finding that significant research is needed to make these

important tools useful to users. We also find that usability issues with mobile managers are a significant impediment to their adoption and usage in the real world, confirming prior laboratory usability study results [31]. Finally, we describe why users adopted their password manager and discuss their efforts at promoting their manager to others, triangulating previous results regarding password manager adoption [1, 2, 5, 6, 13, 23, 28, 30].

We discuss how these results should reshape perceptions of password manager usage and identify future research directions in §1.1. In addition to these takeaways, our study also has implications for our approach to research on password manager usage. First, observation needs to be a critical component of password manager research.Because we observed users using their managers on their own devices, we identified issues not found in prior work, such as the frequent use of multiple managers and problems syncing across devices. To understand the critical importance of observation, consider that in our recruitment survey, all respondents indicated using only a single password manager. In contrast, our observational study revealed that over half of the participants used multiple managers. As such, simply interviewing users without observation is likely only to gain partial information regarding their actual usage. Similarly, while measurements conducted by instrumented tools are ideal for gathering real-world usage, observational interviews are still critical in getting the rationale behind behaviors observed by the instrumented tools.

Second, when surveying users about their password managers, it is imperative to ask more nuanced questions about what manager(s) they use, rather than phrasing the question so that they only provide a single manager. We suggest first asking, "Do you use a password manager provided by your browser? If so, which one(s)? (Chrome, Firefox, Edge, Other)" and then following that question with, "Do you use any additional password managers?" and "If you use multiple managers, which one is your primary manager?"

RESEARCH ARTIFACTS

Our full research instruments, the survey data, anonymized study transcripts, and an interactive version of our concept maps are available for download at https://userlab.utk.edu/publications/oesch2022observational.

REFERENCES

[1] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? In *2016 European Workshop on Usable Security*. Internet Society, 2016.

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

[3] Catherine L Anderson and Ritu Agarwal. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly*, pages 613–643, 2010.

[4] Simone Aonzo, Alessio Merlo, Giulio Tavella, and Yanick Fratantonio. Phishing attacks on modern android. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1788–1801, 2018.

[5] Salvatore Aurigemma, Thomas Mattson, and Lori Leonard. So much promise, so little use: What is stopping home end-users from using password manager applications? In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2017.

[6] Salvatore Aurigemma, Thomas Mattson, and Lori NK Leonard. Evaluating the core and full protection motivation theory nomologies for the voluntary adoption of password manager applications. *AIS Transactions on Replication Research*, 5(1):3, 2019.

[7] Talal Haj Bakry and Tommy Mysk. Precise location information leaking through system pasteboard. https://www.mysk.blog/2020/02/24/precise-location-information-leaking-through-system-pasteboard/, 2020. Accessed: 2020-06-13.

[8] Joseph Bonneau and Stuart Schechter. Towards reliable storage of 56-bit secrets in human memory. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pages 607–623, 2014.

[9] Sunil Chaudhary, Tiina Schafeitel-Tähtinen, Marko Helenius, and Eleni Berki. Usability, security and trust in password managers: A quest for user-centric properties and features. *Computer Science Review*, 33:69–90, 2019.

[10] Mark Ciampa. A comparison of user preferences for browser password managers. *Journal of Applied Security Research*, 8(4):455–466, 2013.

[11] Juliet M Corbin and Anselm Strauss. Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology*, 13(1):3–21, 1990.

[12] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 2873–2882, 2015.

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

[14] Sascha Fahl, Marian Harbach, Marten Oltrogge, Thomas Muders, and Matthew Smith. Hey, you, get off of my clipboard. In *International Conference on Financial Cryptography and Data Security*, pages 144–161. Springer, 2013.

[15] Kristen K Greene. Effects of password permutation on subjective usability across platforms. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 59–70. Springer, 2015.

[16] Kristen K Greene, Melissa A Gallagher, Brian C Stanton, and Paul Y Lee. I can't type that! p@ $$w0rd entry on mobile devices. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 160–171. Springer, 2014.

[17] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough? an experiment with data saturation and variability. *Field methods*, 18(1):59–82, 2006.

[18] N. Huaman, S. Amft, M. Oltrogge, Y. Acar, and S. Fahl. They would do better if they worked together: The case of interaction problems between password managers and websites. In *2021 2021 IEEE Symposium on Security and Privacy (SP)*, pages 1626–1640, Los Alamitos, CA, USA, may 2021. IEEE Computer Society.

[19] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. Privacy attitudes of mechanical turk workers and the us public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 37–49, 2014.

[20] Ambarish Karole, Nitesh Saxena, and Nicolas Christin. A comparative usability evaluation of traditional password managers. In *International Conference on Information Security and Cryptology*, pages 233–251. Springer, 2010.

[21] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. The emperor's new password manager: Security analysis of web-based password managers. In *USENIX Security Symposium*, pages 465–479, 2014.

[22] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. Better managed than memorized? studying the impact of managers on password strength and reuse. In *27th USENIX Security Symposium*, pages 203–220, 2018.

[23] Raymond Maclean and Jacques Ophoff. Determining key factors that lead to the adoption of password managers. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pages 1–7. IEEE, 2018.

[24] Philipp K Masur. *Situational privacy and self-disclosure: Communication processes in online environments*. Springer, 2018.

[25] Sean Oesch, Anuj Gautam, and Scott Ruoti. The emperor's new autofill framework: a security analysis of autofill on iOS and Android. In *Proceedings of the 37th Annual Computer Security Applications Conference*. ACM, 2021.

[26] Sean Oesch and Scott Ruoti. That was then, this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers. In *29th USENIX Security Symposium (USENIX Security 20)*, Boston, MA, Aug 2020. USENIX Association.

[27] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310. ACM, 2017.

[28] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, and Nicolas Christin. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019.

[29] Constantinos N Phellas, Alice Bloch, and Clive Seale. Structured methods: interviews, questionnaires and observation. *Researching society and culture*, 3:181–205, 2011.

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

[31] Sunyoung Seiler-Hwang, Patricia Arias-Cabarcos, Andrés Marín, Florina Almenares, Daniel Díaz-Sánchez, and Christian Becker. "i don't see why i would ever want to use it:" analyzing the usability of popular smartphone password

managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1937–1953, 2019.
[32] David Silver, Suman Jana, Dan Boneh, Eric Yawei Chen, and Collin Jackson. Password managers: Attacks and defenses. In *USENIX Security Symposium*, pages 449–464, 2014.
[33] James Simmons, Oumar Diallo, Sean Oesch, and Scott Ruoti. Systematization of password manager use cases and design paradigms. In *Proceedings of the 37th Annual Computer Security Applications Conference*. ACM, 2021.
[34] Elizabeth Stobert and Robert Biddle. Expert password management. In *International Conference on Passwords*, pages 3–20. Springer, 2015.
[35] Ben Stock and Martin Johns. Protecting users against xss-based password manager abuse. In *Proceedings of the 9th ACM symposium on Information, computer and communications security*, pages 183–194. ACM, 2014.
[36] Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. Can unicorns help users compare crypto key fingerprints? In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3787–3798, 2017.

A SCREENING SURVEY

Q1. Which password manager do you use?
∘ *LastPass* ∘ *Bitwarden* ∘ *KeePass* ∘ *1Password* ∘ *Dashlane* ∘ *Other*

Q2. On what devices do you use your password manager? Select all that apply.
∘ *Desktop PC* ∘ *Laptop* ∘ *Phone* ∘ *Tablet* ∘ *Other*

Q3. Would you be willing to participate in a one-on-one Zoom interview with our research group about how you use your password manager? You will receive compensation for your time. The interview will be less than one hour and will be recorded. As part of the interview, you will share your screen and demonstrate how you use your password manager to complete several tasks. Your interview data will be anonymized and kept confidential.
∘ *Yes* ∘ *No*

Q4. Please rate the following statements about your password creation and usage. Options: Never, Rarely, Sometimes, Often, Always
∘ *I do not change my passwords, unless I have to.* ∘ *I use different passwords for different accounts that I have.* ∘ *When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.* ∘ *I do not include special characters in my password if it's not required.*

Q5. On a 5-point scale ranging from 1 = not at all concerned to 5 = very concerned, how concerned are you about. . .
∘ *How concerned are you about institutions, public agencies, or intelligence services monitoring your online communication?* ∘ *How concerned are you about website or app providers sharing your data with unknown third parties?* ∘ *How concerned are you about other people getting information about you without your consent?* ∘ *How concerned are you about someone misusing your identity on the Internet?* ∘ *How concerned are you about other people spreading information about you without your knowledge?*

Q6. Do people ask you for computer-related advice?
∘ *Yes* ∘ *No*

Q7. Do you know at least one programming or scripting language?
∘ *Yes* ∘ *No*

Q8. How often do you use the programming or scripting languages you know?
∘ *Daily* ∘ *Weekly* ∘ *Monthly* ∘ *Rarely*

Q9. What is your gender?
∘ *Male* ∘ *Female* ∘ *I prefer not to answer* ∘ *Other*

Q10. What is your age?
∘ *Under 21* ∘ *21-34* ∘ *35-44* ∘ *45-54* ∘ *55-64* ∘ *Above 64* ∘ *I prefer not to answer*

Q11. What is the highest level of school you have completed or the highest degree you have received?
∘ *Less than a high school degree* ∘ *High school or GED* ∘ *Some college* ∘ *Trade/vocational/technical* ∘ *Associates (2-year)* ∘ *Bachelors (4-year)* ∘ *Masters* ∘ *Professional* ∘ *Doctorate* ∘ *I prefer not to answer*

Q12. Please specify your ethnicity.
∘ *Hispanic or Latino* ∘ *American Indian or Alaska Native* ∘ *Asian* ∘ *Black or African American* ∘ *Native Hawaiian or Other Pacific Islander* ∘ *Caucasian or White* ∘ *Multiracial* ∘ *Other* ∘ *Prefer not to say*

B INTERVIEW SIGN UP SURVEY

Q1. Rate the following statements regarding device security. Options: Never, Rarely, Sometimes, Often, Always
∘ *I set my computer screen to automatically lock if I don't use it for a prolonged period of time.* ∘ *I use a password/passcode to unlock my laptop or tablet.* ∘ *I manually lock my computer screen when I step away from it.* ∘ *I use a PIN or passcode to unlock my mobile phone.*

Q2. Rate the following statements regarding general security habits. Options: Never, Rarely, Sometimes, Often, Always
∘ *When someone sends me a link, I open it without first verifying where it goes.* ∘ *I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.* ∘ *I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).* ∘ *When browsing websites, I mouseover links to see where they go, before clicking them.* ∘ *If I discover a security problem, I continue what I was doing because I assume someone else will fix it.*

Q3. Rate the following statements regarding software updates. Options: Never, Rarely, Sometimes, Often, Always
∘ *When I'm prompted about a software update, I install it right away.* ∘ *I try to make sure that the programs I use are up-to-date.* ∘ *I verify that my anti-virus software has been regularly updating itself.*

Q4. Enter your MTurk ID below so that we can compensate you $26 after the interview.

Q5. Signup for an interview using this link: https://calendly.com/...

Q6. Enter the meeting ID that you received for your Zoom meeting in the box below.

Q7. Do you use a password manager on your mobile device?
○ *Yes* ○ *No*

If you use your password manager on your mobile device, watch one of the following instructional videos on how to share your screen in Zoom from a mobile device. Please make sure to install Zoom on your mobile device and know how to share your screen prior to the interview if you use your password manager on your mobile device.

Below are some resources that can help you get setup:

(1) Instructions Share Screen Android—0:12–0:50—https://www.youtube.com/watch?v=H0uHVjJQ740
(2) Instructions Share Screen iOS—0:21–0:37, 1:02–1:13—https://www.youtube.com/watch?v=aydCQcYtpwc&t=90s
(3) https://support.zoom.us/hc/en-us/articles/115005890803-iOS-Screen-Sharing

C SEMI-STRUCTURED INTERVIEW SCRIPT

Opening

"First off, thanks for participating in our research. As a reminder, we are going to be recording this session. Is that still Ok?" (If no) Let them know that unfortunately they will be unable to participate in the study. You may now end the study without paying them.

"My name is Sean Oesch and I am a research assistant at the University of Tennessee. In my research group we are trying to understand how people use technology to secure their lives. Our goal is to create security tools that better meet the needs of users like yourself. In this study, we are trying to understand how you use your password manager, [NAME], so that we can improve it to better fit your needs. So the main goal of this study is to understand the way that you use [NAME] in your life.

There are no right answers or responses. We really just want to see how you normally use [NAME]. So just do whatever you would normally do. And if something is hard for you, that is a problem with [NAME] and not with you. Our goal is to make [NAME] better, so any problems you have using it will help us know the ways that [NAME] can be improved. And if at any point in the interview something pops into your mind that you think would help us understand how you use [NAME], please feel free to stop me and share your thoughts.

"Now, let's talk about the structure of the interview just so you know what to expect. The entire interview should take under an hour. I'm going to start by asking you some basic questions about how you use [NAME].

After that, we're going to ask you to share your screen and show us how you use [NAME] on your own device. To protect your privacy and ensure we don't accidentally see any account information, before you share your screen in the interview, we're going to have you log out of [NAME]. We'll then have you login to [NAME] using an email and password that we provide to you.

"Next, I'll ask you to create an account on several websites the same way you normally would in real life, except that you will use an email address I provide to protect your privacy. The reason for doing that is that we want to understand how you use [NAME] when you create and manage accounts. We're not going to ask you to do anything other than create, log in to, or log out of an account on any of the websites we visit. And we'll be deleting all of these accounts after the interview."

Then, if you use your password manager on your mobile device, I'll have you join this Zoom call with your phone and you will complete a few tasks on your phone with [NAME]. At that point we'll close with a few final questions and then wrap up."

If you need any help sharing your screen with Zoom or have any additional questions, please let me know. We just want you to focus on helping us understand how you use [NAME], so just let me know if you run into any issues.

"Before we begin the interview, do you have any questions for me?

"Great! Let's get started."

Pre-interview Checklist:

(1) Enable multiple participant screen sharing
(2) Ask participant to disable webcam
(3) Ask participant to log out of accounts on all relevant devices
(4) Verify participant is able to share their screen from all relevant devices
(5) Start Recording

Interview

Generic questions about usage and login

"First, let's discuss how you use your password manager on your desktop or laptop."

(1) "How often do you use [NAME]?"
(2) "How did you pick [NAME] as your password manager?"
(3) "How did you pick your master password?"
(4) "Do you use anything in addition to your master password to protect your [NAME] account?"
(5) Do you ever suggest that other people use [NAME]? Do you promote password managers to friends or family?" If yes - "What does that look like? What is your motivation for doing so?" If no - "How come?"
    (a) Do you know anyone who has adopted as a result?
(6) Do you ever save your passwords anywhere other than [NAME], such as in Chrome or Firefox?
    (a) If yes - "Why do you use both? How do those two work together? Do you have the same passwords in both?"

Account setup

(1) "When was the last time you set up [NAME] on a new device?"
(2) Before we continue, you'll need to log out of [NAME]. If you need any guidance on how to do that just let me know.
(3) Could you please share your screen now. Wait for them. Could you now login to your password manager using the login information I just sent you over chat. Wait for them."
    (a) "Assuming you had just installed this password manager, would you change any of the default settings before using it? Could you show us which ones?

Register a new account

(1) "We're now going to have you set up an account on Reddit. Have you ever used Reddit before?"
    (a) If no - "Alright, so Reddit is a social media platform where users share news and custom content that they've created."

(b) If yes - "If you are currently logged in to reddit.com, we'll have you log out before creating a new account."
(2) "Now, go ahead and navigate to reddit.com and sign up for a new account with the email I provided. After we are done with the interview, we will delete this Reddit account."
(a) Now that you're done, go ahead and log out of Reddit.
(3) "Now we're going to have you perform a similar task for ebay.com."
(a) Now that you're done, go ahead and log out of ebay.com.
(4) "Do you ever experience problems when trying to save new accounts in [NAME]?"
(5) "Do you normally store credentials for sites like Reddit and Ebay in your password manager? More generally, what types of accounts do you store in [NAME]?"
(a) How do you store passwords if you don't save them in [NAME]?
(6) Thank them

Logging in and updating an existing account

(1) "Now let's go back to Reddit and login"
(2) "Do you ever experience problems when trying to login to websites that you've saved in [NAME]?"
(3) Now let's say you need to update your password for Reddit. Show us how you would go about updating your password for reddit."
(a) If they seem to be searching for a password reset in settings, tell them how to get there.
(4) Now do the same for Ebay
(5) How often do you update passwords?

Other common tasks

(1) Creating a password
(a) "When you want to create a new password, how do you normally go about doing that?"
(b) "Do you create passwords differently for different types of websites?"
(2) Autolock and log out
(a) How often do you log out of your password manager? (desktop/phone)
(b) Does your password manager ever automatically log you out/lock? What is your opinion of that feature?
(3) App Autofill
(a) Do you ever use your pwm to fill apps on your desktop?
(b) (If yes) Do you ever encounter issues when doing so?
(4) Sharing a password
(a) "If you wanted to share a password with someone, how would you normally go about doing that?"
(b) "Did you know that you can share passwords directly with other [NAME] users?"
(c) If no - "Would you like to check it out?"
(d) After showing - "Is this a feature you'd like to use in the future?"
(5) Password health check
(a) "If you wanted to check if any of your passwords were weak or had been compromised in a data breach, how would you normally go about that?"
(b) "Did you know that [NAME] can help you identify weak and compromised passwords?"
(c) If no - "Would you like to check it out?"
(d) After showing - "Is this a feature you'd like to use in the future?"
(6) "We've gone through using [NAME] to create and use accounts, as well as some additional features. Are there any other features of [NAME] you use that we haven't covered? Can you show us?"

"You can stop screen sharing"

Mobile usage

(1) "Do you use [NAME] on your mobile phone?"
(a) If no, skip rest of section
(2) "What are some of the differences between how you use [NAME] on your desktop versus on your phone?"
(a) "Do you create accounts for websites on your mobile device?" If so, "Do you ever encounter problems?"
(b) "Do you use your password manager to log in to apps on your phone?" If so, "Do you ever counter issues when using [NAME] to log into apps?"
(c) "Do you generate passwords on your mobile device?" If so, "How does your experience of generation on mobile devices compare to that on the desktop?"
(3) If they actually use any functionality on their phone - "We want to see how it works for you on mobile. We're going to have you join this Zoom call on your phone and share your screen."
(4) Could you please login to Reddit now.
(a) Great, thanks. Could you log out of reddit now. This is the last we'll use reddit.
(5) If they create accounts on their phone - "We're going to have you create an account again. This time it's going to be for memrise.com, a language learning platform.
(a) "Alright, go ahead and create an account for memrise.com"
(b) If they autofill apps on their phone -"Great, now let's try using the credentials you just created to log in to the memrise app. Please download the memrise app on your device and login using the credentials that you just saved in your password manager."

You can stop sharing your screen.

Other remarks

(1) "Thanks for participating in our interview. Before we wrap up, is there anything left you would like to share that you think would be helpful for us to understand?"
(2) "If there was one feature you could add or thing you would change about [NAME], what would it be?"
(3) If anything else you think would be helpful occurs to you at a later time, feel free to send us an email at userlab@utk.edu.

Explain compensation

(1) We will pay you via a bonus on mturk
(2) Let's verify mturk id for payment - what is your full mturk id? You can just paste that into the chat if that's easier for you.

D CONSENT FORM FOR SCREENING SURVEY

Overivew

Research study title: Password manager screening survey for interviews Time commitment: This survey will take about 5–10 minutes to complete. Compensation: You will be paid $1 for your participation. Requirements: You must be age 18 or older to participate in this study.

In our research group, we are trying to understand how people use password managers so that we can make them more usable and secure. As part of this effort, we want to conduct interviews with individuals regarding their password manager usage. This survey is intended to help us identify potential participants for these interviews.

What will I do in this study?

You will answer demographic questions and questions about your usage of password managers.

Can I say "No"

Being in this study is up to you. After completing the study, we cannot remove your responses because we will delete any information linking your response to your turker ID after we have selected our interview participants.

Are there any risks to me?

We don't know of any risks to you from being in the study.

Are there any benefits to me?

We do not expect you to directly benefit from being in this study. Your participation may help us to learn more about password managers and how they are used, providing indirect benefits.

What will happen with the information collected for this study?

The information from this survey will be used to identify potential participants for an interview on their usage of their password manager. If you are selected, we will offer you a second HIT that can be used to signup and participate in the interview.

Overall demographics and responses to the survey questions will be published and possibly presented at scientific meetings. These results will be anonymous and no one will be able to link your responses back to you. As such, please do not include your name or other information that could be used to identify you in your survey responses.

Will I be paid for being in this research study?

You will be paid $1 when you complete the survey.

Who can answer my questions about this research study? If you have questions or concerns about this study, or have experienced a research related problem or injury, contact the researcher, Scott Ruoti at ruoti@utk.edu.

For questions or concerns about your rights or to speak with someone other than the research team about the study, please contact:

Institutional Review Board
The University of Tennessee, Knoxville
1534 White Avenue
Blount Hall, Room 408
Knoxville, TN 37996-1529
Phone: 865-974-7697
Email: utkirb@utk.edu

Statement of Consent

I have read this form, been given the chance to ask questions and have my questions answered. If I have more questions, I have been told who to contact. By clicking the survey link below, I am agreeing to be in this study. I can print or save a copy of this consent information for future reference. If I do not want to be in this study, I can close my internet browser.

[Survey Link]

Provide the code given to you when completing the survey.

E CONSENT FORM FOR INTERVIEW

Overview

Research study title: Password manager usage interview Time commitment: Signing up for an interview will take about 2 minutes; the interview will take between 30–60 minutes. Compensation: You will be paid $1 for signing up for the interview. After completing the interview, you will be paid $25 as a bonus to this hit. Requirements: You must be age 18 or older to participate in this study.

In our research group, we are trying to understand how people use password managers so that we can make them more usable and secure. As part of this effort, we are conducting interviews with individuals regarding their password manager usage. Based on your answers to an earlier screening survey, you have been selected to participate in these interviews.

What will I do in this study?

In this study you will conduct an interview regarding your password manager usage. This interview will take place over Zoom. During the interview, we will ask that you share your screen at several points so that you can demonstrate how you use your password manager. We will take precautions to avoid recording any sensitive information during the screen shares. You are not required to share video from your webcam during the interview.

Can I say "No"

Being in this study is up to you. After completing the interview, it will not be possible to remove your responses as we will delete any data linking your responses to you.

Are there any risks to me?

We don't know of any risks to you from being in the study.

Are there any benefits to me?

We do not expect you to directly benefit from being in this study. Your participation may help us to learn more about password managers and how they are used, providing indirect benefits.

What will happen with the information collected for this study?
As part of this study, we collect your name and email address so that we can communicate with you. We also keep records of audio from your interview and screen recordings of you using your password manager on your own devices. This We will keep and publish results from this study, including quotes from participants' interviews.

The information collected in this study will be analyzed to identify how to improve the usability and security of password managers. We will record the audio from your interview and the video from the screen recordings, but no other video data. This data is only accessible to research staff at the USER Lab and the raw data will be destroyed at the completion of our research.

These results will be published and possibly presented at scientific meetings. We will clean this data to ensure that this data contains no personally-identifiable information. When referring to participant statements, we will do so using an anonymized label (e.g., 'R12 said, . . . ').

Will I be paid for being in this research study?
You will be paid $1 for signing up for the interview. After completing the interview, you will be paid $25 as a bonus to this hit.

Who can answer my questions about this research study?
If you have questions or concerns about this study, or have experienced a research related problem or injury, contact the researcher, Scott Ruoti at ruoti@utk.edu.

For questions or concerns about your rights or to speak with someone other than the research team about the study, please contact:

Institutional Review Board
The University of Tennessee, Knoxville
1534 White Avenue
Blount Hall, Room 408
Knoxville, TN 37996-1529
Phone: 865-974-7697
Email: utkirb@utk.edu

Statement of Consent
I have read this form, been given the chance to ask questions and have my questions answered. If I have more questions, I have been told who to contact. By clicking the link to signup for an interview, I am agreeing to be in this study. I can print or save a copy of this consent information for future reference. If I do not want to be in this study, I can close my internet browser.

[Interview sign up link]

F PARTICIPANT MANAGER USAGE DEMOGRAPHICS

		Participant	Desktop	Mobile
Multiple managers	External and browser-based	R2	LastPass + Chrome less important accounts	None—look up in Desktop LastPass sometimes
		R3	LastPass + Chrome for all accounts (as backup)	LastPass for autofill but not account creation
		R9	LastPass + Chrome for all accounts (as backup)	LastPass for apps + Chrome for websites
		R12	LastPass + Chrome for accounts that end up in Chrome	LastPass + Android OS for accounts that end up in it
		R13	LastPass + Chrome for all accounts	None
		R14	RoboForm + Chrome occasionally	None
		R15	1Password + Chrome occasionally	1Password + Chrome occasionally
		R16	LastPass + Chrome for all accounts	LastPass + Chrome
		R18	LastPass + Chrome occasionally	LastPass
		R19	KeePass + Firefox for common logins	Keepass2Android
		R20	KeePass + Chrome for common logins	None—look up in Desktop KeePass
		R23	KeePass + Chrome	KeePassDroid + Chrome in browser
		R24	Dashlane + notepad + Chrome occasionally	Chrome + desktop Dashlane as reference
	Other pattern	R6	LastPass	iCloud Keychain
		R7	Chrome for work / Safari personal—nonimportant accounts	aWallet—uses this for all important accounts / Safari
		R11	Chrome for personal + PasswordSafe at work	Android OS (Chrome)
		R17	Chrome	iCloud Keychain
		R21	Chrome + Word doc at work	Chrome
		R25	Chrome + notepad financial accounts	None
		R26	Dashlane + notepad financial accounts	None
		R27	Chrome + Firefox	Android OS (Chrome)
Single manager		R1	LastPass	LastPass as reference book on phone (no autofill/save)
		R4	LastPass	None
		R5	iCloud Keychain	iCloud Keychain
		R8	Chrome	None
		R10	iCloud Keychain	iCloud Keychain
		R22	Chrome	Chrome
		R28	Dashlane	Dashlane
		P1	LastPass	LastPass
		P2	Bitwarden	Bitwarden
		P3	1Password	1Password
		P4	KeePass	None