Understanding How People Share Passwords

Phoebe Moh and Andrew Yang, *University of Maryland;*
Nathan Malkin, *New Jersey Institute of Technology;*
Michelle L. Mazurek, *University of Maryland*

https://www.usenix.org/conference/soups2024/presentation/moh

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

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

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

Understanding How People Share Passwords

Phoebe Moh, Andrew Yang, Nathan Malkin*, Michelle L. Mazurek
*University of Maryland, *New Jersey Institute of Technology*

Abstract

Many systems are built around the assumption that one account corresponds to one user. Likewise, password creation and management is often studied in the context of single-user accounts. However, account and credential sharing is commonplace, and password generation has not been thoroughly investigated in accounts shared among multiple users. We examine account sharing behaviors, as well as strategies and motivations for creating shared passwords, through a census-representative survey of U.S. users ($n = 300$). We found that password creation for shared accounts tends to be an individual, rather than collaborative, process. While users tend to have broadly similar password creation strategies and goals for both their personal and shared accounts, they sometimes make security concessions in order to improve password usability and account accessibility in shared accounts. Password reuse is common among accounts collectively shared within a group, and almost a third of our participants either directly reuse or reuse a variant of a personal account password on a shared account. Based on our findings, we make recommendations for developers to facilitate safe sharing practices.

1 Introduction

It is generally assumed that an individual's password is a secret that no one else knows; yet, in reality, sharing passwords for online accounts is widespread. People share credentials for a variety of rational reasons, including for work, finances, convenience, or as a sign of trust among romantic partners and family members [4, 32, 33, 34, 43]. Others share accounts with trusted parties out of necessity, such as in the case of refugees, older adults, and other members of at-risk populations [26, 42, 49]. In many such cases, users perceive these needs to be a higher priority than account security.

Instead of repeatedly and ineffectually warning users against sharing [52], technology creators and security experts should endeavor to design systems that take into account the reality of sharing. To do so effectively, it is important to understand how credential sharing works in practice. How users create and distribute passwords for shared accounts has important security implications. If users judiciously create unique credentials for sharing, then perhaps the current emphasis on discouraging sharing is misplaced. On the other hand, reusing passwords across personal and shared accounts creates risks to these personal accounts. In this case, new interventions—whether in terms of new system designs that accommodate sharing, better user education, or both—may be needed.

Further, while password creation has been extensively studied in the single-user setting [7, 46], less attention has been devoted to shared accounts. If password creation strategies for intended-to-be-shared accounts differ importantly from single-user-account strategies, different guidance (password meters, strength requirements, suggested strong passwords) may be needed. If these passwords are created collaboratively with the input of multiple users, rather than being dictated by a single user, the situation may be even more complex.

Thus, by understanding how and by whom shared account passwords are created, the motivations behind password strategies these users employ, and whether these shared passwords are reused and in what context(s), we hope to inform safe account sharing practices and design. To do this, we study the following research questions:

RQ1: **Is password creation in shared accounts a collaborative process, or is it predominantly individual? Who is involved in the password creation process?**

RQ2: **When users create passwords for shared accounts, are their priorities and strategies similar to when**

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

they create passwords for personal (non-shared) accounts?

RQ3: **How prevalent is password reuse among shared accounts? Are these passwords also reused for personal accounts?**

To answer these questions, we conducted a census-representative online survey ($n = 300$) among U.S. users. We found that participants tend to share accounts (predominantly streaming accounts) with a small number of users, typically romantic partners and family members. In addition:

- Approximately half of accounts surveyed were originally created with the intention of being shared; the other half began as personal accounts that later became shared. In the latter case, users often do not change the passwords of these personal accounts when they begin to share them.
- Password creation for shared accounts tends to be an individual rather than a collaborative process, and users tend to have similar password creation strategies for both their personal and shared accounts. However, password makers will sometimes take the capabilities of other users into consideration or make security concessions in order to improve access to the shared account.
- Shared-account passwords are frequently reused. Users often have a *group password* for sharing multiple accounts among approximately the same set of users. More concerningly from a security point of view, about a third of participants report reusing (either exact or variant-of) passwords between personal and shared accounts.

Based on our findings, we provide recommendations for technology creators to facilitate safe account sharing while minimizing potential harms.

2 Related work

Reasons and contexts for credential sharing. Account sharing within households and among romantic partners is driven by convenience, practicality, and reinforcing trust [24, 34]. Similarly, account sharing can be used to affirmation of trust between adolescents [33]. Customers of paid accounts have a financial incentive for sharing [18].

People may also share credentials out of necessity. Members of at-risk populations, such as refugees or older adults, often rely on trusted parties for important tasks or to maintain safety [26, 42, 49]. For example, Kenyan cybercafe customers with limited experience with computers sometimes rely on cybercafe managers to remember and manage their account login credentials in order to access essential services [27].

In workplace settings, coworkers share credentials to facilitate sharing files and resources [43], though difficulties often arise from working around systems built on the one user, one account assumption [16, 21]. Cultural norms and expectations can be another driving reason for credential sharing, e.g., among bank customers in Saudi Arabia [4] or young adults in Bangladesh [3].

Account sharing can also continue after people want to stop it. In particular, Park et al. highlighted the difficulties of ending account sharing for romantic partners in the event of breakups, and Obada-Obieh et al. examined the cognitive and psychosocial burdens associated with ending account sharing [30, 34]. While we do not focus on adversarial relationships in this work, account sharing can also be used as a means of surveillance [5].

Kaye argued that password sharing is a nuanced social process rather than a deviant behavior to eliminate [19]. Indeed, these complex social processes are often important for maintaining security—for example, by small groups sharing digital resources to defend against insider and outsider threats [51, 53]. Some paradigms, such as family accounts, embrace account sharing and are designed around allowing multiple users to use a single account in an effort to enforce security without relying solely on social norms [12].

Taking into account the multitude of reasons for account sharing, password sharing is not likely to disappear anytime soon. Although motivations for account sharing are well-documented, the next step in the process—creating a password for the shared account—is not. Our study addresses this gap in knowledge.

Password generation and management by individual users. How people choose passwords for single-user accounts has long been studied both in the field and in the lab. Bryant and Campbell found that their surveyed participants often used meaningful data, such as nicknames, in their email passwords, and both partial and exact reuse of passwords across accounts was common [7]. Ur et al. observed password creation in the lab, finding that while most participants had a well-defined process for creating new passwords, many had misconceptions of what makes a password secure [46]. Studies comparing the security behaviors of experts with non-experts have found that non-experts tend to rely on memory to recall their passwords [8, 17].

Despite attempts at educating users, insecure behavior around passwords persists, often stemming from users' attempts to cope with the sheer number of passwords in daily life. In Stobert and Biddle's 2014 interview study, participants reported having a median of 27 accounts, and the authors found that these users ration effort to best protect important accounts by adopting less secure behaviors, such as reuse and writing down passwords, for accounts they deemed less sensitive or less frequently used [44]. Ur et al. and von Zezschwitz et al. similarly observed participants constructing weaker passwords for less-sensitive accounts [46, 48].

Partial or full reuse of old passwords represents one common effort rationing strategy. Das et al. estimated in 2014 that

43% of their participants directly reused passwords [10]. Shay et al. observed that most of their participants opted to modify an old password instead of creating an entirely new one in response to a university's password policy change [41]. Inglesant and Sasse noted that their participants often used "good" passwords as a resource to generate new passwords, and von Zezschwitz et al. found that weak passwords used by interviewed participants had roots in the first passwords they created [16, 48]. Wash et al. observed participants reusing passwords that were more complex and frequently-entered [50]. Users in Hanamsagar et al.'s study willingly traded security for memorability by reusing passwords in order to manage having many accounts [15]. Misconceptions about the risk of attacks and attacker capabilities were also a contributing factor to password reuse and weak passwords [15, 47]. Often, modifications made to old passwords to generate new passwords are small enough for an attacker aware of typical user behavior to guess the new password [10, 54].

While password creation strategies and motivations have been well-studied in the single-user context, we seek to expand this understanding to the multi-user context. Our explicit focus on shared accounts is an important lens for considering password behaviors employed by users.

Password managers. Security experts often recommend password managers as a means for users to cope with the ever-increasing number of passwords [6]. However, despite password managers' utility, only a relatively small proportion of users employ them. Those who do not use password managers, such as older adults, often cite security concerns and a lack of trust in password managers [35, 36]. While some password managers have aimed to support multi-user contexts [1, 22, 29], it remains unclear how often these features are used.

3 Methods

We designed our survey to understand how people share passwords in their day-to-day lives. We initially developed our protocol by adapting questions from related work on single-user password creation and interviewing seven people in the researchers' personal networks about their account sharing behaviors [7, 10, 40, 47]. To gather feedback, we piloted our survey with eight participants in think-aloud interviews and revised survey wording and presentation for clarity between interviews. Before final deployment, we further piloted the survey with 10 online participants.

Data collection took place in January and February 2023. Table 1 shows the demographic breakdown of our participants. All participants provided informed consent before beginning the survey, and the study was approved by the University of Maryland's institutional review board (IRB).

		Percent	Count
Gender	Female	47.7%	143
	Male	50.3%	151
	Nonbinary	<1.0%	1
Age	18-29	21.0%	63
	30-39	18.0%	54
	40-49	18.3%	55
	50-59	17.7%	53
	60+	23.3%	71
Annual household income	<$50k	33.7%	101
	$50k - $100k	38.7%	116
	>$100k	24.3%	73
Education	<High school	1.0%	3
	High school or equiv.	29.0%	87
	Bachelor or associate	52.0%	155
	Advanced degree	16.7%	50
CS background	Yes	19.3%	58
	No	78.7%	236
Security background	Yes	15.7%	47
	No	82.3%	247

Table 1: Participant demographics. Excludes "no answer" and "prefer not to say" options.

3.1 Survey protocol

Shared accounts (overview). Participants provided consent and then gave an overview of the accounts they shared. We defined a shared account as "any account where you and at least one other person both use the same username (or email address) and password combination in order to access and use the account, either at the same time or taking turns." (Accounts shared without any kind of password exchange were excluded.) For each shared account, respondents self-reported the service the account was for,[1] the type of account, and with whom they shared the account. Account type options presented to participants were initially derived from Park et al.'s survey on shared accounts in romantic relationships [34]. We derived additional account types, such as VPNs, from our own pilots. Table 2 shows the types of accounts participants reported sharing.

Personal accounts. For each shared account type (as defined in Table 2), we asked participants if they had any personal accounts (*not* shared with anyone else) of the same account type. For every account type the participant reported having both personal and shared accounts for, we asked the participant about the strategies and factors that influenced the creation of the password for one such personal account.

[1] Participants were not required to name the service explicitly. See *Survey Instrument* in the Appendix for wording details.

Account Type	Accounts		Participants		Examples
Video/Music Streaming	67.8%	(665)	91.0%	(273)	Netflix, Youtube, Hulu, Disney+, HBO Max, Apple Music
Shopping	14.7%	(144)	42.0%	(126)	Walmart, Amazon Prime, Newegg, Ticketmaster, Costco
Finances	5.2%	(51)	10.7%	(32)	Bank of America, Paypal, Chase, Mint, Fidelity
Rent/Utilities	4.7%	(46)	9.3%	(28)	Accounts for water, rent portals, mortgage accounts, Xfinity
Gaming	1.3%	(13)	4.0%	(12)	Steam, Xbox Live, Playstation Plus
File Sharing	1.3%	(13)	3.7%	(11)	iCloud, Google Drive, Box, Dropbox
Social Media	0.1%	(9)	2.0%	(6)	Instagram, Twitter, Facebook, Snap Chat
Productivity Tools	0.1%	(6)	1.3%	(4)	Google Calendar, Trello, Zoom, Canva
E-books	0.1%	(6)	2.0%	(6)	Kindle, Audible, Viz Media
News	0.1%	(5)	1.7%	(5)	New York Times, Consumer Reports, local newspapers
VPNs	<0.1%	(4)	1.3%	(4)	NordVPN, SurfShark
Health Insurance/Services	<0.1%	(4)	1.0%	(3)	Aetna, Cigna, OptumRx
Travel	<0.1%	(4)	1.0%	(3)	Websites for cruise lines and vacation rentals
E-mail	<0.1%	(3)	1.0%	(3)	Gmail, other e-mail services
Other	0.1%	(8)	2.3%	(7)	

Table 2: Types of accounts reported in the introduction of the survey (981 accounts total). For accounts that provide multiple services (such as Amazon Prime, which provides both shopping and streaming services), the account type was based on the dropdown option the participant selected.

Shared accounts (detailed). For the first four accounts the participant reported in the "shared accounts (overview)" section, we asked follow-up questions about the account, such as who was involved in password creation. If the participant was directly involved in password creation, we asked about the strategies they used and the motivations behind them. We chose to limit this section to the first four accounts reported (or all accounts, if fewer than four) in order to maximize recall and keep survey times manageable. We based the cutoff number on our pilots; pilot participants reported sharing an average of 3.6 accounts each. Because participants in our full study reported sharing an average of 3.3 accounts each, we believe that we achieved reasonable coverage.

Demographics. The survey concluded with demographic questions, which included income, education level, and background in computer/information security.

Data protection measures. We instructed participants not to share their passwords with us and periodically reminded participants that they should not enter their passwords into the survey. Furthermore, we did not collect any directly identifying from participants; participants were only identified by an anonymous Prolific (`https://prolific.co`) platform ID.

3.2 Recruitment

We recruited 300 respondents for our survey using Prolific's representative sampling feature, which recruits a demographically-representative (based on census data) sample of the U.S. population according to age, sex, and ethnicity (Table 1). We chose the sample size based on related survey work [34, 41, 47, 50]. Participants were required to reside within the U.S., be at least 18 years old, and self-report fluency in English. The survey took an average of 16.5 minutes to complete (median 13.9 minutes), and participants were paid $3.75. We asked that participants have at least one account they shared with others in order to take the survey. If participants did not report any shared accounts, we discarded their responses (three overall). We used responses to open-ended questions to validate the quality of data collected, discarding responses (two overall) where participants provided off-topic answers. For discarded responses, we recruited new participants in their place to keep the final number of valid participants at 300.

3.3 Analysis

For open-ended answers, two coders collaboratively applied open-coding content analysis to draw out common themes around password creation and account sharing from responses, as well as surface themes that the researchers may not have initially been expecting. We used responses from the pilot studies and 10% of responses from the full survey to inductively develop an initial codebook [38]. Pilot responses were only used to develop the initial codebook, and we excluded pilot data from the final counts of codes and the remainder of the analysis. After creating the initial codebook, coders independently applied the codebook to an additional 10% of the responses from the full survey and met to discuss codes. Coders repeated this process three times, at which point code saturation and consensus was reached as measured by Cohen's kappa ($\kappa = 0.70$, indicating "substantial agreement") [20, 25, 38]. The remaining responses were divided among the coders to code independently. One coder reapplied

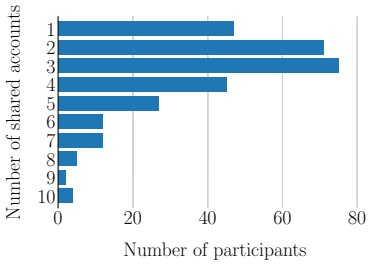

Figure 1: Number of accounts shared by each participant (981 accounts)

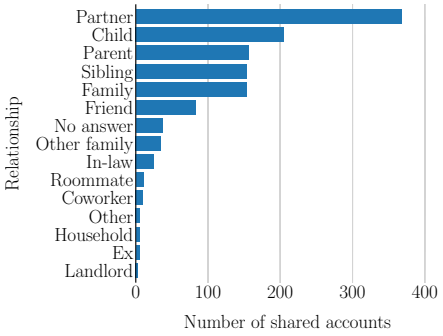

Figure 2: Who participants share their accounts with (981 accounts)

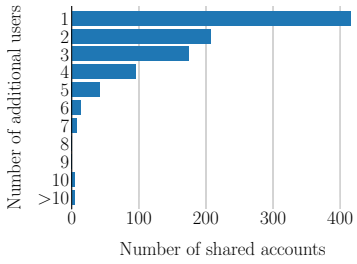

Figure 3: How many people (excluding themselves) participants share their accounts with (981 accounts)

the codebook to all prior responses from the codebook development phase to ensure that the final codes were adequately reflected across all responses.

In order to identify differences in password creation between personal and shared accounts, we built a regression model relating Likert-type responses about password-creation factors to whether an account was shared or personal. Details of this analysis are in Section 4.5.

3.4 Limitations

Our study has limitations inherent to online survey studies. Participants self-reported their password sharing behaviors, and we were unable to ask follow-up or clarification questions. Because we did not collect participants' passwords, we are unable to evaluate how secure these passwords actually were.

Due to social desirability and stigma against credential sharing, participants may not have reported all the accounts they share and may have underplayed insecure behaviors. However, some participants acknowledged their insecure practices ("I use the same password + variants for everything (bad — I know!)," Participant 70; "I know we aren't supposed to be reusing passwords, but this is the best one I have, and I can remember it," Participant 95; "I should have a more secure password, but I don't," Participant 177), and we believe that they were generally honest about their behaviors.

We asked participants in-depth questions about the first four accounts they reported rather than four random accounts in order to maximize recall, which may have biased which accounts were discussed for the participants who reported sharing more than four accounts.

We did not focus on adversarial account sharing or negative outcomes related to password sharing, and our participants did not discuss these topics in their free response answers. As such, our work only applies to voluntary account sharing.

Our sample size is not sufficient to obtain generalizable quantities for some uncommonly shared types of accounts (like VPN accounts). We focused on obtaining a broader view of the kinds of accounts people share rather than focusing on specific types of accounts.

Populations of online crowdsourcing platforms are generally more technologically-savvy than average; nonetheless, they provide reasonable sample populations [37]. In particular, Prolific has been found to be generally representative for user perceptions and experiences [45]. Furthermore, our usage of the platform's demographically-representative sampling feature ensured broader coverage of the U.S. population.

Because culture heavily influences expectations and norms surrounding credential sharing [3, 4, 27, 39], we focused on a single cultural context. Applying our research questions to non-U.S. contexts remains a subject for future research.

4 Results

We begin by describing our participants and the accounts they share (Section 4.1) and the prevalence of collaborative password-making for these shared accounts (Section 4.2). Next, we examine password reuse and other security behaviors (Sections 4.3 and 4.4), and finally we compare password creation strategies and motivations for shared accounts with those of personal accounts (Section 4.5).

4.1 Types of accounts participants share and with whom

Streaming accounts are the most common accounts shared by participants. Participants tend to share accounts with a few people close to them, typically partners and family members.

Our 300 participants reported sharing an average of 3.3 (median 3) accounts each. Figure 1 shows the distribution of shared accounts. Table 2 shows the types of accounts participants reported sharing; video and music streaming accounts are most popular, with 273 participants (91.0%) sharing at least one such account. Shopping accounts are the second most popular account to share, being shared by 126 participants (42.0%). Figure 2 shows with whom participants share

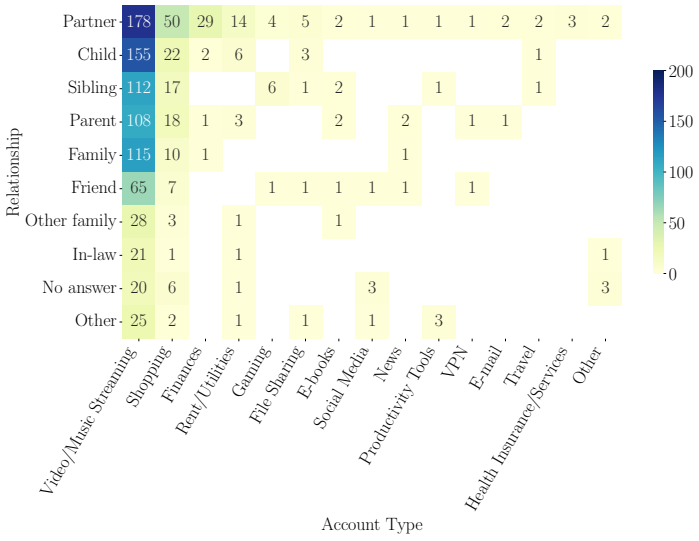

Figure 4: Sharing recipients, broken down by account type, from the "detailed" section of the survey (843 accounts total)

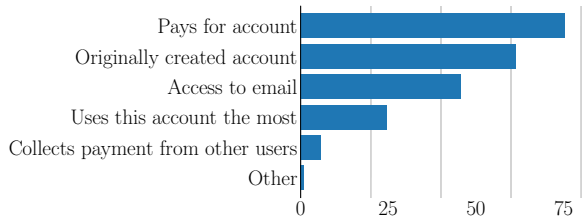

Figure 5: Factors contributing to account ownership. Participants could select more than one option per account.

their accounts. This is most commonly significant others and family members.

We report how many people each account was shared with in Figure 3. Accounts tend to be shared with a relatively small number of people: the median number of additional people (excluding the participant) an account was shared with was 2 (mean: 2.2 [2]). While not common, 20 participants (6.7%) report being unsure of exactly how many people have access to at least one of their shared accounts (35 accounts total).

After our 300 participants listed all of their shared accounts, we asked about the first four of them (or all of them, if fewer than four) in detail; the following results are based on these 843 shared accounts. Figure 4 summarizes who the subset of accounts we examine going forward are shared with and what type of accounts they are.[3]

[2]This statistic excludes 4 accounts for which participants selected the "> 10" option when reporting the number of other users, instead of specifying an exact count.

[3]This subset of accounts is representative of the broader set of shared accounts collected (cf. Figure 7 in the Appendix).

	Ownership			
Collaboration	**Single**	**Multi**	**Other**	***Total***
Single	632	115	0	*747*
Collaborative	9	29	1	*39*
Password generator	23	10	1	*34*
Other	5	5	13	*23*
Total	*669*	*159*	*15*	*843*

Table 3: Account ownership and collaboration in making shared passwords. *Other* includes unsure and no response.

4.2 Makers of shared passwords

Users rarely collaborate to make passwords for shared accounts. Generally, password creation is left to the sole discretion of a single account owner.

Shared accounts may have a single user who acts as the account owner (a single-owner shared account), or multiple users that share account ownership equally (a multi-owner shared account). We asked participants to identify their shared accounts as either single-owner or multi-owner. Table 3 shows that single-owner accounts are dominant, accounting for 79% of all accounts. Participants explained how they determined ownership by selecting (multiple selection allowed) from a list of factors derived from the pilots (Figure 5); who paid for the account (635 accounts, 75.3%) contributed to ownership most often, followed by who initially created the account (518 accounts, 61.4%).

We found that in both single-owner and multi-owner shared accounts, creation of shared passwords is primarily an individual process. Only 39 (4.6%) accounts involved two or more people in password creation, whereas individuals created passwords for 747 of the accounts (88.6%). Password generators were used to create passwords for 34 accounts (4.0%). For the remaining 23 accounts (2.7%), participants reported that they were either unsure of how many users were involved in password creation or elected not to answer. Overwhelmingly, account owners are responsible for creating passwords for shared accounts. Across both single-owner and multi-owner accounts, cases in which non-owner users were involved in password creation (either creating the password by themselves or collaboratively with other users) are few, amounting to only 41 accounts overall (4.9%).

While password creation is primarily handled by one person, password-makers often take into account the capabilities of other users, especially in the case of young or elderly users. In these situations, usability may be prioritized over security. For example, Participant 16 described the password to a streaming account as "very basic" because "My grandparents are, well, grandparents. I wanted to make sure they didn't have any more difficulties getting it set up than they needed." In creating a shopping account password, Participant 96 said,

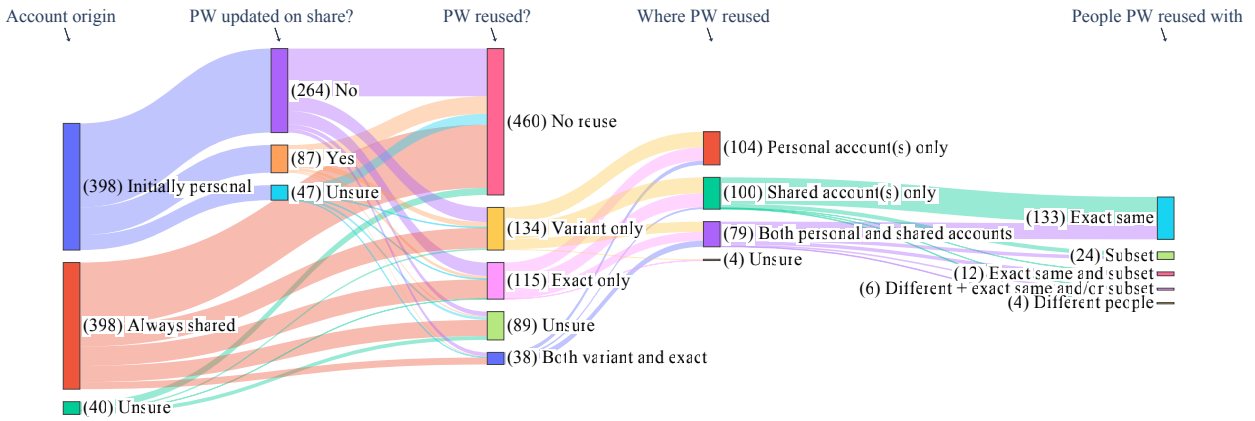

Figure 6: Origins of shared accounts and incidents of password reuse

"security was mildly important, but mostly I wanted an older not-so-computer-savvy relative to be able to enter it correctly." For a shared streaming service, Participant 222 felt that "It is more important for this account to ensure everyone's access than to make the password complex."

4.3 Account origins and password reuse

Shared accounts are created with the intention of sharing as often as not. Users frequently reuse passwords from these shared accounts both in other shared accounts and in personal, non-shared accounts.

Accounts may be created directly for the purpose of sharing or start as a personal (unshared) account; Figure 6 summarizes the sharing and reuse life cycle. We found that 398 (47.2%) of the 843 accounts that participants described in-depth were shared accounts from the start, while the same number, 398 accounts (47.2%), began as personal accounts and were later shared with others. For the remaining accounts, participants were either unsure or elected not to answer.

Account owners often fail to update passwords when personal accounts become shared. Of the 398 shared accounts that began as personal accounts, 264 accounts (66.3%), representing 158 participants (52.7%), did not have their passwords updated when they became shared. Password reuse is also frequent. Nearly half of our participants, (136, 45.3%), reused a shared password elsewhere. In all, 287 shared accounts (34.0%) have their passwords reused in some manner.

Some people reuse passwords verbatim (115 accounts, 13.6%) while others reuse a variant of the password (134 accounts, 15.9%). Because people reuse passwords across multiple accounts, they may also employ a combination of these strategies (38 accounts, 4.5%). Shared passwords see roughly equal reuse in other shared accounts (179 accounts) and in personal accounts (183 accounts).

For passwords reused among multiple shared accounts, the passwords of 133 accounts (15.8%), representing 69 participants (23%), are reused in some manner among accounts shared with the exact same people. However, the passwords for 46 accounts (5.4%), representing 27 participants (9%), are reused among accounts shared by different groups of people. Because this may include subsets or supersets of the original group, or even different people entirely, knowledge of the original user's password or creation strategy may spread widely.

Another risk comes from reusing shared passwords (exact or variant-of) on personal accounts, which was reported by 96 participants (32%). In particular, 104 shared accounts (12.3%) have passwords in common only with personal accounts, and 79 shared accounts (9.4%) have passwords in common with both personal and other shared accounts. In total, 183 shared accounts (21.7%) have their passwords directly or indirectly used for personal accounts.

When explaining password reuse, many participants expressed sentiments similar to those observed in single-user accounts in prior work. This includes reuse to cope with the sheer number of passwords they are expected to remember [15] ("I made it similar to other passwords I have because I cannot remember a bunch of passwords to save my life," Participant 4); rationing effort in accounts perceived to be low-value [46] ("I don't want to have to add seven passwords to my list of different passwords I use, especially not for something of low importance," Participant 118); modifying old passwords perceived to be secure as a means of improving recall [48] ("Variation of a password from my college days, it's pretty much stuck in my memory and complex enough for me to feel safe using it," Participant 63); and reusing passwords for thematically similar accounts [44] ("The password is used on a bundle of streaming services, all with the same password," Participant 250).

However, other participants discussed reusing passwords for the purpose of improving usability of multiple accounts shared among a group. Many reasoned that reusing the same password for all accounts they shared with this common group

Distribution Mechanism	Count	Percent
Verbal	489	58.0%
E-mail/text/IM	332	39.4%
Manually entered for recipient	27	3.2%
Written on physical document	24	2.8%
Via password manager	17	2.0%

Table 4: Password distribution mechanisms. Count may add up to more than 843 due to multi-selection. "Prefer not to answer" not shown.

would circumvent the need for each user to individually remember separate passwords for each account. For instance, Participant 95 said, "...it was easy for our family and users to remember it because it had been previously used for another account we all used." Participant 17 wrote that one of their shared account passwords is "...a variation of the password that we use on all the other accounts we share so that it is easy to remember." Finally, Participant 179 described using the "same password for all shared accounts so that the people sharing it can easily log in."

4.4 Other security behaviors for shared accounts

Two-factor authentication is uncommon in shared accounts. Passwords are often transmitted verbally, and forgotten passwords have the potential to disrupt access or cause conflict in the sharing process.

Two-factor authentication. Only about one fifth of shared accounts surveyed, 174 accounts (20.6%), had two-factor authentication (2FA) enabled. Of the 477 accounts participants said did not have 2FA, users actively disabled 2FA for 36 accounts (7.5%) in order to facilitate sharing. For the remaining 192 accounts, participants were unsure if 2FA was enabled.

Password distribution and retrieval. We asked participants how they distributed or received passwords for the accounts they shared (Table 4). Most of the time, they simply read the password out loud. We hypothesize that this may result in simpler or more pronounceable passwords being favored, though this question requires more research.

We also asked participants what they would do in the event that they forgot the password to their shared account (Table 5). Account owners tended to favor resetting the password, while non-owners most favored asking the owner for the password. Either strategy has the potential to disrupt access or cause conflict in the sharing process: password resets can lock other users out of the account if the new password is not re-distributed, and some account owners expressed that they did not want other users to repeatedly ask them for the password ("I do not want to be bothered each time the password is forgotten," Participant 197).

	Frequency	
Retrieval Mechanism	Owner	Non-owner
Reset password	66.7% (342)	15.1% (50)
Ask another user	22.4% (125)	18.4% (61)
Ask owner/co-owner	12.1% (62)	74.6% (247)
Refer to password distribution message	4.9% (25)	9.7% (32)
Refer to written document	3.7% (19)	1.0% (3)
Refer to password manager	4.7% (24)	1.0% (3)
Guess until gain access	0.0% (0)	<1.0% (1)
Give up access	0.0% (0)	<1.0% (1)

Table 5: What participants would do if they forgot the password to their shared account. Count may add up to more than 843 due to multi-selection.

4.5 Comparison with personal accounts

Participants tend to employ similar password creation strategies for both personal and shared accounts, though account accessibility influences creating passwords for shared accounts. Some, but not all, participants attempt to avoid cross-contamination of personal and shared passwords.

Next, we compare how people treat shared and personal accounts. We focused our analysis on the subset of shared accounts in which participants reported being directly involved in password creation (494 accounts, 232 participants). We compared these to analogous personal accounts and asked each participant for examples of these, if they had any, limiting them to one per account type (as defined in Table 2). Overall, 198 participants described at least one personal account, for a total of 230 personal accounts (Table 6).

Factors important to password creation. For both personal and shared accounts, we asked participants to rate on a five-point Likert-style scale how important the following six factors were for creating their passwords:

- Having a complex password
- Having a memorable (to me) password
- Having a password that is hard to guess
- Having a long password
- Having a password unique from my other passwords
- Being able to store the password in a password manager

We binned these Likert ratings into binary variables for analysis (neutral ratings were grouped with those indicating low importance). To check for correlation between these

Account Type	Count	Percent
Video/Music Streaming	158	68.7%
Shopping	49	21.3%
Finances	9	3.9%
Rent/Utilities	7	3.0%
Health Insurance/Services	2	0.9%
Gaming	2	0.9%
Social Media	1	0.4%
File Sharing	1	0.4%
Other	1	0.4%

Table 6: Types and counts of personal accounts described by participants in "personal accounts" (230 accounts total).

Variable	Odds Ratio	Conf. Int.	*p*-value
Memorable (to me)	1.2	[0.8 - 1.7]	0.350
Hard to Guess	0.6	[0.4 - 0.9]	0.020*
Unique	1.6	[1.1 - 2.3]	0.016*
PW Manager	1.0	[0.7 - 1.4]	0.889

Table 7: Binomial logistic mixed-effects regression on participants' Likert ratings for factors important to password creation in personal and shared accounts. Pseudo-$R^2 = 0.02$ using the Aldrich-Nelson method [14]. Odds ratios above 1 indicate higher likelihood of the variable being rated as important in a shared account compared to a personal account.

binary factors, we calculated the tetrachoric correlation coefficient, appropriate for correlating binary data, between each factor pair [11]. Three factors connected to password composition and strength ("Having a complex password," "Having a long password," "Having a password that is hard to guess") were all highly correlated ($|r_{tc}| > 0.8$). As participants did not rate the importance of these factors differently, we decided to keep the most general of the three, "Having a password that is hard to guess," and exclude the others ("long" and "complex" passwords) from the analysis.

To identify factors differing between shared and personal accounts, we then constructed a generalized linear mixed-effects model (binomial logistic). The dependent variable was if an account was personal or shared; independent variables included the account type (categorical) and the four remaining creation factors (binary). We compared potential models by testing all possible combinations of covariates and selected our final model based on minimum Akaike Information Criterion (AIC) [2]. Table 7 shows the final model. Odds ratios above 1 correspond to increased importance for shared accounts relative to the baseline (personal accounts).

The final model showed that participants were 1.6× more likely to rate password uniqueness as important for shared accounts than for personal accounts. Conversely, participants were 1.7× more likely ($\frac{1}{0.6}$) to rate low guessability as important for personal accounts than shared accounts. These results accord with our other findings: participants do not necessarily prioritize security as highly for shared accounts, but are somewhat more concerned about limiting reuse when sharing a password. Memorability and ability to use a password manager did not show a significant difference between personal and shared accounts; account type was dropped from the final model during model selection.

Password creation strategies and motivations. We asked participants to describe their strategies for creating their passwords for personal and shared accounts. Tables 8 and 9 describe the most popular strategies and motivations. Full codebooks are available in the Appendix (Tables 10 and 11).

Behaviors most commonly reported for both personal and shared accounts reflect password behaviors highlighted in previous literature on single-user accounts. These include incorporating meaningful information like birthdays and names of pets [7], reusing passwords with or without slight modifications [10], and attempting to balance security and memorability of passwords [15, 46].

However, there are a few key differences. Some strategies and motivations more frequently discussed for personal accounts included: password generators and managers, relating the password to the service itself, and following personal algorithms for password generation. In contrast, making the password simpler or easier to use was more commonly reported for shared passwords.

Participants' explanations offer insights explaining these differences. While improving password recall and account security served as common motivators in both personal and shared accounts, participants were more often concerned with making the account easy to access in the shared account scenario. This takes several forms, such as making a password that could be easily entered by all users across different devices such as phones, computers, tablets, and even gaming consoles ("I wanted something simple I could give to my wife so she could watch Netflix on her iPad or use at school on occasion," Participant 62; "We needed a password that we could easily enter using the different interfaces where it is used," Participant 223). Other reasons included simplifying passwords for elderly users and children (as highlighted in Section 4.2) or reusing passwords among accounts shared by members of a group, as discussed in Section 4.3. In addition, for 48 of the 216 (22.2%) shared accounts where improving password recall served as a motivator, password-makers specifically stated that they wanted the password to be memorable for all users on the account rather than just themselves.

Threat models for shared accounts. When discussing security in shared accounts, participants more often expressed concerns over external threats to their accounts, such as hackers ("It's a utility and could be targeted by hackers," Partic-

Code	Frequency		Definition
	Shared	Personal	
Meaningful info.	22.5% (111)	23.0% (53)	Used information that is meaningful to at least one user
Memorable	20.6% (102)	14.8% (34)	Prioritized making the password memorable
Reuse	16.8% (83)	20.0% (46)	Reused (either exactly or a variant of) another password
Secure	14.0% (69)	12.6% (29)	Prioritized making the password secure
Personal algorithm	13.8% (68)	18.7% (43)	Used a personal algorithm for passwords, such as minimum rules or a pattern of units (e.g., numbers-word-numbers)
Password generator	8.5% (42)	10.4% (24)	Used a password generator (i.e., one in a password manager)
Random	5.1% (25)	4.8% (11)	Created randomly without the use of a password generator
Related to service	1.4% (7)	6.1% (14)	Related to the service that the account is for

Table 8: Common (used in more than 5% of either shared or personal accounts surveyed) password generation strategies used by participants for accounts where they were involved in password creation. Participants sometimes indicated more than one strategy per password.

Code	Frequency		Definition
	Shared	Personal	
Recall	43.7% (216)	53.5% (123)	Wanted the password to be easy to recall for users
Secure account	35.4% (175)	43.0% (99)	Prioritized the security of the account
Easy to access account	8.5% (42)	2.6% (6)	Wanted the account to be accessed easily
Easy to make	5.9% (29)	4.3% (10)	Password was easy to make

Table 9: Common (used in more than 5% of either shared or personal accounts surveyed) motivations for participants' choice of password strategy. Participants sometimes indicated more than one motivation per password.

ipant 61; "Amazon is a target for thieves, so I want to be as careful as possible," Participant 96) rather than internal threats. Nonetheless, a few users took precautions to avoid cross-contaminating passwords between shared and personal accounts, even if they did not directly refer to other users as potential security threats ("Because I am sharing this password and don't want it to be the same password I use for other things," Participant 48; "It keeps my other accounts secure as it is unique to this account," Participant 135).

Effort rationing based on perceived account value. Similar to previous work on effort rationing [44], participants discussed conserving effort for accounts they deemed as more sensitive ("I wanted this password to be harder to guess because it's attached to my bank accounts," Participant 142; "More complicated password since a shopping site," Participant 156) and deferring to weaker security practices for "less valuable" accounts ("There isn't much that a hacker could do in this account, so security is not as important for this [travel account]," Participant 233; "Minimal loss if password gets stolen, will just reset, and no real way it can cost us money/security," Participant 203). Sensitive accounts often included shopping accounts, which can have stored credit cards, and utilities accounts, which are associated with physical residences. On the other hand, streaming accounts were often considered to be less valuable by participants due to storing limited information or having little impact if compromised.

5 Discussion

In contrast to prior works, which examine password creation in single-user accounts or account sharing behavior post-password creation, we combine the two and study creation and use of shared passwords in multi-user accounts. Our study sheds light on how people share passwords and offers important implications for system developers.

5.1 Comparisons with the single-user context

Similarities. We observe that usability challenges highlighted by prior works in single-user contexts influence creation of shared passwords in similar ways. As discussed in Sections 4.3 and 4.4, people often reuse passwords in shared accounts to cope with having more passwords than they (or the people they are sharing with) can effectively remember, ration effort spent on low-value accounts, and use old, "secure" passwords as a resource for deriving new passwords [15, 44, 46, 48]. Our participants engaged in common

behaviors previously seen in the single-user setting for both passwords they intend to share and those they do not, such as using meaningful data in their passwords [7] and relying on personal algorithms to create passwords [46].

Differences. We observe that elements specific to the context of sharing exert unique pressures on password-makers. The presence of multiple users may exacerbate the security-usability trade-off; users discuss making deliberate security concessions when creating passwords with the intention of sharing in order to proactively improve usability, such as by making simpler and easier to remember passwords when sharing with young or old users. Further, account sharing engenders a particular type of password reuse: a common password among multiple accounts shared by a group of users.

5.2 Shared passwords created by a single user

Password-making in shared accounts is an individual process, often performed solely by an account owner, rather than as a collaborative effort between users. We note that a similar dynamic has been observed in the context of smart homes, where users who install home smart devices have an outsized role in controlling configurations and repair of these devices [13]. This individual effort comes in two varieties, each with their own unique security implications.

As discussed above, when users create passwords *with* the intention of sharing, they may make security concessions for the sake of usability. When users create passwords *without* the intention of sharing, as in the case of personal accounts that did not have their passwords updated when they were shared, the password inherits the typical mechanisms and weaknesses of other personal account passwords, including the potential for password reuse. In about two thirds of reused passwords (63.7%), participants stated they reused these passwords in both shared and personal accounts. This form of reuse can create additional vulnerabilities for personal passwords when the account becomes shared, increasing the opportunity for the password to be phished, leaked, or otherwise stolen and then used in credential-stuffing attacks.

Because account owners play the primary role in password creation and shared account management, they represent a promising target to improve safety in sharing.

5.3 Implications for developers

Most systems are still designed with the assumption of one person per account. While services may quietly tolerate or outright prohibit account sharing [28, 31], it is nonetheless a common behavior often undertaken for reasons that are important to the user, and as such it will likely continue despite its potential security risks. Technology designers and systems developers should keep this reality in mind and tailor systems and advice to minimize potential harms from sharing.

Account sharing without credential sharing. Services that tolerate or encourage sharing can enable account sharing without password sharing, for example by giving each user of a shared account unique credentials to reduce unintentional propagation of personal passwords. However, the overhead of creating such sub-accounts and associated passwords, as well as untangling and migrating individual user data if this schema were to be applied to existing accounts being shared, may deter users, and they may instead choose to default to using a single shared account, as seen in the smart home setting [23]. Researchers should instead investigate more usable access control alternatives for account sharing.

Helping users discern who is accessing a shared account. Some participants reported they were unsure exactly how many people had access to some of their accounts. It would be helpful for developers to provide a simple and comprehensible view of login history: when and where an account has been used from, together with the ability to annotate logins and associate them with specific users. These account security indicators can alert users to unwanted access and help owners remove no-longer-authorized users [9]. We also find that people tend to reuse group passwords within (approximately) the same group of people; a login history might help users to understand whether a group password has been compromised or has traveled beyond its initial intended recipients.

Password managers. Not all services want to encourage account sharing, including for financial or security reasons. Password managers could play a greater role in enabling sharing while maintaining security and reducing password reuse on services that do not wish to implement account sharing features themselves. Several participants reported using a password manager to distribute and store shared passwords. Indeed, some popular password managers offer family plans and one-time password sharing options that claim to simplify sharing and security [1, 22, 29]. In addition, password managers enable non-owner users to retrieve forgotten passwords without inconveniencing the account owner, synchronize passwords and account access across devices without having to reenter passwords, and generate passwords that are easier to verbalize yet retain security. A number of participants reported disabling 2FA in order to facilitate account sharing; password managers can enable sharing of 2FA-protected accounts through sharing time-based one-time password seeds. However, the usability of these password managers in the context of account sharing has yet to be evaluated. Usability challenges already represent a major hurdle to adoption of password managers in the single-user context [35], and these challenges may be further exacerbated in the shared account setting where users prioritize account accessibility even more.

Trust and social norms. Our participants' account sharing behavior highlights the importance of trust and social norms in maintaining account security while engaging in insecure behavior. Participants primarily shared accounts with trusted family members and partners. While some took precautions to protect themselves from other users, such as by avoiding cross-contamination between shared and personal passwords, many others (almost a third of our participants) did not. Participants more often cited external threats (hackers) over internal threats (other users) when discussing security. While our work centers on users in the U.S., research in other cultural contexts have similarly highlighted the role of trust and social norms in maintaining account security while sharing passwords [3, 4].

This reliance on trust for security can serve as a double-edged sword: users may reuse passwords or disable security measures like 2FA. In the case of reusing passwords from personal accounts on shared accounts, users may be granting others access to accounts they do not intend to share on a technical level, but trust them not to access these accounts or engage in harmful behavior. Similar behaviors have also been observed in the context of smart homes; device owners often rely on trust with other users and social norms rather than strict access controls for security [23, 53]. Interventions will need to find a way to maintain account security if this trust can no longer be relied upon, as in the case of relationships ending. On the other hand, previous literature has suggested that these relationships and group dynamics can be leveraged to improve security behavior of members less versed in secure behaviors [51]. In the account sharing scenario, groups can perhaps encourage adoption of other secure habits among their members, such as the use of password managers or other secure password behaviors.

5.4 Future work

Sharing of highly sensitive accounts. There remain some important open questions about shared accounts and passwords. Our study surveyed sharing of accounts broadly; however, some accounts have greater security implications, such as those for financial institutions and utility companies. While our participants more often reported employing secure strategies like randomization of passwords (versus using meaningful information) for shared financial accounts compared to less sensitive accounts like streaming accounts, we lacked a sufficiently large sample to draw definitive conclusions. Due to their importance, future work could investigate these sensitive accounts, their password strategies, and relative security of these shared passwords specifically.

Password reuse in accounts of varying sensitivity. Our study uncovered a high degree of password reuse between shared and personal accounts. While this is concerning, more information is needed to fully understand the security implications of this reuse. Do the reused passwords span both low- and high-value accounts? Do these personal accounts have additional protection measures (e.g., two-factor authentication), or are they accessible by anyone with the password? Do people understand the ramifications of their password-sharing choices? Future researchers could investigate these questions as well as others about the mental models of those engaging in reuse of shared passwords.

Verbalization of shared passwords. We found that 58.0% of shared passwords in this study were transmitted verbally. We hypothesize that one reason people create weaker passwords for shared accounts is to make them easy to communicate. Future work could test this supposition directly by investigating the relationship between the distribution mechanism and password composition, as well as test the usability of generators that claim to make secure, verbalizable passwords.

Ending account sharing. Previous literature has highlighted that ending sharing and updating passwords to all formerly-shared accounts is a tedious and challenging process for users [30, 34], and we posit that the cross-contamination of passwords between shared and personal accounts discussed by our participants would further amplify the difficulties users face when attempting to end account sharing.

Other sharing contexts. Our participant pool primarily shared accounts with family members and friends. Future work could examine shared password creation in other contexts that have different security implications and different trust dynamics, such as in the workplace.

6 Conclusion

We conducted a U.S. census-representative survey ($n = 300$) to understand password creation in shared accounts. We found that the typical user tends to share accounts with partners and family members, and streaming accounts are most commonly shared. Creation of shared passwords is predominantly an individual rather than collaborative process, typically performed by the account owner. While users mostly employ similar strategies to create both shared and non-shared passwords, prioritization of usability of shared accounts can lead to deliberate security concessions. Password reuse is common, occurring in roughly a third of shared accounts surveyed. Accounts shared by a group are often accessible by a single common password. Among shared accounts with reused passwords, approximately two-thirds of these passwords, representing a third of our participants, are reused in some manner on personal accounts. Technology creators and security experts should take these findings—and the inevitable reality of credential sharing—into account and design systems that can support sharing while minimizing harm.

7 Acknowledgments

This paper results from the SPLICE research program, supported by a collaborative award from the National Science Foundation (NSF) SaTC Frontiers program under award numbers 1955805. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the NSF.

References

[1] 1Password. 1password families, Accessed 2023-05-03. URL https://1password.com/affiliate/families.

[2] Hirotogu Akaike. Information theory and an extension of the maximum likelihood principle. In *Selected papers of Hirotugu Akaike*. Springer, 1998.

[3] Aniqa Alam, Elizabeth Stobert, and Robert Biddle. "this is different from the western world": Understanding password sharing among young bangladeshis. In *Symposium on Usable Security and Privacy (USEC)*, 2023.

[4] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. Security practices for households bank customers in the kingdom of saudi arabia. In *Symposium On Usable Privacy and Security (SOUPS)*, 2015.

[5] Jennifer L. Bevan. Social networking site password sharing and account monitoring as online surveillance. In *Cyberpsychology, Behavior, and Social Networking*, volume 21, pages 797–802, 2018.

[6] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *IEEE Symposium on Security and Privacy (SP)*, 2012.

[7] Kay Bryant and John Campbell. User behaviours associated with password security and management. In *Australasian Journal of Information Systems*, volume 14, 2006.

[8] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No one can hack my mind revisiting a study on expert and Non-Expert security practices and advice. In *Symposium on Usable Privacy and Security (SOUPS)*, 2019.

[9] Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. Account security interfaces: Important, unintuitive, and untrustworthy. In *USENIX Security Symposium (USENIX Security)*, 2023.

[10] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and Xiaofeng Wang. The tangled web of password reuse. In *Network and Distributed System Security (NDSS) Symposium*, 2014.

[11] D. R. Divgi. Calculation of the tetrachoric correlation coefficient. 44(2):169–172, 1979.

[12] Serge Egelman, A.J. Bernheim Brush, and Kori M. Inkpen. Family accounts: A new paradigm for user accounts within the home environment. In *Conference on Computer Supported Cooperative Work (CSCW)*, 2008.

[13] Christine Geeng and Franziska Roesner. Who's in control? interactions in multi-user smart homes. In *Conference on Human Factors in Computing Systems (CHI)*, 2019.

[14] Timothy M Hagle and Glenn E Mitchell. Goodness-of-fit measures for probit and logit. *American Journal of Political Science*, 1992.

[15] Ameya Hanamsagar, Simon S. Woo, Chris Kanich, and Jelena Mirkovic. Leveraging semantic transformation to investigate password habits and their causes. In *Conference on Human Factors in Computing Systems (CHI)*, 2018.

[16] Philip G. Inglesant and M. Angela Sasse. The true cost of unusable password policies: Password use in the wild. In *Conference on Human Factors in Computing Systems (CHI)*, 2010.

[17] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Symposium On Usable Privacy and Security (SOUPS)*, 2015.

[18] Jyun-Yu Jiang, Cheng-Te Li, Yian Chen, and Wei Wang. Identifying users behind shared accounts in online streaming services. In *Conference on Research & Development in Information Retrieval*, 2018.

[19] Joseph 'Jofish' Kaye. Self-reported password sharing strategies. In *Conference on Human Factors in Computing Systems (CHI)*, 2011.

[20] Klaus Krippendorff. *Content Analysis: An Introduction to Its Methodology*. Fourth edition edition, 2023.

[21] Airi M I Lampinen. Account sharing in the context of networked hospitality exchange. In *Conference on Computer Supported Cooperative Work (CSCW)*, 2014.

[22] LastPass. Lastpass families, Accessed 2023-05-03. URL https://www.lastpass.com/products/family-password-manager.

[23] Nathan Malkin, Alan F. Luo, Julio Poveda, and Michelle L. Mazurek. Optimistic access control for the smart home. In *IEEE Symposium on Security and Privacy (SP)*, 2023.

[24] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "she'll just grab any device that's closer": A study of everyday device & account sharing in households. In *Conference on Human Factors in Computing Systems (CHI)*, 2016.

[25] Mary L. McHugh. Interrater reliability: the kappa statistic. *Biochem Med (Zagreb)*, 22(3), 2012.

[26] Helena M. Mentis, Galina Madjaroff, and Aaron K. Massey. Upside and downside risk in online security for older adults with mild cognitive impairment. In *Conference on Human Factors in Computing Systems (CHI)*, 2019.

[27] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "in eighty percent of the cases, i select the password for them": Security and privacy challenges, advice, and opportunities at cybercafes in kenya. In *IEEE Symposium on Security and Privacy (SP)*, 2023.

[28] Netflix. An update on sharing, 2023-02-08. URL https://about.netflix.com/en/news/an-update-on-sharing.

[29] NordPass. Boost your business security with ease, Accessed 2023-05-03. URL https://nordpass.com/nordpass-business-solution.

[30] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. The burden of ending online account sharing. In *Conference on Human Factors in Computing Systems (CHI)*, 2020.

[31] Kate O'Flaherty. The disney password sharing crackdown is about to begin, 2023-08-11. URL https://www.forbes.com/sites/kateoflahertyuk/2023/08/11/the-disney-password-sharing-crackdown-is-about-to-begin/?sh=3e14dae2577c.

[32] Kenneth Olmstead and Aaron Smith. Password management and mobile security. 2017.

[33] Joris Van Ouytsel. The prevalence and motivations for password sharing practices and intrusive behaviors among early adolescents' best friendships – a mixed-methods study. In *Telematics and Informatics*, volume 63, page 101668, 2021.

[34] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. Share and share alike? an exploration of secure behaviors in romantic relationships. In *Symposium on Usable Privacy and Security (SOUPS)*, 2018.

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

[36] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why older adults (don't) use password managers. In *USENIX Security Symposium (USENIX Security)*, 2021.

[37] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *IEEE Symposium on Security and Privacy (SP)*, 2019.

[38] Johnny Saldaña. *The coding manual for qualitative researchers.* Sage Publications Ltd, 2009.

[39] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchil. "privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In *Symposium on Usable Privacy and Security (SOUPS)*, 2018.

[40] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering stronger password requirements: user attitudes and behaviors. In *Symposium on Usable Privacy and Security (SOUPS)*, 2010.

[41] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering stronger password requirements: User attitudes and behaviors. In *Symposium on Usable Privacy and Security (SOUPS)*, 2010.

[42] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the united states. In *IEEE Symposium on Security and Privacy (SP)*, 2018.

[43] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I. Hong, and Laura Dabbish. Normal and easy: Account sharing practices in the workplace. 2019.

[44] Elizabeth Stobert and Robert Biddle. The password life cycle: User behaviour in managing passwords. In *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[45] Jenny Tang, Eleanor Birrell, and Ada Lerner. Replication: How well do my results generalize now? the external validity of online privacy and security surveys. In *Symposium on Usable Privacy and Security (SOUPS)*, 2022.

[46] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "i added '!' at the end to make it secure": Observing password creation in the lab. In *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[47] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users' perceptions of password security match reality? In *Conference on Human Factors in Computing Systems (CHI)*, 2016.

[48] Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In Paula Kotzé, Gary Marsden, Gitte Lindgaard, Janet Wesson, and Marco Winckler, editors, *Human-Computer Interaction – INTERACT 2013*, pages 460–467. Springer Berlin Heidelberg, 2013.

[49] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. Sok: A framework for unifying at-risk user research. In *IEEE Symposium on Security and Privacy (SP)*, 2022.

[50] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding password choices: How frequently entered passwords are re-used across websites. In *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[51] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. "we hold each other accountable": Unpacking how social groups approach cybersecurity and privacy together. In *Conference on Human Factors in Computing Systems (CHI)*, 2020.

[52] Monica Whitty, James Doodson, Sadie Creese, and Duncan Hodges. Individual differences in cyber security behaviors: an examination of who is sharing passwords. In *Cyberpsychology, behavior and social networking*, volume 18, pages 3–7, 2015.

[53] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in Multi-User smart homes: A design exploration and In-Home user study. In *USENIX Security Symposium (USENIX Security)*, 2019.

[54] Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. In *Conference on Computer and Communications Security (CCS)*, 2010.

A Supplementary Figures

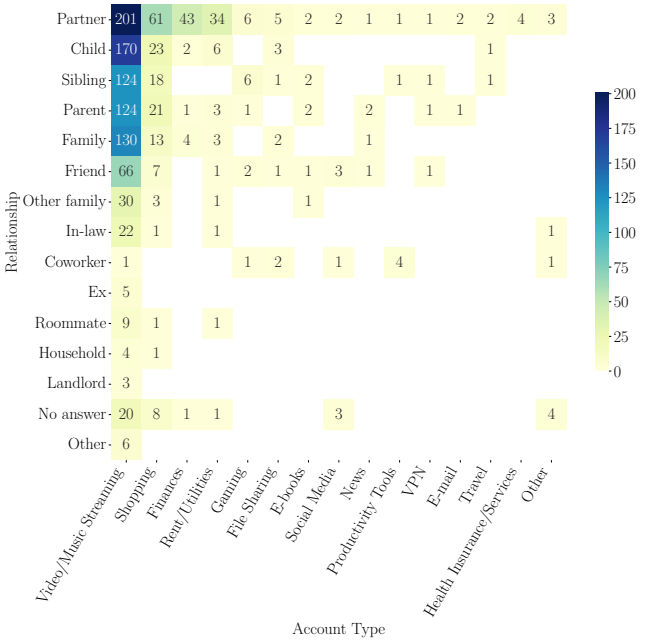

Figure 7: Who participants report sharing their accounts with in "Shared accounts overview," separated by account type.

B Survey Instrument

B.1 Shared accounts overview

In this survey, we will be asking you about the accounts you share with other people.

By **account**, we mean any website or system where you log in with a username (or email address) and password combination in order to access services or content.

People often share accounts (such as those for streaming, shopping, and finances) for a wide variety of reasons.

By **shared account**, we mean any account where you and at least one other person both use the same username (or email address) and password combination in order to access and use the account, either at the same time or taking turns.

This EXCLUDES: Accounts where each person uses a different username (or email) and password combination to log in. Accounts where only a username or password is needed (but not both), such as shared Wi-Fi.

1. How many accounts do you currently share with at least one other person and **can currently log into or access?**

   Using one account per line, please describe them below. If you have multiple accounts for one type of service (such as multiple streaming accounts) that you share with others, please describe them separately.

	What website or service is this account for? Feel free to describe the type of service if you would rather not name the account.	What option best describes this account?	**Excluding yourself**, how many people do you share this account with (to the best of your knowledge)?	Check this column if you **are NOT certain** how many people share this account. -	Who do you share this account with? For example: friends, siblings, coworkers, etc.
Account 1	e.g. "Netflix"			☐	e.g. "parents"
Account 2				☐	
Account 3				☐	
Account 4				☐	
Account 5				☐	
Account 6				☐	
Account 7				☐	
Account 8				☐	
Account 9				☐	
Account 10				☐	

2. If you have any other accounts that you share with other people, please describe each account here with:

(a) The name of the website/service the account is for.

(b) How many people, excluding yourself, use this account.

(c) Who you share this account with.

B.2 Personal accounts

This section is repeated once for every [account type] that the participant reports having a shared account of in Part A

3. Think about the accounts you **DO NOT** share with anyone else (you are the only person with access to these accounts and the only one that knows the username/password combination).

Do you have any **[account type]** accounts that you **DO NOT** share with anyone else?

- ○ Yes - I have a [account type] account that I DO NOT share with anyone else
- ○ No - I do not have such a [account type] account
- ○ Not sure / Prefer not to answer

The remaining questions in this section are only shown if the participant answers "Yes" to the above question

4. Think about one such [account type] account that you DO NOT share with anyone else. What website or service is this account for?

5. Think about the password you made for this account. How important were each of the following factors in creating your password?

	1 - Not important at all	2	3	4	5 - Extremely important	Prefer not to answer
Having a complex password	○	○	○	○	○	○
Having a memorable (to me) password	○	○	○	○	○	○
Having a password that is hard to guess	○	○	○	○	○	○
Having a long password	○	○	○	○	○	○
Having a password that is unique from my other passwords	○	○	○	○	○	○
Being able to store the password in a password manager	○	○	○	○	○	○
Other	○	○	○	○	○	○

6. Think about the password you made for this account. Did you use any of the following strategies to create your password? Check all that apply.

If you are unsure of the password or don't remember it exactly, please check the "I do not remember the exact password to this account" option.

- ☐ Based on the name of someone or something
- ☐ Based on a word or name with numbers/symbols added to beginning or end
- ☐ Based on a word or name with numbers or symbols replacing some letter (e.g. '@' for 'a')
- ☐ Based on a non-English word
- ☐ Based on a date
- ☐ Incorporates a passphrase (e.g. 'correcthorsebatterystaple')
- ☐ Based on meaningful information to you (e.g. names, favorite things, inside jokes)
- ☐ Uses lowercase letters
- ☐ Uses uppercase letters
- ☐ Longer than 8 characters
- ☐ Reused a password I use elsewhere
- ☐ Modified a password I use elsewhere
- ☐ Follows a password pattern I use elsewhere
- ☐ Created with a password manager
- ☐ Intentionally planned to use reset password feature
- ☐ Easy to read/say
- ☐ Uses numbers
- ☐ Uses symbols
- ☐ Other (please specify) _____
- ☐ I do not remember the exact password to this account
- ☐ I would prefer not to answer

7. Please briefly explain your overall strategy for making this specific password.

Please DO NOT tell us your actual password! We are only interested in the strategies you used to come up with your password.

8. Please briefly explain **why** you chose this strategy.

B.3 Shared accounts details

This section is repeated once each of the first four shared accounts that the participant reports in Part A

We'll be asking some questions about the "[account description]" [account type] account that you share with [number shared with] other people, including "[relationship]".

9. Who do you consider to be the owner(s) of this account? Check all that apply.

- ☐ Myself
- ☐ One other user
- ☐ Multiple other users
- ☐ Other (please specify) _____
- ☐ Not sure / Prefer not to answer

10. How did you determine the owner(s) for this account? Please select all that apply.

- ☐ Pays for this account
- ☐ Collects payment from other users
- ☐ Originally created this account
- ☐ Uses this account the most
- ☐ Has access to the email address associated with this account
- ☐ Other (please specify) _____
- ☐ Not sure / Prefer not to answer

11. Did one person come up with the password for this account, or was it a collaborative effort?

- ○ One person came up with the password for this account
- ○ The password for this account was a collaborative effort
- ○ A password manager or other tool was used to generate the password

- ○ Other (please describe) _____
- ○ Not sure / Prefer not to answer

12. Who was involved with creating the password to this "[account description]" account? Please select all that apply.
- □ Myself
- □ Other user(s) that I consider to be the owner or joint owner(s)
- □ Other user(s) that I do NOT consider to be the owner or joint owner(s)
- □ Other (please describe) _____
- □ Not sure / Prefer not to answer

The following question is only shown if the participant reported that they were involved with password creation (selected "Myself" in the previous question).

13. Think about the password you created or helped create for this "[account description]" account. How important were each of the following factors to you in creating this password?

	1 - Not important at all	2	3	4	5 - Extremely important	Prefer not to answer
Having a complex password	○	○	○	○	○	○
Having a memorable (to me) password	○	○	○	○	○	○
Having a memorable (to the people sharing with me) password	○	○	○	○	○	○
Having a password that is hard to guess	○	○	○	○	○	○
Having a long password	○	○	○	○	○	○
Having a password that is unique from my other passwords	○	○	○	○	○	○
Being able to store the password in a password manager	○	○	○	○	○	○
Other	○	○	○	○	○	○

14. To help us monitor the quality of our data, please select "Somewhat disagree".
- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither disagree nor agree
- ○ Somewhat agree
- ○ Strongly agree

The following question is only shown if the participant reported that they were involved with password creation.

15. Think about the password you made for [account description]. Did you use any of the following strategies to create your password? Check all that apply.

If you are unsure of the password or don't remember it exactly, please check the "I do not remember the exact password to this account" option.
- □ Based on the name of someone or something
- □ Based on a word or name with numbers/symbols added to beginning or end
- □ Based on a word or name with numbers or symbols replacing some letter (e.g. '@' for 'a')
- □ Based on a non-English word
- □ Based on a date
- □ Incorporates a passphrase (e.g. 'correcthorsebatterystaple')
- □ Based on meaningful information to you (e.g. names, favorite things, inside jokes)
- □ Uses lowercase letters
- □ Uses uppercase letters
- □ Longer than 8 characters
- □ Reused a password I use elsewhere
- □ Modified a password I use elsewhere
- □ Follows a password pattern I use elsewhere
- □ Created with a password manager
- □ Intentionally planned to use reset password feature
- □ Easy to read/say
- □ Uses numbers
- □ Uses symbols
- □ Other (please specify) _____
- □ I do not remember the exact password to this account
- □ I would prefer not to answer

The following question is only shown if the participant reported that they were involved with password creation.

16. Please briefly explain your overall strategy for making this specific password.

DO NOT tell us your actual password! We are only interested in the strategy you used to come up with your password.

The following question is only shown if the participant reported that they were involved with password creation.

17. **Why** did you choose this strategy?.

The following question is only shown if the participant reported that they WERE NOT involved with password creation.

18. Think about the password for [account description]. Does it use any of the following strategies? Check all that apply.

If you are unsure of the password or don't remember it exactly, please check the "I do not remember the exact password to this account" option.
- □ Based on the name of someone or something
- □ Based on a word or name with numbers/symbols added to beginning or end
- □ Based on a word or name with numbers or symbols replacing some letter (e.g. '@' for 'a')
- □ Based on a non-English word
- □ Based on a date
- □ Incorporates a passphrase (e.g. 'correcthorsebatterystaple')
- □ Based on meaningful information to you (e.g. names, favorite things, inside jokes)
- □ Uses lowercase letters
- □ Uses uppercase letters
- □ Longer than 8 characters
- □ Reused a password I use elsewhere
- □ Modified a password I use elsewhere
- □ Follows a password pattern I use elsewhere
- □ Created with a password manager
- □ Intentionally planned to use reset password feature
- □ Easy to read/say
- □ Uses numbers
- □ Uses symbols
- □ Other (please specify) _____
- □ I do not remember the exact password to this account
- □ I would prefer not to answer

The following question is only shown if the participant reported that they WERE NOT involved with password creation.

19. What do you think the person(s) creating the password were prioritizing by choosing these strategies? If you are unsure, please give us your best guess.

20. Do you use the password for [account description] on other accounts? Please select all that apply.
- □ Yes - I reuse the password exactly
- □ Yes - I use a variant of this password

- □ No - I do not reuse this password anywhere in any form
- □ Not sure
- □ Prefer not to answer

The following question is only shown if the participant reported that they reused this password (selected "Yes - I reuse the password exactly" and/or "Yes - I use a variant of this password" in the previous question).

21. Do you use the password for [account description] on other accounts? Please select all that apply.
- □ Personal account(s) (not shared with anyone else)
- □ Other shared account(s)
- □ Prefer not to answer

The following question is only shown if the participant reported that they reused this password with other shared accounts (selected "Other shared account(s)" in the previous question).

22. How would you describe the other shared account(s) that use the same password as this account? Check all that apply.
- □ I share the other account(s) with **exactly the same people** as I share this account with
- □ I share the other account(s) with **some, but not all** of the people I share this account with
- □ I share the other account(s) with **people I DO NOT share** this account with
- □ Prefer not to answer

23. Was this account always shared, or did it start as a personal account that later became a shared account?
- ○ This account was always shared
- ○ This account started as an individual account that later became shared
- ○ Not sure
- ○ Prefer not to answer

The following question is only shown if the participant reported that this account began as a personal account (selected "This account started as an individual account that later became shared" in the previous question).

24. When this account became a shared account, was the password changed or updated?
- ○ Yes - the password was updated
- ○ No - the password was not updated
- ○ Not sure
- ○ Prefer not to answer

25. Is two-factor authentication (2FA) currently enabled on this account?
- ○ Yes - two-factor authentication (2FA) is currently enabled on this account
- ○ No - two-factor authentication (2FA) is NOT currently enabled on this account
- ○ Not sure
- ○ Prefer not to answer

The following question is only shown if the participant reported that this account does not have 2FA enabled (selected "No - two-factor authentication (2FA) is NOT currently enabled on this account" in the previous question).

26. Was two-factor authentication (2FA) disabled in order to share this account?
- ○ Yes - two-factor (2FA) authentication was disabled
- ○ No - two-factor (2FA) authentication was NOT disabled
- ○ Not sure
- ○ Prefer not to answer

27. How did you distribute the password to other people sharing this account **OR** how did you receive the password to this account? Please check all that apply.
- □ Verbally (either in-person or over a phone call)
- □ Through e-mail, text, or instant messaging
- □ Other (please specify) _____
- □ Not sure
- □ Prefer not to answer

28. If you forgot the password for this account, what would you do? Please check all that apply.
- □ I would use the account's password reset mechanism.
- □ I would ask the account owner for the password.
- □ I would ask another person sharing the account (not the account owner) for the password.
- □ I sent the password to someone else/was originally sent the password through a text message or email, so I would check that.
- □ Other (please specify) _____
- □ Prefer not to answer

B.4 Demographics

29. What is your age? Please type "0" if you prefer not to say.

30. Please select the option that best describes your gender.
- ○ Male
- ○ Female
- ○ Nonbinary
- ○ Another gender (please specify) _____
- ○ Prefer not to say

31. What is your annual household income?
- ○ Less than $25,000
- ○ $25,000 to $34,999
- ○ $35,000 to $49,999
- ○ $50,000 to $74,999
- ○ $75,000 to $99,999
- ○ $100,000 to $149,999
- ○ $150,000 to $199,999
- ○ $200,000 or more
- ○ Prefer not to say

32. Please choose the highest level of education you have completed.
- ○ Have not completed high school
- ○ High school degree or equivalent
- ○ Associate's degree
- ○ Bachelor's degree
- ○ Master's degree
- ○ Professional degree beyond a bachelor's degree (e.g. MD, DDS)
- ○ Doctoral degree
- ○ Prefer not to say

33. Do you have a computer science background? This means working in or holding a degree in computer science or information technology.
- ○ Yes
- ○ No
- ○ Not sure
- ○ Prefer not to say

34. Do you have a background in computer or information security?
- ○ Yes
- ○ No
- ○ Not sure
- ○ Prefer not to say

35. Is there any feedback on our survey or additional information you'd like to provide to help us understand your responses or improve the survey?

C Full Codebooks

Code	Frequency		Definition
	Shared	Personal	
Meaningful info.	22.5% (111)	23.0% (53)	Uses information that is meaningful to at least one user
Memorable	20.6% (102)	14.8% (34)	Prioritized making the password memorable
Reuse	16.8% (83)	20.0% (46)	Reused (either exactly or a variant of) another password
Secure password	14.0% (69)	12.6% (29)	Prioritized making the password secure
Personal algorithm	13.8% (68)	18.7% (43)	Personal algorithm for passwords, such as minimum rules or a pattern of units (e.g., numbers-word-numbers)
Password generator	8.5% (42)	10.4% (24)	Used a password generator (i.e., one in a password manager)
Random	5.1% (25)	4.8% (11)	Created randomly without the use of a password generator
Passphrase	4.7% (23)	4.8% (11)	Passphrase that does not contain any meaningful information
Easy to use	3.2% (16)	0.9% (2)	Easy to use and enter
Unique	3.0% (15)	2.2% (5)	Intentionally avoided reusing an old password or making a similar password
Storage in manager	2.0% (10)	4.3% (10)	Being able to easily store and retrieve their password in a password manager
Related to service	1.4% (7)	6.1% (14)	Related to the service that the account is for
Simple	1.2% (6)	0.0% (0)	Prioritized simplicity
Just meet requirements	1.2% (6)	2.6% (6)	Minimally satisfies the account's password policy
Hard to use	0.8% (4)	0.0% (0)	Cumbersome to use
Another language	0.6% (3)	1.7% (4)	Derived from a non-English language
Environment	0.0% (0)	1.3% (3)	Participant's surroundings were used for parts of the password

Table 10: Password generation strategies used by participants for accounts where they were involved in password creation (494 shared, 230 personal). Participants sometimes indicated more than one strategy per password.

Code	Frequency		Definition
	Shared	Personal	
Recall	43.7% (216)	53.5% (123)	Wanted the password to be easy to recall for users
Secure account	35.4% (175)	43.0% (99)	Prioritized the security of the account
Easy to access account	8.5% (42)	2.6% (6)	Wanted the account to be accessed easily
Easy to make	5.9% (29)	4.3% (10)	Password was easy to make
Habit	4.0% (20)	3.0% (7)	Did what they normally did for password creation
Avoid reuse	3.0% (15)	3.9% (9)	Specifically wanted to avoid reusing a password
Low-value account	3.0% (15)	2.2% (5)	Felt that the account is low-value or does not have sensitive information, and that influenced their choice of password
Recommendation	2.2% (11)	1.7% (4)	Chose their strategy because others recommended it
Avoid reset	1.8% (9)	2.6% (6)	Did not want to be troubled to reset the password
No need to remember	1.6% (8)	1.3% (3)	Strategy would obviate need to remember password
Frequent use	0.6% (3)	0.4% (1)	Account is used often
High-value account	0.6% (3)	0.4% (1)	Felt that this account is valuable/has sensitive information influenced password creation for this account
Speed	0.6% (3)	0.4% (1)	Wanted to access the service as quickly as possible
Easy reset	0.2% (1)	0.0% (0)	Resetting the password is easy
Fun	0.0% (0)	2.2% (5)	Following strategy is enjoyable to them personally
Just meet requirements	0.0% (0)	1.7% (4)	Minimally satisfies the account's password policy

Table 11: Motivations for participants' choice of password strategy (among 494 shared, 230 personal accounts). Participants sometimes indicated more than one motivation per password.