Normal and Easy: Account Sharing Practices in the Workplace

YUNPENG SONG*, Xi'an Jiaotong University, China
CORI FAKLARIS, Carnegie Mellon University, USA
ZHONGMIN CAI†, Xi'an Jiaotong University, China
JASON I. HONG†, Carnegie Mellon University, USA
LAURA DABBISH, Carnegie Mellon University, USA

Work is being digitized across all sectors, and digital account sharing has become common in the workplace. In this paper, we conduct a qualitative and quantitative study of digital account sharing practices in the workplace. Across two surveys, we examine the sharing process at work, probing what accounts people share, how and why they share those accounts, and identifying the major challenges people face in sharing accounts. Our results demonstrate that account sharing in the modern workplace serves as a norm rather than a simple workaround; centralizing collaborative activity and reducing boundary management effort are key motivations for sharing. But people still struggle with a lack of activity accountability and awareness, conflicts over simultaneous access, difficulties controlling access, and collaborative password use. Our work provides insights into the current difficulties people face in workplace collaboration with online account sharing, as a result of inappropriate designs that still assume a single-user model for accounts. We highlight opportunities for CSCW and HCI researchers and designers to better support sharing by multiple people in a more usable and secure way.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in collaborative and social computing**.

Additional Key Words and Phrases: Accounts; passwords; workplace; cybersecurity

ACM Reference Format:
Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I. Hong, and Laura Dabbish. 2019. Normal and Easy: Account Sharing Practices in the Workplace. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 83 (November 2019), 25 pages. https://doi.org/10.1145/3359185

1 INTRODUCTION

Modern collaboration involves interacting with and through a large number of internet-connected platforms and tools with an increasingly diverse set of individuals across multiple organizations. In 2018, Hanamsagar et al. estimated that each person has around 80 online accounts across their

*This work was done when Yunpeng Song visited Carnegie Mellon University.
†Corresponding authors.

Authors' addresses: Yunpeng Song, ypsong@sei.xjtu.edu, Xi'an Jiaotong University, MOE KLINNS Lab, China; Cori Faklaris, cfaklaris@andrew.cmu.edu, Carnegie Mellon University, 5000 Forbes Ave, Pittsburgh, PA, 15213, USA; Zhongmin Cai, zmcai@mail.xjtu.edu.cn, Xi'an Jiaotong University, MOE KLINNS Lab, China; Jason I. Hong, jasonh@cs.cmu.edu, Carnegie Mellon University, 5000 Forbes Ave, Pittsburgh, PA, 15213, USA; Laura Dabbish, dabbish@cs.cmu.edu, Carnegie Mellon University, 5000 Forbes Ave, Pittsburgh, PA, 15213, USA.

2573-0142/2019/11-ART83 $15.00
https://doi.org/10.1145/3359185

work and personal lives [32]. At the same time, many if not all workplace platforms and tools, even those for collaborative work, are designed assuming that a single account is associated with a single person. For example, Saltzer and Schroeder's classic paper on information security discusses passwords in the context of a single user and does not mention password sharing [64]. The same is true for NIST's 2017 Digital Identity Guidelines [28]. The single user assumption can naturally lead to many difficulties in collaborative work where there are dependencies among the tasks people do and a need to share information and access.

As a result, sharing online accounts with other individuals is a practice that seems to permeate every sector of society. For example, at the end of 2017, British politicians prompted a heated discussion of password sharing on Twitter when credentials for accounts full of sensitive government information were shared not only with staff members but also with interns on exchange programs [37]. We define account sharing as situations in which multiple individuals access a single account, sharing the login and password for that account. In a U.S.-census-representative online survey conducted by SurveyMonkey this year [27], 34% of the 1,507 U.S. adults in their sample reported sharing passwords or accounts with their co-workers. With 95 million knowledge workers in the U.S., an estimated 32 million people in the U.S alone may be sharing their account information at work.

In this research, we take an approach focused on the needs and motivations of the people using collaboration tools and platforms, as opposed to the organizations within which they work. Although organizations' policies [22, 56, 70] often regard account sharing as a deviant practice, studies have shown that sharing is not simply a deviant practice to be stopped, but rather a behavior that should be treated with special thought and care [45, 46, 49]. For example, in non-work settings, sharing among intimate social groups is often motivated by access convenience and can be a way to signal trust in relationships [54, 59].

A more complete understanding of the nature of account sharing at work will help in designing tools, platforms, and organizational policies that better support collaboration as well as in prioritizing further research efforts on this topic. Towards this end, we present the results of our mixed-method research to understand the practices and challenges of account sharing in the workplace. We conducted two survey studies of account sharing: a qualitative survey on account sharing motivations, behaviors, and challenges, and a quantitative survey validating the behaviors observed.

Our findings demonstrate that online account sharing in the modern workplace has become a primary option rather than a workaround, with people sharing, on average, 11 accounts with their co-workers. People tend to employ simple strategies to share their credentials, and workplace sharing has very legitimate collaboration drivers. However, people still struggle with a lack of activity accountability and awareness, conflicts over simultaneous access, difficulties controlling access, and collaborative password use. We consider how improvements to the design of account and password management could address some of these challenges.

Our research is part of a broader effort to increase understanding of social influences on security and privacy. Our goal in this work is to bridge the socio-technical gap between collaboration needs in the workplace and account security designs that assume that a single user is associated with an account [1]. Designing account access and credential systems with social aspects in mind will lead to more-secure technology-supported collaboration.

2 RELATED WORK

Previous work in both non-workplace and workplace contexts has touched on the topic of account sharing [2, 9, 38, 45, 49, 50, 54, 59, 65, 67]. We discuss this related work in more detail below. Our

study builds on this prior work to add a more detailed picture of account sharing in the modern workplace across a variety of organizations and contexts.

2.1 Collaboration in the modern workplace

Work is being digitized across all sectors as internet connected platforms are used to generate, share, refine and process information in organizations [24, 57, 71]. As early as 2005, studies showed that workers switch among email, corporate intranets, messaging applications, internet portals, and corporate websites to accomplish their work [19, 55]. Employees are required to manage access to a myriad of internet-connected platforms as they work with colleagues and collaborators across the globe [15]. In their study of digital nomads, Jarrahi et al. describe how an increasing level of personal agency is applied in adopting and adapting digital tools at work against a background of digitally mediated social relationships with collaborators, clients, and peers [44]. Account sharing is a key behavior that people use to navigate the interconnected nature of digital account use in the modern workplace.

2.2 Account sharing in the workplace

Account sharing appears to be a common practice in the workplace in the U.S. and other countries, despite the fact that it is often discouraged or violates organizational information technology policy. In a large-scale U.S. survey (n=1167), Stanton et al. [68] found that 23% of respondents sometimes shared their passwords with members of their work groups, 7% shared their passwords with someone in their company but outside their work groups. In another large-scale study (n=1208), Happ [33] found that one-third of the participants indicated that they knew at least one of their colleagues' passwords, and 22% of participants had shared accounts with at least one colleague. In a smaller study (n=36), Kaye [45] estimated that 20% of people had shared their work email passwords with colleagues. In a 2017 survey of Israeli medical staff on Facebook, 220 (73.6%) out of 299 participants reported they had obtained the password of another medical staff member in the course of doing their work [34].

Several studies of security behavior in the workplace note scenarios that led to account sharing within particular settings including information technology and medical organizations. For example, Inglesant and Sasse [38] described how password sharing was the *de facto* method among their participants of controlling access to password-protected shared files. Blythe [9] reported sharing as a workaround used in large groups to access useful services, sometimes because of the services charged by person rather than by organization. Bartsch et al. [6] showed how sharing passwords to access documents in their organization's system helped colleagues to circumvent long wait times for official authorization. Koppel et al. [49] found that in a hospital setting sharing was taught as the correct way to gain quicker access to medical resources, with medical staff taping sticky notes with passwords onto devices; a password to a medical resource was shared throughout an entire hospital in this way. Hassidim et al. [34] reported that medical staff, especially students, interns, and residents, shared accounts because they were sometimes not given system accounts despite having to use these systems to fulfill duties. Similar to findings on account sharing in families and among romantic partners, Weirich et al. [73] and Sasse et al. [65] found that password disclosure was seen as a sign of trust between colleagues and that social pressures made it difficult for people to refuse a request to share their password.

Past work focuses on security behaviors within a single organization and focused on enterprise-wide internal accounts or resources. None of this work focused exclusively on account sharing behavior, and so could not provide a complete picture of the different ways people share accounts and why they do so. These studies primarily noted account sharing as one behavior among a set of security practices in a particular context, and they observed sharing mainly as a workaround

to circumvent security barriers. In our study, we sought to provide a more complete picture of account sharing in the workplace for both internal and public online accounts from employees at a variety of organizations across different industries.

2.3 Sharing in non-workplace contexts

Sharing has been more extensively studied in non-workplace contexts. A body of research on account sharing in the home, among family members, and in romantic relationships, highlights social considerations and logistics as key sharing motivations. One commonly observed social motivation for account sharing is demonstrating trust. Singh et al. [67] investigated bank account and PIN numbers sharing behaviors in Australia and found sharing was an expression of trust rather than a lack of awareness of the need to keep access codes confidential. In the Kingdom of Saudi Arabia (KSA), Alghamdi [3] found that sharing bank accounts within households was common and arose from religious and cultural practices; withholding banking information from a spouse was seen as a sign of distrust. In the U.S., Matthews et al. [54] found trust in the household member was a strong influence on the decision to share accounts, on the level of security enforced on the shared accounts, and on the number of security precautions used.

Account sharing is also used to define and enforce relationship status. Dunphy et al. [20] collected tweets on the topic of passwords and reported that in some cases, the sharing of passwords appeared to be a social obligation among romantic partners or friends. Park et al. [59] and Jacobs [43] found account sharing was a way to maintain romantic relationship well-being and promote intimacy. Bevan [7] found password sharing for social networking sites (SNS) was a form of online surveillance between romantic partners.

Another key motivation for sharing accounts is to facilitate a shared task or activity. Studies such as [43, 54, 59] highlighted that convenience, along with proximity, was a key driver of password sharing in household and family environments. Others [3, 67] noted how such sharing helped in solving specific practical or logistic problems, for instance how to purchase retail goods or conduct banking while disabled or living far from urban areas.

Although social considerations and logistics motivate account sharing among close ties, it is not clear to what extent these motivations arise in the workplace. In the workplace a different set of relational considerations, expectations and norms are in place. Our study seeks to complement and extend the previous research on account sharing into the workplace setting.

2.4 Account sharing and the socio-technical gap

Account sharing falls clearly in the socio-technical gap described by Ackerman [1], where there is a divide between what we know we must support socially and what we are currently able to support technically. Although account sharing is commonplace, it is not something most digital accounts are designed to do and violates many technical assumptions about account security. Security architectures and practices often assume a one-account-one-user model (e.g., see [28, 64]) and either do not incorporate or refuse to consider a one-account-multiple-users model.

User experience designers often design account affordances for individuals rather than groups, resulting in difficulties in account sharing. For example, Brush [10], Lampinen [50], and Matthews [54] found that family members had trouble presenting multiple people in a single profile, struggled to customize settings and content, and expressed the time cost and mental effort of switching among multiple profiles was often too high. Park et al. [59] found similar usability issues for romantic partners who shared accounts.

Account sharing is also often strictly forbidden by official organizational security policies. Kirlappos et al. [46, 47] labeled the use of workarounds to restrictive organizational security policies as "shadow security." They found that rather than violating security policies maliciously,

Table 1. Study 1 - demographic breakdown of participants from MTurk ($N = 98$)

Gender		Age		Education		Employment		Organization size	
Female	37.8%	18-24	16.3%	High school or less	11.2%	Full time	88.8%	2-19	18.4%
Male	61.2%	25-34	38.8%	Some college	24.5%	Part time	8.2%	20-99	25.5%
Other	1.0%	35-44	27.6%	2-year college	12.2%	Other	3.1%	100-999	32.7%
		45-54	14.3%	4-year college	45.9%			1000+	20.4%
		55+	3.1%	Graduate	6.1%			I don't know	3.1%

employees did, in fact, try to behave in a secure way even when defying official policies, although their behaviors were not those the security experts recommended.

In order to bridge the socio-technical gap around account sharing at work, we conducted two studies on workplace account sharing. Our goal was to add to the body of knowledge on who shares workplace accounts and why, as well as what challenges or problems are experienced with account sharing and how widespread these problems are. In Study 1, we conducted a qualitative survey with open-ended questions to capture the variety of motivations for and behaviors around account sharing at work as well as the challenges people currently have with account sharing. In Study 2, we designed and deployed a follow-up quantitative survey with close-ended questions to examine the prevalence of account sharing behaviors and motivations and delve more deeply into shared account security challenges.

3 STUDY 1: QUALITATIVE SURVEY ON ACCOUNT SHARING

Our goal in the first study was to obtain an understanding of the range of account sharing practices, motivations, and challenges across a variety of individuals working in different industries, organization sizes, and roles.

3.1 Methods

We asked open-ended questions about participants' experiences with and stories about account sharing in the workplace. We used initial screening questions to identify participants who worked full-time or part-time in the last three months for pay at an organization apart from crowdsourcing platforms, and who shared at least one account with others in their workplace. Participants were asked to list accounts they shared and describe how and why they shared those accounts, as well as the challenges they faced in sharing.

3.2 Sample

We used an online crowdsourcing platform, Amazon Mechanical Turk (MTurk), in order to recruit participants from diverse workplaces across the United States. Past work suggests that online crowdsourcing platforms, such as MTurk, can facilitate access to participants with different backgrounds and socioeconomic status. MTurk samples can be more representative than many traditional pools, such as local convenience samples which can be dominated by college students and internet samples in general [11, 58, 63]. Only a small subset (less than 14%) of U.S.-based MTurk workers report Mechanical Turk as their primary source of income [31, 40, 58] suggesting it is possible to obtain responses on MTurk from people employed elsewhere full or part time.

We posted our survey on Amazon Mechanical Turk in April 2018 and collected 98 responses after removing invalid responses. We limited participation to U.S. residents above 18. Participants had to have more than 50 tasks approved with an approval rating over 95%. The average time to complete the survey was 6.2 minutes (Median=5.4, SD=6.4) and we paid $1 to each participant.

Table 2. Password sharing methods

Type	Behavior	Example Quotes
Direct sharing	Tell others verbally Tell others via email Tell others via SMS, Slack, etc. Write it down on paper	"My boss informs us at our morning meeting or an email is sent with the information." (P75, UPS, Non-profit, 50-99 person organization)
Common location	Update it on a shared spreadsheet or file Write it on a post-it or board	"We actually just write them down and stick them on a board next to the computers that they are used on." (P19, Amazon account, Manufacturing, 20-49 person organization)
A shared system	Update the password based on a formula Use a password manager to share it	"We use a company-wide password manager that will update on all computers at the same time if needed." (P35, Social media, Real estate, 50-99 person organization)
Access sharing	Help someone else log in Share the password reset link	"It's a bit annoying for me personally, because I have to login for everyone else." (P67, Ecommerce account,Technology, 10-19 person organization)

3.3 Results

The authors used a bottom-up approach, open coding to identify themes from the responses in the survey within each of the three central categories of sharing motivations, practices, and challenges. Within each category, we discussed the identified codes until we reached a consensus that the codes covered all the themes emerging from responses. We list *Participant ID, Shared account, Industry, Size of organization* after quotes in parentheses to provide a more detailed picture of the story.

3.3.1 Password Sharing Strategies. To better understand peoples' practices around sharing accounts, we looked at the methods people were using to exchange login information for different accounts and maintain shared access. Apart from taping passwords onto a shared device [49] and directly telling others [6], participants described a wide variety of ways they shared account credentials with their co-workers, which we organized into four categories: direct sharing, using a common location, a shared system, or access sharing. Table 2 summarizes the sharing strategies participants described using to inform others of new passwords. While many of their sharing methods were simple, our participants were aware of the potential security issues, and they employed their own methods to protect those accounts.

The first category of password sharing methods involved *directly sharing password information.* Direct sharing methods included telling other people the login and password information verbally (without leaving any physical trails), writing it down to give others, or sending the login through an email message or messaging application (e.g. Slack, SMS). In some cases people tried to maintain security when sharing by using an encrypted email, sending the password and user name separately.

Common location methods involved putting login and password information in a commonly accessible place such as a shared whiteboard, or shared spreadsheet. Many participants were aware of security risks around sharing passwords in a common location and added an extra layer of protection to keep the password from those who should not have access. They described trying to hide or lock the paper with passwords on it or use another password to protect the file containing other passwords.

> "If a new person we did not know gets hired we take our password information down and disclose that information to the new hire after their probation period is over and then we put the login information back up on the board." (P19, Amazon, Manufacturing, 20-49 person organization)

Table 3. Motivations for sharing and example quotes (with *Participant ID, Shared account, Industry, Size of organization* in parentheses)

Motivations	Example Quotes
1. Centralizing collaboration	
Central place to share work and information.	"We have a common Google drive account with all our work loaded on it for efficiency, my team is good at divvying up work and making sure everyone does their share." (P24, Google Drive, Transportation & logistics, 100-499 person organization)
Collaboratively manage company official accounts.	"It gives the brand one image, don't want to confused customer with multiple accounts." (P14, Facebook, Hospitality, 2-19 person organization)
Transparency of activities, work, and transactions.	"We pool our finances and it's easier to pay and see what the other is spending." (P32, eBay, Retail, 2-5 person organization)
2. Ease of boundary management	
Fewer logins and passwords.	"I usually only have to look up ad content on a few occasions, so it is easier to just use their account rather than setting up and maintaining another account." (P63, Twitter, 10-19 person organization)
Temporary or emergency access.	"I share these accounts because it is convenient for another person to help when I am unavailable." (P66, Instagram, Manufacturing, 100-499 person organization)
3. Saving money on shared resources	"For the shipping accounts it saves a good amount of money because we get money off by how much is shipped under the same account." (P19, UPS, Manufacturing, 20-49 person organization)
4. Demonstrating trust	"[It']s just more convenient and make the other person feel closer to you" (P80, Facebook, Manufacturing, >1,000 person organization)

> "We actually have a book that has all of the shared log in/password information. We lock the book in a file and have to lock it up when it is done being used." (P11, ESL, Education, >1,000 person organization)

Another method of sharing passwords was *having a shared system* for password generation or access so that everyone who knew or used the system could generate the password as needed and log in. Shared systems involved generating a password following a formula or accessing the password using a password manager. People were not given the password directly, but they could figure it out when necessary. P16 described how using a shared formula let him and his collaborators update their account password bi-weekly without having to share it directly:

> "We have a system that we use to update the password so it is changed bi-weekly and everyone knows the formula for how the password is changed so everyone always knows the updated password based on the date." (P16, Shipping, Transportation & logistics, 100-499 person organization)

Similarly, by using a password manager, people did not need to share the password directly, as the account credentials could be auto-filled by the password manager.

Finally, participants reported using *access sharing methods* whereby a few people mainly took charge of the account and others usually did not know the password. This method involved sending the password reset link to a co-worker so they could create a new password for the account and access it temporarily. In other cases, people granted access to another co-worker by physically logging him/her in at their device rather than giving them the password for the account.

3.3.2 Motivations for Sharing. Contrary to security news that describes account sharing as careless and non-compliant with security policies [14, 26], we observed account sharing was treated as a preferred option rather than a workaround; there were very legitimate collaboration drivers behind account sharing and people sharing accounts were trying to create smooth and efficient workflows. We coded four general themes emerged from our data (centralizing collaboration, ease of boundary

management, saving money on shared resources, and social benefit) along with several sub-themes, described below. Motivations for account sharing are presented in Table 3, along with example quotes from our participants illustrating each theme. Our findings are consistent with the prior work in identifying some of the same motivations for account sharing in the workplace, including temporary or emergency access [6, 34, 48] (belonging to ease of boundary management), saving money on shared resources [9], and demonstrating trust [65, 73]. However, we identified a new set of motivations focused on streamlining workflows in modern workplace collaboration through online accounts.

Centralizing collaboration. Collaboration with online accounts plays a key role in account sharing in the modern workplace. A major reason people described sharing accounts was to create a central place that could act as a hub for team activity in order to provide a shared understanding of the status, progress, and details of ongoing work activities by their collaborators.

Participants described using shared accounts within their teams as a central platform to post tasks, share resources, and schedule activities. Whenever they wanted to access the most current information, they turned to the shared account to find what they want. As one participant described:

> "Having one account for multiple people to use allows multiple people to easily access the information on that account rather than having to split the information between multiple accounts... Plus it allows all files to be stored on that one account which is also more convenient." (P64, Email, Education, 500-999 person organization)

As another participant described, the shared account acted as the "combined intelligence" for their group:

> "We choose to share these accounts because it is, in a sense, our combined intelligence. We trade heavily together and thus use the same account to pull funds from/leverage our own funds against. It's more efficient to share one account than have separate accounts for each employee since we act as a team." (P56, Funds account, Technology, 6 - 9 person organization)

Organizations are paying more attention to building and promoting their brand images online, leading to much essential work to be done through social media and customer service platforms. But organizations often only have one verified Facebook account or a few official email addresses to simplify communication for customers and these accounts are usually designed for single users. As a result, several people reported simply directly sharing official social media accounts and emails (see Table 3).

Transparency, that is the ability to observe and obtain awareness of others activity, was another collaborative motivation for sharing accounts. Participants were concerned with two key aspects of transparency: financial activity and work progress. Our participants said that they shared the same account to track what others purchase and facilitate financial transparency.

> "The logistics account is used by many to track incoming things for receipt inspection." (P6, Logistics, Engineering/Architecture, >1,000 person organization)

Participants also expressed the need for transparency of work progress, to make sure everything goes well and to know what others are working on.

> "Sometimes we need access to each other['s] documents, especially when we are out of the office. It helps us communicate better as well to know what each of us is working on." (P30, Email, Retail, 2-5 person organization)

Ease of boundary management. The other primary motivation for sharing accounts was to lower the cost of boundary management. Setting up and creating new accounts was described as high effort and sometimes delaying work. Sharing an account meant people could avoid having to create a new account, maintained fewer accounts, and managed fewer passwords.

> "[It is] easier for work to just use the same account to have fewer passwords." (P33, Skype, Retail, 500-999 person organization)

> "It was convenient to work with the same account instead of having to create multiple accounts to access the same thing." (P11, Email, Retail, 100-499 person organization)

Our participants also reported the need for temporary or emergency access as a reason for account sharing. Simply sharing login credentials and then changing the password afterward provided a low cost way of temporarily sharing access to a shared resource. As one participant described:

> [I share the account] so that there can be someone there in time when I am off. (P45, HRIS platform, Technology, 100 - 499 person organization)

In this case, account sharing was viewed as a low effort way to support temporary access for task delegation and work sharing when workloads increased.

Saving money on shared resources. Similar to past work examining sharing of accounts in the context of households [54], romantic relationships [59], and workplace [9], economics were also a motivation for sharing accounts at work. Sharing a single account among a team or multiple colleagues saved money and provided a resource the entire team could still use.

> "Design company user accounts - here this is more about saving money because the organization doesn't have money for multiple accounts." (P64, Design website, Education, 500-999 person organization)

Demonstrating trust. Account sharing was also used for emotional and social connection among coworkers. Sharing acted as a way to demonstrate trust for colleagues, reinforcing existing ties.

> "[B]ecause we all work on the trust system but in this way we can work well together." (P46, Tyler solutions account, >1,000 person organization)

Sharing as a sign of trust is also mentioned by several past studies as a motivation for account sharing among family members or in romantic relationships [48, 54, 59, 65, 73].

3.3.3 Sharing Challenges. Since most accounts are typically designed for one person, a wide range of usability and security issues emerged when accounts were shared. Each challenge highlights a limitation in existing collaboration system design that assumes single-user access and points to ways we might better support collaboration on a shared resource.

Lack of Activity Accountability. Although shared accounts were employed to centralize information and support activity awareness, this use sometimes backfired because of difficulty differentiating who did what within an account at what time. Since everyone was using the same set of login credentials, all actions were tied with a single account merging the activity of multiple individuals into a single whole, with notifications of new activity delivered sometimes only to the person currently logged in.

People reported a lack of accountability for actions on shared accounts as well as difficulty knowing when or whether something had happened because they did not receive notifications of new activity. A common model for accounts regards all the people with the same credential as one

Table 4. Challenges in sharing

Challenges	Example Quotes
1. Lack of Activity Accountability	
Lack of accountability	"It can be confusing to know if my coworker has responded to messages or if I need to respond to customer question. So there have been situations where we fix a problem twice." (P12, Facebook, Government, 20-49 person organization)
Notification failure	"One of us may read a new message and the other person misses it because the notification disappears." (P42, HRIS platform, Technology, 100-499 person organization)
2. Conflicts over Simultaneous Access	
Conflicting changes made by multiple access	"Sometimes we'll start an email on one computer and try to finish it on another but the account won't sync across devices." (P96, Microsoft Office 365, Public Relations, 100 - 499 person organization)
Logging each other out of the account	"Multiple people can not typically work on the same site at the same time. It usually kicks someone out." (P38, Online Registration Site, Education, 100-499 person organization)
3. Controlling Access	
Informing of new passwords	"They have forgotten to input the new logins on the shared spreadsheet and no one could do any of our customer contacts until the manager who changed them came in the next day." (P97, Email, Technology, 20-49 person organization)
Access violations	"The shipping account's password never changes, even when people leave the company, which is a security concern." (P90, Shipping, Education, 500-999 person organization)
4. Collaborative Password Use	
Easily locked by multiple incorrect attempts	"There have been several instances where passwords were changed and the person who changed one did not communicate that to the rest of us, and we tried over and over again so the account would get locked out." (P19, Amazon, Manufacturing, 20-49 person organization)
Losing access to password reset email	"I have had the problem in the past of my former employers contacting me years after I left the company[,] looking for passwords of the social media I had set up with my email in the past." (P76, Facebook, Finance, 20-49 person organization)
Two-factor authentication	"I once had to wait on two-factor authentication, when the other person was not available. I had to switch and work on something else instead." (P63, Twitter, 10-19 person organization)

single user, and thus the account activities from different people are all merged together without any way to tell people apart, making it hard to trace who did what. One participant described challenges associated with lack of accountability when a mistake took place,

> "In the past we've dealt with discrepancies and issues such as wrong information being entered into a financial account and then later not being able to confirm who exactly was responsible." (P8, financial account, Retail, 20-49 person organization)

Besides the situation above, participants reported three scenarios where a common activity history also sometimes harmed productivity due to lack of awareness of actions made by other co-workers with access. For example, team members made efforts to fix a problem and only to find that it was solved multiple times (see Table 4). As one participant explained, picking up tasks through the same account meant they could not tell whether or not co-workers had finished a fair share of the work since all the tasks were posted together:

> "We use the twitter together to announce new products or to share goodwill messages with customers just to keep us on their mind...[Some are] not picking up jobs fast enough even though they are on duty, it is hard to track this." (P60, Request login, Technology, >1,000 person organization)

This lack of accountability for actions in a shared account also led to small accidents that were difficult to detect and undo, for example putting files in the wrong place in Dropbox, changing the names of files, and unintentionally deleting other people's files, all of which led to trouble in finding the correct files. Since the operations came from multiple people, it was hard to notice and fix the problems.

People reported missing updates because of notification failures in shared accounts. Because a new notification dismisses once it is read by a user, others missed notifications of shared activity.

A merged activity history also caused problems as participants complained that it was difficult to backtrack the information they needed.

> "History of searches is flooded with other workers history which makes it difficult to go back and look at certain products." (P14, Email, Retail, 100-499 person organization)

Conflicts over Simultaneous Access. Many accounts are designed so that people can only be logged in from one device at a time. Because of this people ran into two common issues: being kicked out of the account and conflicting changes by multiple people.

Some accounts only allow one instance at a time, leading some participants to report being logged out because someone else tried to log in (See Table 4 for examples). Our participants reported that when multiple users are working simultaneously on a shared account they would sometimes be locked out of the shared account, delaying work or canceling out changes the person had been trying to make.

> "[W]e have had more than 1 person at a time mak[ing] adjustments and had them cancel each other and the account locked." (P81, Google AdWords, 20-49 person organization, Business Intelligence)

Even when people could simultaneously access the account, low synchronization rates for different instances under the same account caused collaboration problems. People worked together on the account but changes were not shown to each other in a timely manner meaning they could inadvertently undo each other's work or conflict with it.

> "Sometimes it is hard when multiple people are working at once because the changes come up delayed and cause conflicts." (P63, Google Drive account, Accounting, 50 - 99 person organization)

Controlling Access. Account sharing in the workplace also raised difficulties around controlling or limiting the set of people who could access the account. Access control for shared accounts meant keeping track of and managing who had the credentials and informing the right people of updates to passwords.

While it might be easy to keep password sharing working smoothly in a small group, things got harder for large groups or when the turnover rate was high. As a result, several participants reported suffering work delays and problems waiting for new passwords.

> "It is easy for too many people to have the password, and challenging when it needs to be changed and you have to update everyone." (P81, Shipping, Non-profit, 100 - 499 person organization)

The use of a central place for password information, and the informal and sometimes manual nature of tracking who had access to an account led to difficulties limiting or revoking access in the face of turnover or team membership changes. People reported challenges with account information being shared with people who should not have access through shared spreadsheets.

> "The spreadsheet allows anyone who sees it to know the current password even if they are not authorized to use the company email." (P37, Email, Health, 100-499 person organization)

People also described challenges with former employees retaining access to shared accounts because passwords were not changed even after someone left the organization. They also noted how shared password locations could lead to people in other groups having credentials to a shared account as well.

> "We actually just write [password] down and stick them on a board, ... Someone from outside from ups or fedex could see our amazon login information and use the companies account." (P22, Amazon, Manufacturing, 20 - 49 person organization)

Collaborative Password Use. Participants described shared passwords as having its own set of associated challenges. People had to collaboratively maintain a secure password on a shared account and ensure all co-workers or collaborators had up to date information about the password and login. We identified three key issues associated with password management on shared accounts: account lockouts, losing access, and two-factor authentication. These issues stemmed in part from the fact that it was difficult to notify everyone with account access to a new password in a timely manner.

People described not being able to access a shared account because their co-workers accidentally locked the account after multiple incorrect login attempts, a common security practice for many online services. For a shared account, this event would lock everyone out of the account.

> "We have the constant problem of people logging in with the wrong password, if someone does this three times it locks everyone out until we get a system administrator to reset everything. I wish there was a way to lock someone out individually or to make it easier for us to get access if it is locked." (P60, Work order login, Technology, >1,000 person organization)

Shared accounts were often associated with one individual or one email address, meaning changing or updating the password could only be done by that person. Because of this, participants also encountered the problem of losing access to the password reset email. One participant described how he had set up a shared social media account with his own email, and after he left the organization no one had access to the password reset email (See Table 4).

Lastly, while two-factor authentication (2FA) is highly recommended by security experts [16, 39], it caused problems with accessing shared accounts. 2FA typically augments "what you know" (typically a password) with "what you have" (e.g. a secret code sent to a phone) to authenticate valid account users. However, the "what you have" is usually associated with a token (e.g., a co-worker's personal phone, a USB security key), which may not be easily available for other people and severely impacting the usability of 2FA.

> "If an employee is not around to enter a code on their phone, it makes logging in slow and I will have to wait till they are available to input the code texted to them." (P53, Bank of America, Retail, >1,000 person organization)

3.3.4 Study 1 Summary. In Study 1 we identified practices around account sharing, motivations for sharing accounts, and challenges people had with the accounts they shared. People used a variety of strategies to share account credentials including directly providing the login and password, using a shared place to store account information, a shared system for generating passwords, and facilitating access rather than sharing credentials. They were aware of potential security issues and employed their own methods to protect the account. We found people had very legitimate collaboration

drivers behind account sharing to create smooth and efficient workflows; they shared accounts to provide a central hub for collaborative activity, shared access to a common set of resources, awareness of actions and changes to those resources, and to lower the cost of managing access. However, people ran into challenges tracking who did what within these accounts, simultaneously accessing the accounts, controlling access as people left organizations or moved across teams, and collaboratively managing the account password.

Although this study provided an understanding of the variety of account sharing behaviors, it did not tell us how common these behaviors were and how they varied based on the nature of work people were doing. We conducted a follow-up study described in the next section in order to understand how many accounts people shared, how account sharing varied across industries and organization sizes, and the relative frequency of different account sharing behaviors.

4 STUDY 2: QUANTITATIVE SURVEY ON ACCOUNT SHARING

Based on the responses from Study 1, we designed a follow-up quantitative survey with close-ended questions to examine the prevalence of behaviors and motivations identified in Study 1.

4.1 Survey Design

We used the themes from Study 1 to create closed-ended survey questions about sharing behaviors, motivations, and challenges. We divided the survey into three sections of questions about account sharing behaviors in the workplace. Section 1 asked the full range of accounts each person shared to give us an overview of the number and types of accounts being shared. Section 2 was intended to capture detailed information about a subset of each person's accounts (1-3) to allow us to conduct account level analyses. Finally, section 3 asked about the participants' work contexts and demographics.

Section 1 - Account sharing overview. In the first part of the survey, we asked participants to select which accounts they shared with colleagues in the workplace, choosing from a list of 498 common accounts grouped by category. For each category, we also asked participants if there were any other accounts in that category that they used and shared. Our category organization and account list were drawn from top-ranking websites and apps listed on Alexa.com, Google Play, Apple App Store, G2 Crowd, Capterra, and SimilarWeb (see Table 8) and refined based on feedback from expert colleagues and pilot tests.

We regard websites or apps with the same username and password but with highly different uses as separate accounts. For example, we consider Gmail and YouTube as separate accounts even though one could login using one set of credentials. We felt that merging Gmail and YouTube into one account would confuse the analysis, since Gmail and YouTube fall into different categories and obviously have dissimilar sharing patterns. For accounts which support sharing a single file rather than sharing access to the entire account, such as Google Docs and Dropbox, we added an explanation at the beginning of the survey as well as on pages with such accounts, explaining the difference between selective sharing and sharing the entire account, and asking participants to only report on account sharing.

Section 2 - Shared account details. In the second part of the survey, participants provided details about 3 shared accounts randomly selected from those the indicated sharing in the first part of the survey. Our questions in this section are briefly presented in Table 9.

Section 3 - Work context and demographic information. In the third part of the survey, we asked participants about their organization size, industry and about their job role and demographics.

In order to ensure data quality, we inserted an attention check question between section 1 and 2. The attention check question asked participants to select an account they did not share in the

Table 5. Study 2 - demographic breakdown of participants from MTurk (N = 140) and Prolific (N = 148)

Gender		Age		Education		Employment		Organization size	
Female	55.6%	18-24	16.7%	High school or less	7.9%	Full time	75.0%	2-19	25.4%
Male	43.4%	25-34	35.8%	Some college	19.1%	Part time	21.2%	20-99	22.2%
Other	1.0%	35-44	18.1%	2-year college	15.3%	Other	3.8%	100-999	25.7%
		45-54	20.0%	4-year college	39.2%			1000+	24.7%
		55+	9.4%	Graduate	18.4%			I don't know	2.1%

first part of the survey from a list of 4 options. We only report here data from participants who correctly answered the attention check question [41].

4.2 Sample

We conducted Study 2 on Amazon Mechanical Turk and Prolific Academic between July and August 2018. Prolific Academic is a newer but more diverse crowdsourcing platform with better quality and a low overlap of participants with MTurk [53, 60].

Participants in Study 2 were restricted to U.S. residents above the age of 18. We had a total of 288 participants, including 140 from MTurk and 148 from Prolific, after excluding 24 responses that failed the attention check questions (14 from MTurk and 10 from Prolific). The average time to complete the survey was 29.1 minutes (Median=24.1, SD=16.0) and participants were compensated $4. Our study samples from MTurk and Prolific were not significantly different in demographic makeup, in terms of age (χ^2(4, 288)=0.59; p>.8), gender (χ^2(2, 285)=0.22; p>.6), education levels (χ^2(4, 288)=6.72; p>.1), and organization sizes (χ^2(3, 282)=3.02; p>.3). We merged the two samples to conduct our analysis presented below. See Table 5 for a breakdown of sample characteristics. A large fraction of the participants had a Bachelor's or higher and was also younger compared to the US population overall [62]. These differences are a function of the demographics of the crowdsourcing platform, which tends to attract younger more technology-savvy users [35]. Our 288 participants each provided sharing details for up to 3 accounts, for a total of 814 account sharing reports.

5 RESULTS FOR STUDY 2

We conducted both quantitative analyses investigating what accounts people share in the workplace, characteristics of those shared accounts, motivations to share, and their sharing strategies in practice. We also conducted some qualitative analysis on our probes about password managers and securing accounts in the face of employee turnover.

5.1 Overview: Sharing Levels, Categories, and Frequency of Use

Our 288 participants indicated sharing a total of 3318 accounts overall. We conducted a series of analyses on this data to look at how many accounts people shared on average and what types of accounts were more shared than others.

5.1.1 Number of accounts shared. In general, the results indicate that people share many accounts with their co-workers. On average, participants reported sharing 11.4 accounts (Min=1, Max=34, Median=10, SD=8.0) in the workplace. Over half of our participants (52%) shared 10 or more accounts with colleagues and co-workers. Only one-fifth (21%) of participants shared less than 5 accounts. Note that Hanamsagar et al. estimated 80 total online accounts (work and non-work) per user in 2018 [32], so sharing almost 12 accounts on average with co-workers is not surprising.

5.1.2 Most-shared categories and accounts. Participants reported sharing across various account categories. Figure 1 shows the most commonly shared accounts in our data. Due to space constraints,

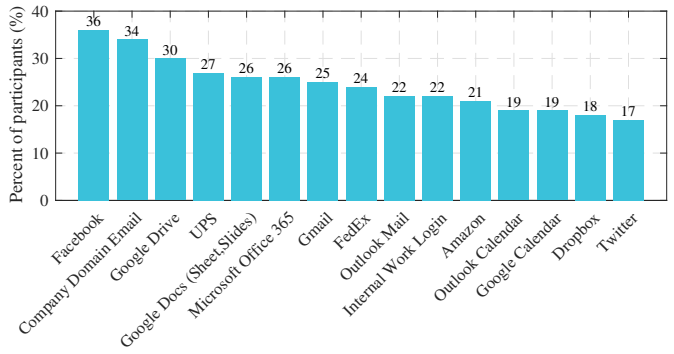

Fig. 1. The 15 most-shared accounts, along with percent of people sharing

we only list the top 15 accounts shared by our participants. Facebook was shared by the largest proportion of our participants, followed by company email accounts. Facebook was often managed by multiple people and our qualitative data in the study suggested sharing helps for "advertising" and 24/7 "customer service". Company email was also commonly shared, used as a unified identity to respond to people outside their team, get order notifications from places like Amazon, and broadcast among themselves.

5.1.3 Breadth of Sharing and Frequency of Use. In order to understand the nature of sharing and the importance of shared accounts, we looked at how widely accounts were shared and how frequently shared accounts were used among the 814 accounts that our participants described in detail.

Breadth of sharing. A majority of the accounts in our sample (55%) were shared with a small group of no more than 5 people. Combined with results from Study 1, this finding suggests a great deal of account sharing may be happening within work groups and teams. The other accounts are shared with more than 5 people and 20% of accounts were shared with even larger groups of more than 10 people.

Frequency of use. Participants frequently accessed the shared accounts they reported on, suggesting shared accounts are central to their work. 62% (501) of the accounts are used at least once a week and 21% (170) are used more than 3 times a day.

5.2 Sharing Motivations and Strategies

Building on our qualitative work, we were interested in the relative frequency of password sharing strategies and sharing motivations. Participants in our survey provided strategies and motivations for sharing each of the three accounts they described in detail in response to a closed-ended question.

5.2.1 Password sharing strategies. Table 6 shows the sharing strategies participants used to inform others of a new password. The most common strategy used for 34% accounts was to tell others verbally, followed by writing the password down on paper or board (19%). Writing passwords down is often seen as a violation of policy, but as we explained in Study 1, people used their own methods to make the strategies safer. In practice, it seems to be a popular way to share passwords. We noticed that 5% of the accounts changed the password based on a predetermined formula.

Besides the password sharing strategies above, we also noticed that 13% of the accounts in our sample had 2-factor authentication enabled. This adoption rate is only slightly lower than 17% reported by Daniel Humphries [36] for workplace passwords in general.

Table 6. Account sharing strategies to inform others of a new password (N=814)

Sharing Strategies	Percent of accounts	Sharing Strategies	Percent of accounts
Told others verbally	34%	Updated it on a shared spreadsheet or file	7%
Wrote it down on paper or board	19%	Used a password manager to share it	6%
Told others via email	17%	Updated the password based on a formula	5%
Helped by someone else to log in	14%	Shared the password reset link	4%
Told others via SMS, Slack, etc.	9%	Other (e.g., I don't know the password)	8%

Table 7. Motivations for sharing (N=814)

Themes	Motivations	Percent of accounts
Centralizing collaboration	Central place to share work and information.	49%
	Collaboratively manage company official accounts.	40%
	Transparency of activities, work, and transactions.	36%
Ease of boundary management	Fewer logins and passwords.	33%
	Temporary or emergency access.	24%
Saving money on shared resources	Saving money.	18%
Demonstrating trust	Trust and connection.	8%
Other reasons	Other reasons	4%

5.2.2 Motivations for Sharing. Centralizing collaboration was the most important theme for sharing accounts in our sample. The most common sharing motivation was having a central place to collaborate (49%). 40% of accounts were shared to collaboratively manage company official accounts. Transparency was another primary reason for sharing in the work context, with 36% of accounts in our sample shared for this reason. Many of the participants described how accounts were shared to lower boundary management costs. This included reducing the number of logins and passwords (33%), or providing Temporary or emergency access (24%). Note that in past work examining sharing of devices within households [54] and sharing accounts in romantic relationships [59], economic reasons and emotional needs were the dominant reasons for sharing. However, in the work context, these two reasons (18% for economics and 8% for emotional needs) were less prevalent.

5.3 Security Challenges associated with Collaborative Password Use

In Study 2, we included open-ended questions about specific accounts, to probe details about sharing-related security challenges observed in Study 1. We asked participants whether they used a password manager, and if not, why. We also asked how they managed employee turnover.

5.3.1 Password managers for sharing. Password managers are emphasized as a best practice by many popular media (New York Times [8], BBC news [72], and Washington Post [25]) and security experts [29, 32, 39, 66]. Nevertheless, even though password managers were used more often for high sensitivity accounts, they generally had a low adoption rate (6%).

We found many participants lacked a good understanding of password managers and were not aware of the security benefits. One participant wrote:

> "A password manager is just one more account to worry about" (P228, Email, consulting, 100-499 person organization).

For those that did understand password managers, participants reported other reasons for not adopting them. (1) Password managers perceived as insecure because of ease of use. One participant wrote,

> "The company does not want such easy access for security reasons." (P120, UPS, Manufacturing, 50-99 person organization)

The assumption here is quite different from a household, since there may be unfamiliar people in a workplace, and people perceived that convenience could lead to unexpected access. (2) Team decision. For password managers to work, an entire group had to agree to all use the same password manager and in some groups this did not happen. If someone feels it is *"too high tech for most people" (P209, Amazon, Education, >1,000 person organization)*, the team is likely to discard the idea. (3) Company policy. Some organizations had their own password policy which directly or indirectly forbade password managers. For example,

> "My company doesn't allow passwords written, typed or saved anywhere." (P192, SUNGARD account, administrative, 10-19 person organization).

5.3.2 Handling Employee Turnover. Employee turnover was a major issue for shared accounts described in Study 1 since former employees with malicious intent could do harm via the shared account. One participant in our Study 1 reported a particularly negative experience with turnover:

> "One of our employees left on bad terms. And as a parting gift he changed some passwords. He also managed to change the recovery email address and it took some time to recover access to the accounts." (P59 in Study 1, website login, Technology, >1,000 person organization)

Therefore, in Study 2, we examined how people handled shared credentials in light of staff turnover. When someone left the company, people most commonly changed the password on the shared account to secure it (42%). Our participants reported other methods, too (15%). For example, participants indicated the IT team might revoke the former employee's access. They also reported limiting physical access to the device on which the account was logged in. A few participants reported that whenever the account was accessed, they would receive notification emails, so they could keep a close eye on whether or not it was being used illegitimately by any ex-employees. One participant indicated they would simply create a new account to restrict ex-employee access.

Of all the responses, 19% said *"We did not do anything"*. When looking into these responses, we found four major reasons leading to inaction. The first was that they would like to continue sharing the accounts with ex-employees. They usually got along well with the former employees in this case and kept the password unchanged if the shared account could benefit the former employees. For example,

> "We kept the password the same, as I told the former employees if they wished to still leverage the repository to enhance their learning, they were more than welcome to" (P35, Lynda.com, Health, 50-99 person organization).

The second reason people reported was that they worked on the trust system and trusted ex-employees. They believed former employees would not harm the accounts.

> "When someone we trust leaves on good terms, we do nothing. When someone leaves on poor terms, we come up with a new formula [for password] and system" (P199, One Drive account, Retail, 50-99 person organization).

The third reason was they explicitly didn't care about account security since it was their organization at risk instead of themselves. As one participant described:

> "[T]o be perfectly honest it's the company who's paying for all of the things we order. We don't really care if someone else gets into the account or not" (P169, Amazon, Technology, 50-99 person organization).

The last reason was that the account was not sensitive so continued access had little risk. As one participant described:

> "This account generally doesn't have info that is too sensitive. If someone sees it, it's no biggie" (P20, company email, Printing, 50-99 person organization).

However, even a non-sensitive account credential leakage could lead to a chain-reaction of other account compromises [17, 32, 42] due to password reuse in the workplace [36].

6 DISCUSSION

In our two studies, our findings support and extend the results of previous studies of account sharing. Consistent with previous work, we found that people often share passwords in work settings for temporary access, saving money, and demonstrating trust [2, 9, 38, 48, 49, 65, 73]. Our work extends this previous work by illustrating the methods people use for sharing passwords with each other and their motivations behind doing so, particularly as they associate with collaborative work in the modern workplace. We present a qualitative and quantitative analysis of motivations for sharing beyond convenience and getting work done, strategies for how passwords are shared and why those strategies are used, as well as challenges in sharing (such as employee turnover, two-factor authentication, lack of accountability, being locked out of accounts due to others, and being logged out). Below, we focus on the new findings from our work and provide some implications for design.

6.1 Account Sharing as a Preferred Option

In the prior literature on security in the workplace, account sharing was usually regarded as a workaround when official work policies failed in daily activities. However, we noticed our participants expressed that sharing was often a better option than having separate accounts (See example quotes in 3.3.2). Participants explicitly opted to share one account even when they had the choice to use different accounts. This shift from an alternative workaround to a preferred option is facilitated for three reasons.

First, organizations are now expected to use social media and other digital communication to keep in touch with customers. Even small businesses carefully build their brand image online. For such commercially branded social media and email, communicating from one account is a preferred choice in order not to confuse the customers.

The second reason is online services (e.g., Google account, UPS, and even online finance) play a crucial role in the modern workplace collaboration. However, distinct from custom-built internal systems tailored around a specific organization's needs, these public online services are not designed exclusively for a certain work task or setting. Their design is purposely open-ended to support a wide variety of uses across many different domains. People may find using a shared account with these services makes their workflow and collaboration more efficient than separate ones simply because of the nature of the work they are doing or because of limitations in the service design for their unique purposes.

Third, people may prefer sharing to streamline the number of distinct services and accounts they need to manage. Online services sometimes require users to create a bunch of new accounts to access different aspects of the service while the internal services and systems in the workplace usually already provide a mandatory account for each user and could also implement Single sign-on (SSO) with one account accessing all the resources. In an age where people are managing 80 accounts across their work and personal lives on average [32], sharing is a way they can reduce the burden of creating, remembering, as well as maintaining an account.

The fact that online accounts now permeate both workplace (using public online accounts for certain work-related tasks) and daily life (already having too many non-work accounts to remember and maintain) contributes to account sharing shifting from a workaround to the first option. The fact that only a small portion of our respondents indicating sharing as a means to circumvent

the authorization and save money suggests service providers could take responsibility to improve account access designs.

6.2 Balancing the Security / Collaboration Tradeoff

Our findings reveal a tension in online account design between security and some of the basic requirements of collaborative work. Participants in our study wanted to maintain collective access to and awareness of a central repository of information, a basic need in collaborative work with any level of activity interdependence [52]. Because people used a single authentication they had challenges with simultaneously accessing that information store, accidentally overwriting or undoing others work on that shared repository and identifying who made what changes.

It is important to consider how authentication for collaborative work can provide social translucence while maintaining security. The concept of social translucence introduced by Erickson and Kellogg describes socially translucent systems as those that "support coherent behavior by making participants and their activities visible to one another" [21]. They derive a set of principles for such systems from face to face interaction: visibility, awareness, and accountability. Current single user accounts that are co-opted for shared collaborative purposes lack all three of these. It is not always possible for people to see when another person is logged in to a shared account, they cannot tell what actions another person is taking on the account, and it is very difficult to tie actions to individuals meaning there is no accountability for the actions being taken.

The vast literature on coordination in CSCW may provide some basic guidelines designers, developers, and security researchers can draw on to inform more socially appropriate account authentication and access. In one of the earliest CSCW papers on the topic, Malone and Crowston delineate three generic types of interdependencies each implying a different set of information online platforms can make visible [51]. These include things like displaying timing and history of activity to support coordinating timing of activity. The CSCW literature on awareness also provides frameworks and learnings designers can draw on as they consider how to balance security against coordination needs (e.g. [12, 13, 30]). Early work by Gutwin and Greenberg delineates elements that contribute to people's workspace awareness including presence information (who is involved in an activity), objects (what objects are they using), and actions (what are they doing), among other things. More recent notions of social transparency consider the design space of online platforms that can hide or make visible details about the individuals, their actions on shared artifacts and their interactions with others in the platform [69].

Designers and developers of online platforms need to recognize account sharing as a prevalent behavior and can draw from existing theory and results in CSCW to design for collaboration while maintaining information security.

6.3 Implementing Selective Sharing is Not Enough

Some accounts, such as Google Drive, allow people to share a single file rather than sharing access to the entire account. As noted in our methods section, to distinguish between this kind of selective sharing and sharing accounts, we added an explanation on pages with such accounts, explaining the difference between selective sharing and sharing the entire account, and asking them just report on account sharing. Interestingly, even with selective sharing features, a large number of these accounts, such as Google Docs and Dropbox, were still shared by participants. Several responses for Microsoft Office 365 and Google Drive directly mentioned that sharing the account was much easier to avoid having to forward links and modify permissions.

From the user's perspective, there are some disadvantages to selective sharing. First, selective sharing costs more to set up and maintain all the accounts needed, since each member of the entire group has to have an individual account. However, our results suggest one-third of accounts are

shared for fewer logins and passwords, indicating a lack of motivation to create and maintain multiple accounts. Second, using a shared password removes the burden of remembering an individual password. Participants in Study 1 expressed that they did not worry about remembering the shared password at all since they were able to ask around easily at any time. Third, as discussed before, people get tired of forwarding links and managing permissions. Thus, even though implementing selective sharing is useful to deal with some challenges such as activity tracking, it is not a one-size-fits-all solution in the wild.

6.4 Improving Adoption of Password managers

Password managers offer at least three benefits in terms of account sharing with others. First, the sharer is able to hide the password while still allowing access and can revoke access if someone leaves the organization. Second, password managers usually provide a log of which passwords were accessed, by whom, and when. Third, there is no need to inform others of changed passwords, as things are synced automatically. Past literature talked about the obstacles for individuals to adopt password managers [4, 5, 23, 31]. However, they all considered inaction from an individual-centric perspective. In this paper, we reported how a group of people might collectively decide not to use password managers in the workplace.

We have two implications for design here. First, there are many common misunderstandings as to how password managers work which need to be rectified before they can be more widely adopted. Second, past work has found that more social features, and observability in particular, can help with the adoption of security features on Facebook [18]. It may be possible to incorporate more of these kinds of features into password managers, to facilitate incremental adoption by a group rather than convincing the entire group all at once. For example, a password manager might allow a password to be sent to another person in the group via email (along with an easy way to install the password manager).

6.5 Implications for the Design of Online Accounts

Our findings build on previous work to uncover some of the basic motivations for account sharing along with a number of challenges in sharing accounts in the workplace. In particular, we saw people struggle with activity accountability in shared accounts, controlling access to the account, and collaborative password use. While there does not seem to be a simple solution for addressing all of these challenges, there are some relatively simple things that services could do to address some of these problems.

One account - multiple email addresses. One easy feature platforms could add is allowing two or more email addresses for an account, which could help with password recovery in the case of employee turnover and facilitate awareness of login attempts (both successful and failed) by others.

Simultaneous access. Another feature that would address some of the challenges observed in our study would be allowing multiple people to be logged in at the same time. There are, however, economic and technical reasons why services might disallow this.

Multiple profiles. Yet another possible feature that could address issues of activity accountability would be multiple profiles. People could still login with a single common account but could then select who they are after logging in. One example of this type of authentication system is Netflix which offers multiple profiles per subscription. One issue with Netflix's implementation is that there is no shared area or representation of joint actions on information. Individuals' information and actions are confined to the profile. Adding a shared log of actions that distinguishes who did what would facilitate awareness and an area for collaboration. However, multiple profiles could suffer from malicious insider attacks (since a person could easily lie about profiles), and doesn't

address the problems of password management and employee turnover (e.g., continued access to an account).

Single user name, multiple passwords. One potential feature that could address challenges with password management is having one username with multiple passwords. This would leave the burden of creating and maintaining the account to the first user to create an account within a team or organization. This first user could distribute passwords to the other users and these passwords could potentially distinguish their activities within the account. The advantage of this method is that it is transparent to later users and does not change their current workflow. The service would be able to tell different users apart by the password they used to log in. Furthermore, an account owner could revoke access in an easy way. However, with more passwords, an account may be more vulnerable to attacks, such as dictionary attacks [61]. In this case, using a tool such as a password manager to auto-generate a strong and unique password could mitigate the risk.

Task delegation support. Our results also highlight the opportunity to design explicitly for task delegation. Account sharing represents an all-or-nothing approach to delegation that may allow broader access than is desirable. Systems could implement temporary access mechanisms like logins with an expiration date to prevent extended access after a task is complete. Another possibility is task-specific restricted data access within an account to minimize potential for harm or data loss beyond what the task requires.

6.6 Limitations

Our study has some limitations. First, we relied on self-report survey data. This allowed us to sample participants across a broad variety of job roles and organizations. It also limited, however, the extent to which we could contextualize sharing behaviors within the nature of participants' work and interactions with collaborators. An important area for future research is examining how the account sharing behaviors and motivations we observed may vary with contextual features like organizational culture, teamwork arrangements, task type, remote work, and physical context.

The use of self-report may also mean there is some inaccuracy in responses. In the first part of Study 2, even though we alphabetically listed the popular accounts in each category to help participants recall as many shared accounts as possible, participants may still have missed some. However, in early testing of our surveys, we observed that participants experienced a hard time recalling their shared accounts. Compared with recalling without any cues, we believe our method is more accurate. Second, we screened for people who shared at least one account, so our survey population may be biased. For example, we did not capture people sharing no accounts. However, given past work about the prevalence of account sharing, along with our results about the number of accounts shared and how many people those accounts are shared with, we feel that our results offer good insights into this phenomenon. Third, in our data, we only know the number of accounts they share, but we miss the number of accounts they have. So we do not have a shared account ratio for our participants as a baseline, therefore our data tells who shares more accounts but fails to tell who likes to share accounts more.

7 CONCLUSION

We conducted a qualitative and quantitative study of digital account sharing practices in the workplace. Across two surveys, we examined the sharing process at work, probing what accounts people share, how and why they share those accounts, and identifying the major challenges people face in sharing accounts. Our results demonstrate account sharing in the modern workplace serves as a normal rather than a simple workaround; centralizing collaborative activity and reducing boundary management effort are key motivations for sharing. But people still struggle with a lack of activity accountability and awareness, conflicts over simultaneous access, difficulties controlling

access, and collaborative password use. Our work provided insights into the current difficulties people face in workplace collaboration with online account sharing as a result of inappropriate designs that still assume a single user model for accounts. We highlight opportunities for CSCW and HCI researchers and designers to better support sharing by multiple people in a more usable and secure way.

ACKNOWLEDGMENTS

We are grateful for the insightful comments proposed by the anonymous reviewers. The work is supported in part by the National Science Foundation under Grant No. CNS-1704087, National Natural Science Foundation of China under Grant No. 61772415, and the scholarship from China Scholarship Council under Grant No. 201706280183.

REFERENCES

[1] Mark S Ackerman. 2000. The intellectual challenge of CSCW: the gap between social requirements and technical feasibility. *Human–Computer Interaction* 15, 2-3 (2000), 179–203.
[2] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.
[3] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. 2015. Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. In *SOUPS*. 297–308.
[4] Nora Alkaldi and Karen Renaud. 2016. Why Do People Adopt, or Reject, Smartphone Password Managers? (2016).
[5] Salvatore Aurigemma, Thomas Mattson, and Lori Leonard. 2017. So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? (2017).
[6] Steffen Bartsch and Martina Angela Sasse. 2012. How users bypass access control and why: the impact of authorization problems on individuals and the organization. (2012).
[7] Jennifer L Bevan. 2018. Social Networking Site Password Sharing and Account Monitoring as Online Surveillance. *Cyberpsychology, Behavior, and Social Networking* 21, 12 (2018), 797–802.
[8] J. D. Biersdorfer. 2017. Taking Your Passwords With You Anywhere. https://nyti.ms/2uT4b4D
[9] Jim Blythe, Ross Koppel, and Sean W Smith. 2013. Circumvention of security: Good users do bad things. *IEEE Security & Privacy* 11, 5 (2013), 80–83.
[10] AJ Bernheim Brush and Kori M Inkpen. 2007. Yours, mine and ours? Sharing and use of technology in domestic environments. In *International Conference on Ubiquitous Computing*. Springer, 109–126.
[11] Michael Buhrmester, Tracy Kwang, and Samuel D Gosling. 2011. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on psychological science* 6, 1 (2011), 3–5.
[12] John M Carroll, Dennis C Neale, Philip L Isenhour, Mary Beth Rosson, and D Scott McCrickard. 2003. Notification and awareness: synchronizing task-oriented collaborative activity. *International Journal of Human-Computer Studies* 58, 5 (2003), 605–632.
[13] John M Carroll, Mary Beth Rosson, Gregorio Convertino, and Craig H Ganoe. 2006. Awareness and teamwork in computer-supported collaborations. *Interacting with computers* 18, 1 (2006), 21–46.
[14] CIOReview. 2019. Password Sharing and its Impact on Enterprise Data Security. https://www.cioreview.com/news/password-sharing-and-its-impact-on-enterprise-data-security-nid-28268-cid-145.html
[15] Amy Colbert, Nick Yee, and Gerard George. 2016. The digital workforce and the workplace of the future.
[16] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 456.
[17] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The Tangled Web of Password Reuse. In *NDSS*, Vol. 14. 23–26.
[18] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. 2015. The role of social influence in security feature adoption. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. ACM, 1416–1426.
[19] Thomas H Davenport. 2005. *Thinking for a living: how to get better performances and results from knowledge workers*. Harvard Business Press.
[20] Paul Dunphy, Vasilis Vlachokyriakos, Anja Thieme, James Nicholson, John McCarthy, and Patrick Olivier. 2015. Social media as a resource for understanding security experiences: A qualitative analysis of# password tweets. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 141–150.
[21] Thomas Erickson and Wendy A Kellogg. 2000. Social translucence: an approach to designing systems that support social processes. *ACM transactions on computer-human interaction (TOCHI)* 7, 1 (2000), 59–83.

[22] Facebook. 2018. Terms of Service. https://www.facebook.com/legal/terms
[23] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences* 7, 1 (2017), 12.
[24] Chris Forman. 2005. The corporate digital divide: Determinants of Internet adoption. *Management Science* 51, 4 (2005), 641–654.
[25] G. A. Fowler. 2019. Help Desk: Digital life after death, passwords on Post-its and a new Comcast nightmare. https://www.washingtonpost.com/technology/2019/02/28/help-desk-digital-life-after-death-passwords-post-its-new-comcast-nightmare/?utm_term=.e3c1ea71752b
[26] Bradley Freedman. 2017. Important Changes to Password Best Practices Guidance. https://www.lexology.com/library/detail.aspx?g=25b5cdc0-ab11-4224-9044-fa49114b7b83
[27] J Gebhardt. 2019. Password sharing is a huge security threat, so why do people do it? https://www.surveymonkey.com/curiosity/why-people-share-passwords-with-coworkers/
[28] PA Grassi, JL Fenton, EM Newton, RA Perlner, AR Regenscheid, WE Burr, JP Richer, NB Lefkovitz, JM Danker, Yee-Yin Choong, et al. 2017. NIST Special Publication 800-63b: Digital Identity Guidelines. https://doi.org/10.6028/NIST.SP.800-63b
[29] Eric Grosse and Mayank Upadhyay. 2013. Authentication at scale. *IEEE Security & Privacy* 11, 1 (2013), 15–22.
[30] Carl Gutwin and Saul Greenberg. 2002. A descriptive framework of workspace awareness for real-time groupware. *Computer Supported Cooperative Work (CSCW)* 11, 3-4 (2002), 411–446.
[31] Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2018. User Behaviors and Attitudes Under Password Expiration Policies. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 13–30.
[32] Ameya Hanamsagar, Simon S Woo, Chris Kanich, and Jelena Mirkovic. 2018. Leveraging semantic transformation to investigate password habits and their causes. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 570.
[33] Christian Happ, André Melzer, and Georges Steffgen. 2016. Trick with treat–Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior* 61 (2016), 372–377.
[34] Ayal Hassidim, Tzfania Korach, Rony Shreberk-Hassidim, Elena Thomaidou, Florina Uzefovsky, Shahar Ayal, and Dan Ariely. 2017. Prevalence of sharing access credentials in electronic medical records. *Healthcare informatics research* 23, 3 (2017), 176–182.
[35] Paul Hitlin. 2016. Turkers in this canvassing: young, well-educated and frequent users. http://www.pewinternet.org/2016/07/11/turkers-in-this-canvassing-young-well-educated-and-frequent-users/
[36] Daniel Humphries. 2015. Best Practices for Workplace Passwords. Retrieved January 20, 2015 from https://www.softwareadvice.com/security/industryview/password-workplace-report-2015/
[37] Troy Hunt. 2017. The Trouble with Politicians Sharing Passwords. Retrieved December 4, 2017 from https://www.troyhunt.com/the-trouble-with-politicians-sharing-passwords
[38] Philip G Inglesant and M Angela Sasse. 2010. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 383–392.
[39] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *SOUPS*, Vol. 15. 1–20.
[40] Panagiotis G Ipeirotis. 2010. Demographics of mechanical turk. (2010).
[41] Panagiotis G Ipeirotis, Foster Provost, and Jing Wang. 2010. Quality management on amazon mechanical turk. In *Proceedings of the ACM SIGKDD workshop on human computation*. ACM, 64–67.
[42] Blake Ives, Kenneth R Walsh, and Helmut Schneider. 2004. The domino effect of password reuse. *Commun. ACM* 47, 4 (2004), 75–78.
[43] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. 2016. Caring About Sharing: Couples' Practices in Single User Device Access. In *Proceedings of the 19th International Conference on Supporting Group Work*. ACM, 235–243.
[44] Mohammad Hossein Jarrahi, Gabriela Philips, Will Sutherland, Steve Sawyer, and Ingrid Erickson. 2019. Personalization of knowledge, personal knowledge ecology, and digital nomadism. *Journal of the Association for Information Science and Technology* (2019).
[45] Joseph'Jofish' Kaye. 2011. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2619–2622.
[46] Iacovos Kirlappos. 2016. *Learning from "shadow security": understanding non-compliant behaviours to improve information security management*. Ph.D. Dissertation. UCL (University College London).
[47] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. 2015. Shadow security as a tool for the learning organization. *ACM SIGCAS Computers and Society* 45, 1 (2015), 29–37.
[48] Iacovos Kirlappos and Martina Angela Sasse. 2015. Fixing Security Together: Leveraging trust relationships to improve security in organizations. Internet Society.

[49] Ross Koppel, Sean W Smith, Jim Blythe, and Vijay Kothari. 2015. Workarounds to computer access in healthcare organizations: you want my password or a dead patient?. In *ITCH*. 215–220.
[50] Airi MI Lampinen. 2014. Account sharing in the context of networked hospitality exchange. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. ACM, 499–504.
[51] Thomas W Malone and Kevin Crowston. 1990. What is coordination theory and how can it help design cooperative work systems?. In *Proceedings of the 1990 ACM conference on Computer-supported cooperative work*. ACM, 357–370.
[52] Thomas W Malone, Thomas W Malone, and Kevin Crowston. 1994. The interdisciplinary study of coordination. *ACM Computing Surveys (CSUR)* 26, 1 (1994), 87–119.
[53] Diogo Marques, Tiago Guerreiro, Luís Carriço, Ivan Beschastnikh, and Konstantin Beznosov. 2019. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM.
[54] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. She'll just grab any device that's closer: A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 5921–5932.
[55] Andrew P McAfee. 2006. Enterprise 2.0: The dawn of emergent collaboration. *Enterprise* 2 (2006), 15–26.
[56] Microsoft. 2018. Microsoft Services Agreement. https://www.microsoft.com/en-us/servicesagreement
[57] Sara B Morris-Docker, Angela Tod, Joy M Harrison, Dan Wolstenholme, and Richard Black. 2004. NursesâĂŹ use of the Internet in clinical ward settings. *Journal of Advanced Nursing* 48, 2 (2004), 157–166.
[58] Gabriele Paolacci, Jesse Chandler, and Panagiotis G Ipeirotis. 2010. Running experiments on Amazon Mechanical Turk. *Judgment and Decision Making* 5, 5 (2010).
[59] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*.
[60] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153–163.
[61] Benny Pinkas and Tomas Sander. 2002. Securing passwords against dictionary attacks. In *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 161–170.
[62] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 666–677.
[63] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. In *How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples*. IEEE, 0.
[64] Jerome H Saltzer and Michael D Schroeder. 1975. The protection of information in computer systems. *Proc. IEEE* 63, 9 (1975), 1278–1308.
[65] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the "weakest link" - a human/computer interaction approach to usable and effective security. *BT technology journal* 19, 3 (2001), 122–131.
[66] Richard Shay, Iulia Ion, Robert W Reeder, and Sunny Consolvo. 2014. My religious aunt asked why i was trying to sell her viagra: experiences with account hijacking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2657–2666.
[67] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 895–904.
[68] Jeffrey M Stanton, Kathryn R Stam, Paul Mastrangelo, and Jeffrey Jolton. 2005. Analysis of end user security behaviors. *Computers & security* 24, 2 (2005), 124–133.
[69] H Colleen Stuart, Laura Dabbish, Sara Kiesler, Peter Kinnaird, and Ruogu Kang. 2012. Social transparency in networked information exchange: a theoretical framework. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*. ACM, 451–460.
[70] UPS. 2019. UPS Technology Agreement. https://www.ups.com/us/en/help-center/legal-terms-conditions/technology-agreement.page?
[71] Patricia Wallace. 2004. *The Internet in the workplace: How new technology is transforming work*. Cambridge University Press.
[72] M Ward and M Wall. 2018. How can we stop being cyber idiots? https://www.bbc.com/news/technology-45953238
[73] Dirk Weirich and Martina Angela Sasse. 2001. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms*. ACM, 137–143.

A APPENDIX

Table 8. Account categories and example accounts presented in the survey

Purpose	Category	# of Accounts Presented	Examples
Social networking	Email, Messaging, and Video Call	20	Gmail
	Social, Blogging, and Forum	20	Facebook
Shopping & Shipping	E-Commerce	20	Amazon
	Logistics and Delivery	20	UPS
Productivity	Cloud Storage and Computing	20	Dropbox
	Documents and Scheduling	20	Office 365
	Internal Network Software	12	Internal Work Login
	Scientific Software	16	Autodesk
	Training and Digital Library	28	Lynda.com
Business	Advertising and Marketing	28	MailChimp
	Customer Relationship	16	Salesforce
	Human Resources	20	Indeed
	Business Intelligence and Survey	24	Qualtrics
	Project Management and ERP	28	Sharepoint
	Website Builder	20	GoDaddy
Finance	Accounting, Payroll and Tax	28	QuickBooks
	Banking and Payment	24	PayPal
	Crowdfunding and Fundraising	16	GoFundMe
	Insurance	20	Aetna
	Utilities	24	Xfinity
Government	Government	18	irs.gov
LifeStyle	Entertainment	20	YouTube
	Health and Fitness	16	Mayo Clinic
	Food and Travel	20	Uber

Table 9. Account specific survey questions (types are *MC*: multiple choice, *Y/N*: yes/no, *Free*: open-ended entry, *Likert*: Likert scale)

Question category	Type	Question description
Overview	MC	Frequency of the account being used by the participant
	MC	Number of people who share this account
	Y/N	Paid account or free account
General usage	Free	Rationale for using this account
	Likert	Self-reported sensitivity level of the account
Sharing behaviors	MC	Sharing motivations
	MC	When the password was changed last time
	MC	Sharing strategies
Account Security	Y/N	Two-factor authentication or not
	Y/N	Password manager or not
	Free	Reasons why participant does not use a password manager
	Free	Coping strategies with the shared account when there is turnover
Issues in sharing	MC	Frequency of issues with the account
	Free	Other issues

Received April 2019; revised June 2019; accepted August 2019