

‘It’s Problematic but I’m not Concerned’: University Perspectives on Account Sharing

SERENA WANG*, Human-Computer Interaction Institute, Carnegie Mellon University, USA

CORI FAKLARIS*, Human-Computer Interaction Institute, Carnegie Mellon University, USA

JUNCHAO LIN, Human-Computer Interaction Institute, Carnegie Mellon University, USA

LAURA DABBISH, Human-Computer Interaction Institute, Carnegie Mellon University, USA

JASON I. HONG, Human-Computer Interaction Institute, Carnegie Mellon University, USA

Account sharing is a common, if officially unsanctioned, practice among workgroups, but so far understudied in higher education. We interview 23 workgroup members about their account sharing practices at a U.S. university. Our study is the first to explicitly compare IT and non-IT observations of account sharing as a “normal and easy” workgroup practice, as well as to compare student practices with those of full-time employees. We contrast our results with those in prior works and offer recommendations for security design and for IT messaging. Our findings that account sharing is perceived as low risk by our participants and that security is seen as secondary to other priorities offer insights into the gap between technical affordances and social needs in an academic workplace such as this.

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

KEYWORDS

account sharing, usable security, academic collaboration, higher education

ACM Reference format:

Serena Wang, Cori Faklaris, Junchao Lin, Laura Dabbish, and Jason I. Hong. 2022. “It’s Problematic but I’m not Concerned”: University Perspectives on Account Sharing. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6, CSCW1, Article 68 (April 2022), 27 pages. <https://doi.org/10.1145/3512915>

1 INTRODUCTION

Though much work today takes place via secured computing systems that support collaboration among multiple users [8,13,28,54], designs for information technology (IT) and cybersecurity often presume an individual user. Today’s employee also does not simply access computing networks from within a secured perimeter [54]. They may have as many as 80 online accounts for personal and work use [26], and switch between IT-specified systems and user-preferred

This work was sponsored by the U.S. National Science Foundation under grant no. CNS-1704087. Faklaris was also supported by the Center for Informed Democracy and Social Cybersecurity (IDeaS) at Carnegie Mellon University.

Authors’ address: Human-Computer Interaction Institute, School of Computer Science, Carnegie Mellon University, 5000 Forbes Ave., Pittsburgh, PA, 15213, USA.

* Wang and Faklaris contributed equally to the paper.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

2573-0142/2022/April – Article#68 \$15.00

© Copyright is held by the owner/author(s). Publication rights licensed to ACM.

<https://doi.org/10.1145/3512915>

devices permitted under Bring Your Own Device (BYOD) or Choose Your Own Device (CYOD) policies [69]. Despite IT accommodations like these, the gap between technical affordances and social needs [1] often forces workers who are security-conscious [2,31] to make compromises with official IT policies and procedures in order to get their jobs done [7]. One compromise is account sharing, in which more than one person uses the same username and password to access a work resource [57]. In fact, a recent survey of gig workers who also are employed in settings such as retail or shipping found that sharing accounts designed for individual use is now accepted as a “norm” [57].

However, one important work setting has so far been understudied: the research university. In 2018 in the U.S., about 6,000 postsecondary schools employed nearly 4 million [70] and served 16.6 million enrolled undergraduate students [71]. These are unlike other workplaces because of their mission of *academic freedom* – the freedom to teach, to learn, to publish, and to inquire [4,46,72]. Consequently, IT strategies for securing the information network-in-use [73] is likely to center on intrusion detection [30] and to not include top-down methods of controlling user behavior (such as social media use policies, internet firewalls, or monitoring for data loss prevention). Some institutions use a federated IT model, which allows for subunits of the university such as schools or departments to hire IT staff and operate their own systems to, in part, “enable research, teaching and community service” [74]. They will tolerate or encourage CYOD and self-management of IT for their workforce, which is a mix of traditional in-office employees and of remote and/or mobile workers such as “digital nomads” [16,29,40]. For non-IT users, this could result in “shadow security,” workarounds to official rules and setups that help employees manage the risks they understand while getting their jobs done [35]. Academic freedom complicates the implementation and communication of university IT policies [14,62,63] and has led to conflicts with copyright holders over campus use of peer-to-peer file sharing [51].

Table 1: In comparison with a typical large-scale non-academic business in the U.S., the university in our study has a federated IT model and, among student employees, high turnover and many part-time jobs.

Point of comparison	Specific U.S. university in our study	Typical large-scale U.S. non-academic business
Limits on tech use	Culture of no limits due to academic freedom	Limited by company policies and culture
Organization structure	Divisional [65]	Hierarchical [65]
IT model	Federated [74]	Centralized [75]
Types of sensitive data	Student data covered by the Family Educational Rights and Privacy Act (FERPA), payroll data, intellectual property, and other research-related data	Varies by industry [76]
Research as priority	High	Varies by industry
Employee turnover	High for students, lower for faculty or staff	Varies by industry (Hospitality high, utilities low) [77]
Part-time share of jobs	Many part-time jobs for student employees, mostly full-time for faculty and non-student staff	Varies by industry (Hospitality and retail high, information and financial low) [78,79]

Vulnerabilities	Multiple points of entry for attackers, compromised data, malware, low security awareness across networks [10,75]	Single points of failure that can take down system, ransomware, risk is concentrated among key employees and their support staff [10,75]
Resource constraints	Research expenses constrained by grant sizes and by grantor restrictions; operations expenses constrained by bureaucracy, uncertain revenues from student services and from tuition and fees.	Hiring constrained by projected product/service sales; operations expenses constrained by bureaucracy, uncertain revenues from product/service sales.

Meanwhile, educational institutions are the site of frequent cyberattacks. In response to one such incident, a U.S. university official estimated that their institution received an average of 20 million attacks a day, describing this as “typical for a research university” [58,80]. Education as a whole suffers an average of 28 days per year of credential stuffing attacks using stolen identifiers for cloud email accounts, vs. a global median of 8 days per year for other industries [67]. In fact, the education sector is the second-most-affected by data breaches after healthcare, at 16.8% in 2015 [81]. Threats facing the education sector include ransomware and stolen credentials attacks with unique characteristics [58,67,81,82]. Verizon reports education now is “the only industry where malware distribution to victims was more common via websites than email,” chalking this up to the many “students on bring-your-own devices connected to shared networks” [67].

All of the above makes the educational sector of particular interest for CSCW and usable security researchers. A fuller picture of users’ attitudes and behaviors regarding their noncompliance with university IT policies will help better understand how to address insider threats, in which users misuse privileges in a way that exposes the network to cyberattack [21,67,68] and which one source estimated cost \$11.45 million in 2020 across all surveyed workplaces [69]. Such a study will also help update how IT and cybersecurity professionals accommodate the logistical and social needs of the human “weakest link” in security, in the spirit of Sasse, Brostoff and Weirich [55].

With the above in mind, we developed the following guiding research question:

RQ: What forms of account sharing are prevalent in a university setting, and what is motivating this sharing among different workers (graduate students, faculty, or nonacademic staff)?

To pursue these answers, we conduct a qualitative interview study. In contrast with a survey, the interview method gives us the chance to ask follow-up questions and get more context around behaviors. We screen and interview 23 employees (staff, students and faculty) who use computing systems for collaborative work at a large U.S. research university. The employees represent a mix of office-bound workers and those with more flexible work arrangements, such as those coming and going from a research lab or who largely worked away from an office even before the pandemic hit. We focus on the practices of non-IT workers, but also interview IT workers to shed more light on the practices they observe among their customers and how they respond. We code the interview transcripts with a combination of top-down and bottom-up themes drawn from initial interview transcripts and literature review, respectively. We then report the key results and situate these within prior academic work.

We find account sharing in this setting to be widespread in our study, as 17 of 23 participants (74%) report sharing accounts either officially via an Enterprise Random Password Manager

(ERPM), via the unofficial but secure method of an individual password manager, or unofficially via ad-hoc methods such as plaintext messages stored in a group chat. Participants report sharing accounts to manage logistics for account-linked services in the cloud, to control 2FA requests, and to share access to platforms such as social media accounts. We find that these workgroups are motivated to share accounts because they perceive it as low-risk and important for saving money, because security is secondary to other priorities such as research, and because trust in colleagues and in authorities are social norms. Of our participants, IT workers and students have the more systematic approaches to account sharing, with the IT practices being more reliably secure.

Our study of account sharing is the first to explicitly compare the perspectives of IT and non-IT employees and to shed light on the practices of student employees vs. full-time employees. Our finding that non-IT participants perceived account sharing as low risk in this setting contradicts findings in three recent prior works where participants cited harms or “unease” with the practice. Further, our study finds that many of our participants see security as secondary to job duties, a theme that is not present in two recent survey studies. We discuss how *paternalistic norms in educational settings* [6,9] and the culture of academic freedom may magnify these motivations at this university, with participants trusting in colleagues and in authorities perhaps more than they should from a security perspective.

We also add qualitative insights specific to the university setting of how people use account sharing as a “shadow security” practice to streamline workflows and to save money, such as to accommodate undergraduate employee turnover and vacations around school breaks. Finally, we offer specific recommendations for security design and for IT messaging that are tied to our findings.

The main contributions of our paper are summarized as follows:

- A comparison of account sharing by employee groups (IT vs non-IT, students vs. full-time).
- A comparison of our findings with those of five prior works on account sharing.
- Insight into how the culture and norms of higher education (specifically, academic freedom and paternalism) influence account sharing in a university workplace.

2 RELATED WORK

2.1 Workplace Collaboration

Early work in CSCW and elsewhere often focused, either explicitly or implicitly, on large-scale enterprises as the site of collaboration. Allen and Cohen [3], Kraut [37,38], Fussell [20] and others documented the significance of physical proximity, finding that researchers co-located on the same floor were more likely to collaborate, and that informal contacts in hallways and elsewhere drove new ideas and helped them to stay aware of each other and to coordinate work. Malone and Crowston [44] looked to coordination theory to help conceptualize and identify how workplace collaboration occurs in practice, noting the interdependencies among activities and actors. Gutwin and Greenberg [22–25] and Carroll et al. [12] examined how notifications and other designs affect workgroups’ awareness of shared activities. Forman [18] found that internet technology, despite being unevenly dispersed, helped to lower the costs of coordination among geographically dispersed workers and, with Zeebroeck [19], of collaborative research.

More recently, researchers have examined workplace collaboration in a wider variety of settings. Colbert et al. [13] noted that "digital fluency" (a level of proficiency with digital technology that allows someone to achieve strategic goals) is a core competency of the modern workforce, and that technology has blurred the lines between work and nonwork domains. Jarrahi [32], Hemsley [29], Lee [40], and others have documented the processes and communications of "digital nomads" — people who are geographically mobile and work remotely, and who have formed online communities to network and share information. Sutherland and Jarrahi note their similarity of digital nomads' knowledge networks and cobbled-together tech and social practices to those of gig workers for ride-sharing apps or odd-job marketplaces [59]. Sawyer [56], Erickson and Jarrahi [17] describe the layers of both technical and social knowledge that modern workers must draw on as "infrastructural competence," a form of bricolage [43] in which people apply any resources at hand in their given work conditions or contexts toward the desired goals.

We consider our research university to be similar in scale to the large enterprises in prior studies of collaboration, and students and faculty as akin to "digital nomads" in their collaborative work. These academic workers are likely to carry laptops from room to room on campus to gain proximity to their collaborators. When not physically near to each other, they use messaging apps such as Slack to maintain mutual awareness and to coordinate work, and they share and store data through cloud-based databases. They frequently work off-campus, either at nearby locations such as coffee shops or at distant conferences and workshops. Many had created home office areas before COVID-19.

2.2 Account Sharing in the Workplace

2.2.1 Logistical Needs. Prior work has often focused on password workarounds in traditional office settings. Adams and Sasse [2] and Inglesant and Sasse [31] found that otherwise security-conscious users often had to work around password policies that were too stringent or inflexible for their needs. Bartsch and Sasse [7] found that enterprise users would use a different password to access job-critical information while waiting for access control changes to be processed. Blythe et al. [11] noted users sharing passwords to get jobs done and to more closely align electronic work processes with those in the physical world. Kaye [33] found that colleagues reported sharing passwords for commercial sites they order from, to avoid having to create individual accounts, and to get access to library materials. And in a 2019 CSCW paper, Song et al. [57] discovered account sharing to be a "norm rather than a simple workaround," with workers motivated by a desire to centralize collective activity and to reduce effort in managing boundaries.

Another concept of note in this context is "shadow security." Kirlappos, Parkin, and Sasse [35] defined this as a type of security, not visible to system administrators, in which employees create workarounds to official policies that retain some protections and enable them to get their jobs done. Kirlappos and Sasse [34,36] found that, while official security is rooted in trust between the administrators and employees, shadow security emerges from the trust relationships among employees themselves. Song et al. [57] alluded to shadow security as an example of workarounds and Ackerman's socio-technical gap [1] — the difference between technical affordances and social requirements that much CSCW research seeks to narrow.

Following Song et al. [57], we defined account sharing to be when more than one person uses the same username and password to access a work resource.

2.2.2 Social Factors. A growing number of researchers are focusing on the everyday social factors in cybersecurity attitudes and behaviors. In regards to account sharing, Weirich et al. [55,64] argued for understanding users' mental models, such as the need to demonstrate trust.

Kaye [33] found that users shared passwords for personal email, Facebook and work accounts with others who they trusted and shared responsibilities with, chiefly spouses, partners and colleagues. Lampinen [39] documented struggles with account sharing for multi-person households that offered to host visitors recruited through a website. Happ et al. [27] found that invoking a reciprocity social norm, through giving a small incentive, increased people's willingness to share passwords. Among studies of romantic partners sharing accounts [41,42,49], Park et al. found that romantic couples' motivations to share accounts were both logistical and emotional, but that some chose to hide accounts to hide other relationships, to avoid conflict, or because they saw the accounts as irrelevant to the relationship. Obada-Obieh et al. [48] found that ending account sharing posed numerous cognitive and psychosocial burdens, such as remembering whom the password had been shared with.

A related issue is that of insider threat, in which system users misuse their privileges in a way that exposes the network to cyberattack [67,68]. Salem et al. [53] defined such threats as malicious and of two types, traitors (legitimate users inside the system who act contrary to security policy and mean to do harm) and masqueraders (outsiders who impersonate or steal the credentials of legitimate users, in order to do harm). However, Greitzer et al. [21] noted the existence of a third and non-malicious type, the unintentional insider threat (UIT) that occurs when legitimate users "accidentally jeopardize security through data leaks or similar errors."

We see all types of insider threat as potentially present inside this academic setting. However, our study is most concerned with UIT arising from problematic occurrences of account sharing within the university's workgroups.

2.2.3 University Setting. Some recent work has explicitly examined the usability of security in a university setting. Colnago et al. [14] documented the attitudes and behaviors surrounding two-factor authentication (2FA) as it was rolled out at a large research university. Regarding account sharing, the authors found that 2FA interfered with the ability of some students to share their financial accounts with parents, because the parents could only use the shared password at a time when the students were available to answer the 2FA push notification. They also found that some students were more concerned about a physical attack, such as someone getting into their computer if they walked away from it, than a remote and opportunistic attack. Around the same time, Weidman and Grossklags [62,63] sought and analyzed the information security policies of 200 top universities. They found that about half did not make their security policies publicly accessible, and that these policies were seldom consistent or shared source materials; moreover, the policies tended to be difficult to read, lacking in emotional language, and worded ambiguously and/or tentatively, such that the takeaways were unclear.

With our study, we seek to add to knowledge of attitudes and behaviors in a university setting and to add insights that are not focused on 2FA use as with Colnago et al. [14] We document end users' awareness, motivation and knowledge of how to comply with their university's information security policies, adding a ground-level perspective to Weidman and Grossklags' review of such policies [63]. Our study contributes what appears to us as the first study of account sharing in a university setting.

3 METHOD

We chose a qualitative interview method to document these issues in depth. We settled on our own large U.S. university as the site of our inquiry because it made logistics easier during COVID-19 restrictions on research, because it gave us easy access to workers and IT staff, and because

we could bring our personal knowledge of the campus culture to the project. In contrast with a survey, the interview method gives us the chance to ask follow-up questions and get more context around behaviors. Our university offered relatively easy access to both office-bound and remote and/or mobile workers to comment on the usability of security policies and procedures, as well as a robust IT workforce that could speak to the security practices (and any resulting problems or threats) that they have observed among the non-expert employees that they support. The university setting also enabled us develop knowledge that applies to other organizations with similarly collaborative and innovation-driven work and employee mix of personal and work accounts and devices.

Our research design, recruitment and consent language, and survey and interview protocols were approved by our Institutional Review Board as an exempt study under Category 2 of the U.S. Revised Common Rule [66]. See the Supplemental Materials for study protocols, such as interview script and pre-screening survey.

3.1 Interview Protocol Development

To help us develop and refine our interview protocol, we conducted six semi-structured pilot interviews with students and staff [A1-6] and used these to iterate the protocol until we had an optimal script to elicit the desired data. Our final interview protocol consists of the following sections: background, types of digital accounts held and shared, devices, workgroup security norms, IT policies, and coronavirus adaptation. Our questions cover account sharing along with general cybersecurity practices. We include general cybersecurity because it gave contextual information, and how the subject regards cybersecurity influenced their sharing practices.

3.2 Participant Recruitment

Our priority in recruiting participants was to locate a wide range of people in job roles that were likely to involve computer-supported collaborative work, and who could, as a group, offer a mix of expert and non-expert perspectives on the tensions between usability and security that drive account sharing and other compromises (Table 2). First, we searched the university’s available staff databases and emailed subjects with the job titles that we hypothesized would be able to contribute data regarding account sharing, due to the types of technology use and work practices that these jobs involve. Second, we posted flyers across the campus and Twitter and did mass email advertising via department mailing lists, to locate more potential participants who were missed or unavailable through direct outreach. Our efforts were complicated by the abrupt closure of the campus in Spring 2020 and the move to completely remote instruction in Summer/Fall 2020. This caused many invited employees to turn down participation due to stresses of juggling work at home with family life and/or shifting to remote instruction.

Table 2: Specific job roles that we looked for in recruiting participants, along with typical technology use or work practices that might lead them to engage in or observe account sharing. Not all participants fell into these specific roles.

Job role on campus	Why seek to recruit
Administrative assistant	In charge of organizing and coordinating schedules, so there is a high chance they will have full or temporary access to team members’ accounts.

	Responsible for onboarding and offboarding, so it is probable for them to have insight on how to add or delete members of a shared account.
Graduate student researcher	Responsible for their undergraduate assistants' temporary and shared accounts.
IT worker	Required to keep up with cybersecurity developments and likely to manage user accounts that may be shared. More likely to have seen examples of strong and poor cybersecurity practices.
Manager of workgroup	More likely to be in contact with their respective IT department to distribute important information or get something approved, making them likely to know relevant IT policies. Inclined to be involved in most projects within their team, as such would need access to any accounts related to those projects.
Marketing and communications staff	Likely to have several social media accounts, many of which can only be shared by distributing one set of login credentials.

3.3 Pre-Interview Screening

We used a pre-interview online survey, made with Google Forms, to record acknowledgement of receiving study information and consent to participate, and to collect data to help us distinguish those people interested in taking part in our study who had the potential to contribute useful insights and who met the criteria of being age 18 or older and employed in some capacity by the university. These people would either use shared accounts, have knowledge of shared accounts, have knowledge of cybersecurity best and worst practices, or have insight about account sharing in the university. The screening questions also identified age, gender, income, job status (full-time/part-time/student/unemployed), workgroup size, and work-related accounts, devices, and policies regarding sharing those accounts and devices. We asked participants to list all their work-related accounts and devices, with no specification of shared accounts, to obtain the least biased results. We include this account and device data in Supplemental Materials.

3.4 Compensation

Interested persons who completed the pre-interview survey received a \$5 Amazon electronic gift card. This amount was set using a \$10/hour rate for surveys and a completion upper bound of 30 minutes, due to the estimated cognitive effort of listing work-related devices, accounts, and policies. Those who were selected and participated in interviews received additional compensation of \$25/hour paid via Amazon electronic gift cards. We based this on U.S. Bureau of Labor Statistics wage data for office and administrative workers [83].

3.5 Interview Data Collection

Of the 36 survey respondents, we invited those for interviews who appeared to have sufficient IT and collaboration responsibilities in their work to provide insights for our research questions. We enrolled 23 participants (10 identifying as female, 12 as male, 1 as nonbinary/gender-nonconforming) for a 60-minute structured 1:1 interview (Table 3). Interviews took place between March and August 2020. A few interviews were conducted on campus, but most were conducted via Zoom due to COVID-19 constraints. We found themes repeated following the 16th interview and determined that we had reached data saturation.

Table 3: Participants in the interview study (n=23), listed by study ID and self-reported characteristics. The majority were non-IT workers (n=15) and full time (n=18).

ID	IT Status	Job Status	Job Role
B1	IT	full time	IT worker
B2	IT	full time	IT worker
B3	IT	full time	Manager of workgroups (IT)
B4	non-IT	full time	Marketing and communications staff
B5	non-IT	student	Graduate student researcher
B6	IT	full time	IT worker
B7	non-IT	full time	Manager of workgroups (marketing and communications)
B8	non-IT	full time	Manager of workgroups (administration)
B9	non-IT	student	Graduate student researcher
B10	non-IT	full time	Marketing and communications staff
B11	non-IT	full time	Other – Library staff
B12	non-IT	full time	Manager of workgroups (administration)
B13	non-IT	full time	Marketing and communications staff
B14	non-IT	full time	Other – Engineering staff
B15	non-IT	student	Graduate student researcher
B16	non-IT	student	Graduate student researcher
B17	non-IT	student	Graduate student researcher
B18	non-IT	full time	Other – Academic advising staff
B19	IT	full time	IT worker
B20	IT	full time	IT worker
B21	IT	full time	IT worker
B22	IT	full time	Manager of workgroups (IT)
B23	non-IT	full time	Manager of workgroups (faculty)

All interviews were recorded and transcribed, with participants being notified in advance through the consent documents of these processes and given the chance to opt out of audio/visual recording and potential third-party transcription. Most transcriptions were done by hand by the authors, with a small portion done through Rev’s transcription service to save time.

3.6 Interview Data Analysis

The authors used a thematic analysis approach [15,47]. One author open-coded the first three interviews to establish themes, and then connected these codes with those identified in literature review, iterating on the list in discussions with the study team. This resulted in codes grouped by background, sharing motivations, accounts, devices, security norms, sharing practices, and socio-technical gap. The code book was imported into Dedoose, where one author coded the transcripts. The team reviewed and discussed these results. We include tables of Dedoose code applications and occurrences in the Supplemental Materials.

4 RESULTS

We found account sharing in this setting to be widespread in our study. Fully 17 of 23 participants (74%) reported sharing accounts officially via an Enterprise Random Password Manager (ERPM), via the unofficial but secure method of an individual password manager, or unofficially via ad-hoc methods such as plaintext messages stored in a group chat. Many shared accounts were for accessing third-party cloud services (frequently, Amazon or Google) or social media (Instagram and Twitter). Crucially, however, no one in our study reported sharing university email linked to their personal identity, which may speak to the success of the onboarding training in educating users about the need to keep this credential confidential.

To answer our guiding research question (Table 4): the forms that account sharing took in our sample were to manage logistics for account-linked services in the cloud, to control 2FA requests, and to share access to platforms such as social media accounts. We found that these workgroups were motivated to share accounts because they perceived it as low-risk and important for saving money, because security was secondary to other priorities such as research, and because trust in colleagues and the institution was a social norm. Of our participants, non-IT workers and/or staff practices around account sharing were less organized, compared with the practices of IT workers and/or students. Sections 4.1-4.3 give details.

Table 4: Summary of themes that emerged from interviews. While we found participants’ reports of account sharing to be widespread for streamlining workflows, no one shared their university email linked to their personal identity. Many participants did not see their sharing of third-party accounts as risky, and non-IT participants were unaware of which IT policies governed this sharing or where to find them.

Theme	Sub-themes	Examples
Forms of account sharing (Section 4.1)	Manage logistics for services	Use one Amazon account for departmental purchasing, create guest accounts for transient undergraduates
	Control 2FA requests	Funnel all requests from remote workers through one coworker, avoid interruptions from requests during teaching or off-hours
	Share access to platforms	Enable social-media takeovers for promotion, cover for vacations or emergencies
Motivations for account sharing (Section 4.2)	Perceived as low risk	Perceived lack of interest to attackers, lack of serious consequences of a breach
	Saving money is a priority	Higher education fiscal policies, collaborators lack funds
	Security secondary to job duties	Machine updates for fixes, research is first priority
	Trust as social norm (trust in peers at work, and trust in authorities)	Trusting an ex-employee not to abuse shared passwords, belief that university IT safeguards systems despite non-IT’s lax security methods
Comparisons by job categories (Section 4.3)	IT vs. non-IT	Procedural use of ERPM by IT, disorganized and infrequent practices

Student vs. full-time	by non-IT, no knowledge of IT policies among non-IT workers Established procedures for sharing resources among students, no established procedures among full-time employees, students’ parents as a weak link in security
-----------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4.1 Forms of Account Sharing

4.1.1 *Manage Logistics for Account-Linked Services, e.g., Cloud Servers.* Some non-IT participants reported sharing an email account because they needed to sign up for a shared service with an email address, such as Amazon.

“We have a shared Amazon email that we use for department purchasing... there’s a specific finance email attached to that ... [But since] I don’t have access to the actual inbox... especially when there’s an order issue, I have to request my coworkers who do have access to the finance inbox to forward me anything... so that I understand what’s going on... [Or] sometimes someone will forget the [Amazon] password and then they’ll request to have the password resent to their email address and... realize... this was sent to an email inbox [they] don’t have access to.” [B18, non-IT, full time]

Participant B5, a PhD student, said they create guest accounts to control access by the undergraduates, who come and go frequently. This is evidence of “shadow security” through temporary access as described in Kirlappos and Sasse [34] emerging from the trust relationships among employees, rather than for cost-sharing as in Bartsch and Sasse [7].

4.1.2 *Control 2FA Requests for Workgroup Accounts.* Several services now require two-factor authentication (2FA) as a security measure in the form of approving a login attempt via email or mobile application or by entering a passcode sent to a device. Some workgroups opt to use a coworker’s device or account to control 2FA requests.

“Especially because we are remote now, sometimes [research assistants] from let’s say, [a different state], need to get into ... the lab Gmail account. And it would pop up on my phone that someone who’s not from [our city] is trying to access [the shared account], and it can get a little confusing.” [B15, non-IT, student]

However, this means that one person oversees the entire workgroup’s 2FA requests, which can happen frequently with several team members logging in from unrecognized devices. It can be difficult to determine the authenticity of the login attempt, and the person in charge of 2FA is likely to be occupied during the 2FA request, leaving the other person waiting. As a result, some reported creating a new email account for the sake of approving 2FA requests.

“When people log in from unrecognized devices, [Amazon] does dual authentication sometimes... if I had that sent to me that would be really obnoxious if I’m teaching classes or out of commission... [and] a student couldn’t run their study. So we have it go to this Google account and the only purpose... is to receive those messages and allow people to login effectively to MTurk.” [B23, non-IT, full time]

4.1.3 *Share Access to Account-Linked Platforms, e.g., Social Media.* Several accounts don’t have an option to have several collaborators on one account, forcing people to share one set of account credentials to collaborate on the same project. A prime example of this is social media accounts,

which Song et al. also found was widely shared as a result [57]. B4 noted with regards to Instagram,

“Students or alumni will often offer to do [Instagram] takeovers, which I think are so fun... but then they have to have our password and that makes me nervous... Sometimes [sharing accounts] happens because it has to, for example Instagram [is] just one page, you have one password.” [B4, non-IT, full time]

B13 said they have shared Instagram and Twitter with supervisors so they can take over accounts during vacations or emergencies. They also created and shared a Squarespace account that can also be accessed with social media credentials. This indicates the potential for cross-site attacks if one account is breached or misused [21,60,67,68].

4.2 Motivations for Account Sharing

4.2.1 Low Risk/Downside Perceived from Shared Account Breach. Many non-IT participants have lax account sharing practices because there would be minimal impact to them and their workspace if the shared account credentials were leaked or if the account was hacked. A primary characteristic of a low-risk account, in some participant’s words, is an account with no financial information linked to it. Another type of low-risk account described by participants were those with no confidential information on them. While not explicitly a result in Song et al. [57], their work indicated similar attitudes in survey respondents. The chief risk in these cases seems to stem from cross-site attacks using reused passwords stolen in breaches.

“I’m a little flippant about some of my work accounts... I don’t deal with highly secure stuff at work... I pay a lot more attention to my personal accounts because there’s financial information associated with them.... [so] how I behave relates to the kind of information that I am working with. ... Some areas of the University... have to be very, very careful, where if someone gets access to my story, so what.” [B7, non-IT, full time]

The outlier was B8, who said their work is classified. This participant reported using several levels of security such as multiple VPN’s, zero account sharing, and strict provisions for teleconferencing platforms.

4.2.2 Account Sharing to Save Money. We also find, as did Blythe et al. [11] and Song et al. [57], that the workers in our study use account sharing to save money. The types of accounts shared due to financial reasons ranged from unimportant accounts with infrequent usage, such as B11’s use of Survey Monkey for their job related to the University library, to accounts that were vital to the participant’s job, such as B16’s use of Qualtrics for graduate research. Two participants described account sharing as a fiscal policy.

“I think historically individuals had their own accounts and there was a decision to make a unified account... because... there’s a cost associated with having the account and given the level of use it made more sense to have one account as opposed to multiple accounts that people were using less. And so when that decision was made we all received an email that said if you want to have access and continue to use SurveyMonkey, add this mailbox. This is where you’re going to be able to find the credential.” [B11, non-IT, full time]

“But I think sometimes [sharing accounts is] a result of the university being frugal, they don’t want everyone to make their own account to save money. So if we only have one login, we don’t have to pay, but if we have one login with five users, we do have to pay.

And so I think there's something maybe to be explored there, where "yeah we're higher ed and we always try to cut costs," but I think that there is a trade-off between security and money." [B4, non-IT, full time]

Graduate students are known particularly to be under pressure to save money and find workarounds for expensive tools. B16 said the situation at this university, which is well-funded and emphasizes behavioral research, is an improvement from a previous university, where graduate students' accounts were not funded even for individual use. Still, they have difficulties because their collaborators' accounts are not funded:

"Most specifically my problem with Qualtrics is that the method I'm using [requires] an upgraded account, so it has extra features, and then I've had my current research assistants ... create their own free accounts. And so long as I share the survey from my upgraded account ... they seem to have had access to ... the features for that specific survey ... they don't have the features if they start their own survey. ... So things get kind of lost in translation there." [B16, non-IT, student]

4.2.3 Security Compliance Is Secondary to Other Priorities. A primary reason why non-IT workers do not keep updated on cybersecurity practices is because it has little to do with their job and what they are getting paid to do. This was noted by both non-IT workers and by IT personnel. It echoes our anecdotal conversations with security professionals and prior published work [2,7,31] that users prioritize getting jobs done over security compliance, but also Colnago et al. [14], in which a university IT department implemented a solution for two-factor authentication that was only required for those on the payroll in order to limit who was inconvenienced.

"The only measure I remember is updating the machines with security fixes as they come. And yeah, we are not very good at it in the sense that I mean, our primary job is not to ... maintain the machine, our primary job's to get the job done." [B5, non-IT, student]

"My job is security ... but I fully recognize the people I'm helping, their job isn't to know everything about security and stay up to date. Their job is to do the research. So how much ... burden do we put on the user to stay abreast of best practices?" [B2, IT, full time]

When asked to give an example of problematic sharing practices, several non-IT participants brought up account sharing or the methods their workgroup takes to share accounts. Participants know account sharing is a security risk, but convenience triumphs over security, a finding also in Song et al. [57]. Several IT participants noted that faculty and others with administrative assistants will use account sharing to delegate responsibilities to these assistants but without much oversight, resulting in at least one embezzlement case.

"[One] individual was sharing their password with an assistant for the purpose of being able to get out of certain types of meetings or fend off vendors or schedule appointments... they didn't have a good way of getting the assistant access to that information other than giving them the account password... One fine day the PIN [Personal Identification Number] for online banking was changed and delivered in email to the account. The administrative assistant obtained the bank account number and an online access PIN and started funneling small amounts of money out of the account. Eventually, the small amounts of money turned into large amounts of money, and that caused a real serious issue." [B21, IT, full time]

4.2.4 Evidence of Trust as a Social Norm (Trust in Colleagues and Trust in Authorities). Separate from convenience, three IT workers brought up users being trusting of their coworkers, environments, and technology as a prime reason for not complying with account security protocols.

Comments from non-IT participants also indicated trust in coworkers who they shared account passwords with; one said they trusted that student employees would not abuse shared lab accounts even after their jobs had ended.

A few non-IT participants also admit to trusting “the system” and the IT departments that support them.

“People in general tend to be very trusting. I can’t even tell you how many people have volunteered to give me their [university] credentials because I work with them, and they like me and they trust me.” [B19, IT, full time]

“I’m just a dummy to think [the University] keeps everything secure for me, but maybe they don’t, I don’t know.” [B7, non-IT, full time]

This trust in authorities is different from demonstrating trust in peers or near-peers [55,64] or evolving “shadow security” within a trusting environment [34–36]. The quotes point to this trust as a function of the paternalistic norms of educational enterprises in general, in which authorities such as IT or “the system” are assumed to provide care, protection and guidance [6,9]. In these cases, non-IT employees are relying on authorities rather than doing the work of the authorities.

4.3 Comparisons of Account Sharing by Job Categories

4.3.1 IT vs. non-IT. Because IT workers have oversight of and help troubleshoot user systems and accounts, all our IT subjects were well versed in the best and worst practices a user could employ for cybersecurity. One IT worker described their workgroup’s rigorous practice of storing shared credentials in Enterprise Random Password Manager (ERPM), an electronic vault that is linked to the university’s general account so that only the accounts that are given permission can log in. Passwords stored in this vault are long and complicated and cannot be memorized.

“A big electronic vault... is where we keep all our passwords encrypted for different systems... that we need in order to... create custom web apps... The electronic vault also keeps a very strict record of who is accessing it and who is checking out a password because when you open [the vault] you don’t see the passwords, you only see the list and you have to check it out. When you check it out [the vault] does a record: who accessed it, when, and why... I have access to whatever I have access, because you can also partition what you need to have access to, and [the vault] is going to record every step of my activity within the vault, based on my initial [university account] login.” [B3, IT, full time]

Most non-IT workers described more-lax password storage and sharing methods, with periodic implementation.

“[The MTurk] password has been shared by email. One of our old grad students... created the login credentials and... she just emails it to anyone who needs it. [For onboarding] basically there’s no system, we just wait until the moment when somebody panics and realizes that they need it and they don’t have access, and then... the person... who created the account... or anyone else who knows it can just share [the password] ... [When

someone leaves the team] nothing happens, password doesn't change." [B16, non-IT, student]

Of the eight IT personnel we interviewed, five (63%) used individual password managers. The other three said they memorized passwords. Of the IT subjects that used password managers, one of them used it as part of their workgroup's password sharing and storage methods.

Of the 15 non-IT personnel, four (27%) used password managers. One non-IT participant used the password manager as part of their workgroup's password sharing and storage measures. In general, participants said the password manager worked well for them. In a few cases, participants expressed irritations with the password manager filling in the wrong username and password.

Only two non-IT personnel (13%) could explicitly remember an IT policy regarding accounts or devices. Most provided their assumptions of what an IT policy would be or stated they did not know any. In fact, some IT personnel themselves could not remember specific policies regarding account or device sharing. One non-IT participant said that IT policies were not made clear enough or accessible enough, echoing Weidman and Grossklags' findings [63].

"I think the understanding is not to share login credentials with people outside the lab unless you have explicit permission to do so... that's just an assumed policy, because it's never come up before. It might be written somewhere in the onboarding manual, but it's so obvious that I just haven't committed it to memory." [B17, non-IT, student]

Several participants expressed having proficient technology knowledge and stated that, therefore, IT advice and policies were unnecessary for them.

4.3.2 Student vs. Full Time. We found that (disregarding IT workers), the student participants had more systematic approaches to account sharing than full-time workers. Two students mentioned using a shared Google Calendar to indicate times they would use a shared resource. As such, students had fewer challenges of using a shared resource at the same time. Most full-time workers, on the other hand, did not have established procedures for using shared resources.

"[The TeamViewer account] uses a schedule [so] no two people can log into the same machine at the same time. ... We have a Google Calendar so people can log in their intended time of use so that there is no conflict." [B9, non-IT, student]

Such systematic approaches may still be *problematic*, as when passwords are shared via printed notes, or with plaintext or cleartext [B2, B22], though at least one student indicated they felt the benefits to the group outweighed the risks.

"Our passwords are plaintexts, stored in a group chat where lots of people can see them... It's problematic, but I'm not concerned about it." [B17, non-IT, student]

Regarding student account sharing, one IT employee also expressed frustration at parents who circumvent IT policies and share students' credentials with third parties such as financial aid consultants. For example,

"There was a small number of students, maybe 20 or so of them, all from the same geographic area. ... They all shared their account names and passwords with their parents. Their parents were working with a small company that assisted with financial aid and looking at loans and grants and things like that. And we discovered in all 20 cases that there were logins coming from the same place, same IP address in the same location to all 20 student accounts, going into the [student] system. That's all supposed to be private data. And there are ways to share the information with your parents, but

what happens when you've got shared passwords is you lose control of them completely... The students knew their parents had the passwords, but they had no control over who the parents were giving the passwords to... Now you've got a problem because you don't know what people are doing with your account... We run into things like that all the time." [B21, IT, full time]

5 DISCUSSION

Our study of account sharing is the first to explicitly compare the perspectives of IT and non-IT employees and to shed light on the practices of student employees vs. full-time employees. We also add qualitative insights from this setting to complement recent survey studies of account sharing within social contexts and extend findings from older studies of account sharing to the age of widespread personal account use. We found, as prior work did, that users in this university community share accounts to streamline workflows [57] and to save money [11,57]. These findings seem to demonstrate similar “shadow security” practices through temporary access as described in Kirlappos and Sasse [34] (to streamline workflows) and in Bartsch and Sasse [7] (to save money). We summarize comparisons of our results with themes in five prior works that deal with account sharing in Section 5.1.

Our participants describe their “shadow security” practices as driven by constraints specific to the university setting, such as to use two-factor authentication that is tied to the mobile phone of a team member away from the lab; to accommodate undergraduate turnover and vacations around school breaks, and to abide by university budget restrictions and policies. Moreover — and reinforcing anecdotal information from security professionals — these users see security as secondary to other priorities. In this case, such a perception may be magnified by the culture of *academic freedom*, which is antithetical to top-down restraints on user behavior. We discuss this in Section 5.2.

Many non-IT participants did not seem aware of the risks to the larger network or to colleagues of an incident such as malware infection or a cross-site attack using stolen credentials. Even if they were aware that it was “problematic,” they were “not concerned about it,” with quotes indicating that some felt that IT or “the system” would take care of security for them. Our finding that non-IT participants perceived account sharing as low risk was in opposition to findings in three recent prior works that participants either feared or had experienced harms from account sharing or were “uneasy” about circumventing the one-user-one-account design for authorization. We see these perceptions as magnified by the *paternalistic norms of educational enterprises*. We discuss this in Section 5.3.

Finally, our comparisons of the perspectives of employees with different job roles shows that students and full-time employees in this study would benefit from using password managers, but also that messaging about practices such as this does not seem to be reaching non-IT participants. We discuss these findings further in Section 5.4.

5.1 Comparisons and Contrasts with Prior Work on Account Sharing

When we compare our results with those in five prior works that deal with account sharing (Table 5), we find that our study's results differ most strongly for three themes: (1) that account sharing is motivated by the view that security is secondary to job duties; (2) that account sharing also is motivated by a perception that it is low risk; and (3) that account sharing differs by job categories (IT vs. non-IT, and student vs. full-time).

Table 5: We summarize the similarities and disconnects with five prior works on account sharing (Song et al. [57], Park et al. [49], Bartsch and Sasse [7], Kaye [33], and Weirich et al. [64]). Our comparisons of account sharing by job categories is the most novel, followed by our findings that university participants see account sharing as low risk, and that they see security as secondary to job duties.

Results	Similar themes in prior work	Disconnects with prior work
(Forms, 4.1) Manage logistics for services	"Centralizing collaboration," "ease of boundary management" for coworkers' sharing in Song et al. "Convenience" and "household maintenance" for couples' sharing in Park et al. "Colleagues" sharing passwords for commercial sites and to avoid creating individual accounts, in Kaye.	Not present explicitly but related to "circumventing authorization measures" in Bartsch and Sasse. Not present explicitly but related to criteria underlying the decision to disclose passwords, in Weirich et al.
Control 2FA requests	"Collaborative password use" involving two-factor authentication in Song et al.	Not present explicitly but related to "convenience" in Park et al. Not present in Bartsch and Sasse, Kaye, or Weirich et al. as a theme.
Shared access to platforms	"Centralizing collaboration," "ease of boundary management" for coworkers' sharing in Song et al. "Convenience" and "household maintenance" for couples' password sharing in Park et al. "Colleagues" sharing passwords for access to library materials, in Kaye. "Have somebody access your account," "necessary for work" as reasons to disclose, in Weirich et al.	Not present explicitly but related to "circumventing authorization measures" in Bartsch and Sasse.
(Motivations, 4.2) Perceived as low risk	"Why conventional fear appeals don't work for most users" - lack of personal impacts, in Weirich et al.	Dissimilar to "lack of activity accountability," "controlling access" with turnover, in Song et al. Dissimilar to "reasons for hiding" accounts - to hide relationships and to avoid conflict - in Park et al. Dissimilar to "circumventing authorization measures" - sharers "generally feel uneasy," in Bartsch and Sasse. Not present explicitly but related to "family" sharing for "things that don't need to be very secure," in Kaye.
Saving money is a priority	"Saving money on shared resources" among coworkers in Song et al.	Not present explicitly but related to "colleagues" sharing passwords for library access, in Kaye. Not present in Park et al., Bartsch and Sasse, or Weirich et al. as a theme.
Security secondary to job duties	"Circumventing authorization measures" due to policies blocking info access, in Bartsch and Sasse.	Not present but related to introduction that security creates overhead for "primary" task, in Weirich et al.

		Not present in Song et al., Park et al., or Kaye as a theme.
Evidence of trust as a social norm (trust in colleagues and trust in authorities)	"Demonstrating trust" in coworkers with whom accounts are shared with, in Song et al. "Trust" and "relationship maintenance" for romantic couples in Park et al. "Colleagues" demonstrating trust within a workplace in Kaye. "It is seen as a sign of trust," with refusal to share seen as an indicator of distrust, in Weirich et al.	Neither trust in colleagues nor trust in authorities present in Bartsch and Sasse as a theme. Trust in authorities not present in Song et al., Park et al., Kaye, or Weirich et al. as a theme.
(Comparisons, 4.3) IT vs. non-IT	None.	Not present in Song et al., Park et al., Bartsch and Sasse, Kaye, or Weirich et al.
Student vs. full-time	None.	Not present in Song et al., Park et al., Bartsch and Sasse, Kaye, or Weirich et al.

5.2 Security as Secondary to Job Duties for University Participants

5.2.1 *Academic Freedom.* That our study explicitly surfaced the theme of security being secondary to job duties reflects that this university workplace has a core mission of *academic freedom*. Such a mission makes it salient in the minds of all participants that academics have a job to do that is not related to security, and that they must be given the space and ability to do it without restraints or responsibilities that would distract them. As one IT participant said: “Their job is to do the research. So how much ... burden do we put on the user to stay abreast of best practices?” The non-IT participants are not likely to even be aware of what is happening behind the scenes to secure the network. Their behavior is not being policed as in other organizations by top-down methods such as social media use policies, internet firewalls, or monitoring for data loss prevention, and they are able to bring their own devices (BYOD) to work, to carry their work devices home, and otherwise to manage their own needs under an IT model that prioritizes customer satisfaction. They can just trust that “IT” or “the system” is taking care of things, as noted above.

This mission of academic freedom may also contribute to blind spots regarding the likelihood of security threats from colleagues. Those engaged in research, particularly, might choose to trust anyone who is doing what Weirich et al. called the “enabling” work, because it is more convenient and less trouble to hand off even sensitive financial data to them without question than to periodically check up on them personally or to set up a system for secondary oversight of how they handle shared accounts. We found that faculty and others with administrative assistants will use account sharing to delegate responsibilities to these assistants but without much oversight.

5.2.2 *Implications for Security Design.* This latter finding, particularly, highlights the ongoing need for designing *task delegation with secured accounts*, with features such as temporary access mechanisms and task-specific restrictions on data access that could limit harms from malicious insiders [57]. We admit, however, that such features will only be as useful as they are used; the example of parents bypassing use of the accounts set up expressly for them is not encouraging.

To address the overall low priority of security compared with academic core mission, we suggest implementing a *cybersecurity buddy* program. Such programs pair a security employee with a workgroup [5,84] to regularly take part in group meetings and to offer a direct line for

guidance and troubleshooting. Anecdotally, we know of such “buddies” setting up office hours or sitting with their assigned workgroup for one or more days per week. This method of supplementing “self-serve” online guidance and the on-demand help desk could help to prevent unintentional insider threat (UIT) [21] resulting from insecure practices, while not imposing more burdens on academic employees. It also could provide an emotional bond with an IT professional that reframes their role to be of a peer rather than an authority figure. This approach seems like the best alternative to implementing a more-controlled, top-down approach to security, which is not likely to be accepted or adopted in this environment due to the culture of academic freedom.

5.3 Account Sharing Seen as Low Risk by University Participants

5.3.1 Social Norms and Threat Modeling. We suspect the discrepancies in findings of risk perception are driven partly by differences in security cultures for the university in our study vs. the organizations in prior studies. Indeed, we found that account sharing here was evidence of trust as a social norm, of two different types: trust in colleagues, and trust in authorities (university participants’ quotes regarding trust in IT or “the system”). The latter type of trust seems an extension of the *paternalistic norms of educational enterprises*, in which authorities are assumed to provide a level of care, protection and guidance akin to that of a parent [6,9]. Only the former type seems similar to themes of “demonstrating trust” in prior works about account sharing, because those data appeared to involve others who were peers or near-peers in a social unit. Peers at work differ from authorities in that their interactions involve social pressures and mutual monitoring in pursuit of common or overlapping productivity goals [45].

However well we think trust speaks to the collaborative environment of this university, we are troubled that many non-IT participants found little risk or downside to ad-hoc account sharing, with only a minority using password managers to facilitate such sharing. Similar to the finding in Weirich et al. [64] of why conventional fear appeals didn’t work for most users, our data implies that employees’ internal threat modeling is overly focused on *personal impacts* to their own financial data or workflows. Correspondingly, their threat modeling is either not aware of or not focused on the impacts to others from the theft of confidential information, or to the entire community from ransomware, or the several other organization-wide risks facing higher education [58,67,81,82]. Unauthorized people can obtain access to shared systems via any worker’s account, perhaps through cross-site attacks on that person’s credentials, or from the installation of malware through an infected website that facilitates theft of credentials [67].

5.3.2 Implication for Security Design. We see a need for *explicit training within academia* and other research-focused organizations about threat modeling for everyday security [61] that boosts people’s awareness of how their accounts can be targeted as the gateway to a shared system. Universities such as this may be able to slot such training in as an additional module during routine security awareness training for incoming students and new full-time employees. We particularly see the value of providing this training as an on-demand online certification that is a prerequisite for research participation, similar to how mandatory training for human subjects research is often handled. This would ensure that people receive the information closer in time to when they are in a position to put it into practice. An on-demand online training also can be taken at the person’s convenience and incorporate quizzes at the end of each section, to test whether the person is retaining the information and to give them incentive to pay attention.

5.4 Lessons from Comparisons of IT vs. non-IT and Student vs. Full-time

5.4.1 Differences in Password Sharing Practices by Job Categories. Our IT participants had the most systematic and least problematic approaches to account sharing, with one workgroup using an Enterprise Random Password Manager (ERPM), an electronic vault that is linked to the university's general account so that only the accounts that are given permission can log in. These findings seem consistent with Pearman et al.'s finding that those who use separately installed tools for password management are motivated by security concerns (as the IT participants in our study were) and that those with the most positive experiences had technical backgrounds (as our IT participants did) [50].

Among non-IT participants, we found that students' approaches to account sharing were more systematic than those of full-time employees, but were still problematic, as when passwords were shared via printed notes, or with plaintext or cleartext. Full-time employees had the most disorganized approaches to account sharing. We theorize that the more systematic practices of students are due to their performing the job of project manager for their collaborative research. Many graduate students described managing accounts in conditions of constant undergraduate turnover and while working around school breaks such as vacations, and they prioritized convenience in their methods.

One solution for students and for full-time employees would be to start using password managers. Given that saving money is a priority, we suspect that many non-IT employees who are aware of group password managers would use them if it did not cost them, their individual departments, or their research labs any money. This suggests a need for *a university-funded password manager solution for workgroups*, akin to the software catalog made available for on-demand download, and consistent with their funding of mandatory software for other security needs, chiefly Virtual Private Network (VPN) access and two-factor authentication (2FA). An IT specialist may also need to be hired to help manage this vendor software and to troubleshoot issues that arise, because users of password managers with non-technical backgrounds may find it difficult to set them up or to put them into full use [50].

5.4.2 Disconnects Between IT Messaging and Non-IT Workgroups. Few non-IT university workers in our study were consciously aware of policies and trainings for account sharing limits and procedures, and many said they are not easily accessible or comprehensible, echoing Weidman and Grossklags' findings [55,56]. The picture that emerges from our interview data (Figure 1) contradicts our expectation that cybersecurity policies and procedures also would impact workgroups from a university IT and from personal level. In fact, many non-IT participants hold higher standards for their personal accounts versus their shared work accounts, since they feel that their work accounts do not contain financial or confidential data that are of interest to attackers. While their individual accounts may be of low interest, the network that the accounts are connected to is of high interest to attackers; a research university such as this controls hundreds of millions of dollars in financial assets and a substantial amount of sensitive data and intellectual property.

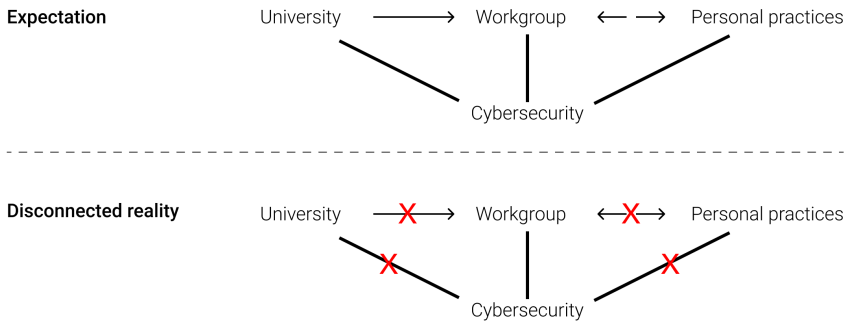


Figure 1: A diagram of (above) the expectation that university messaging on cybersecurity will directly reach workgroups, and those workgroups and personal behaviors will reinforce each other; (below) the reality that emerges from our interview data is of disconnection. Our participants indicated that university policies are unknown to workgroups and strong personal practices do not permeate through the workgroup. The main influencer is what the workgroup as a collective decides upon.

We see the issues as less with the IT policies and procedures themselves, or the personnel skill or knowledge of work practices, than with the difficulties of communicating policies and persuading users to comply with them in such a decentralized work environment as a research university [58]. Prior work as far back as Sasse, Brostoff and Weirich [55] documents that technological advancements and IT recommendations are not enough to convince users to change; persuasive communications and designs are needed [64].

5.4.3 Implications for Security Messaging. We suggest that *user-testing* is as important for communications as for tool or practice designs. We recommend the recent work of Redmiles et al. identifying the criteria of *comprehensibility*, *perceived actionability* and *perceived efficacy* for evaluating advice quality [52]. User evaluation can help find a middle ground between being overly complex and overly patronizing in security messaging — extremes participants noted and that were found by Weidman and Grossklags in their review of IT policies [62,63]. An improvement in security messaging clarity and effectiveness will boost awareness of the security threats that the entire university faces and of the security practices that workgroups can follow to protect against these threats, such as adopting password managers.

Specifically, we recommend the IT department either themselves develop evaluation rubrics set up to measure these criteria, or to make use of existing user research resources to develop them. The rubric and delivery method could be as simple as coding the following directly into a survey interface: *Thank you for (participating in a preview of security training/reviewing a recent security email). On a 1-5 scale: To what degree did you understand the information? To what degree do you think you can put the information into action? How effective do you think this information will be for keeping your data and accounts safe? Please tell us more about why you assigned these ratings ____.*

As to who would evaluate the advice using these rubrics, we think non-IT testers are more likely to be useful evaluators because of not necessarily having specialized knowledge of security. In-house IT personnel should still be on hand as moderators to clarify terms in the messaging or to make on-the-fly adjustments, then to check with the testers that the adjustments answer the testers’ concerns while still being technically accurate.

We recommend recruiting testers who are representative of the different non-IT constituencies in the university community, to capture the diverse awareness and attitudes regarding cybersecurity. These would include undergraduate students and graduate student researchers, research-oriented faculty and teaching-oriented faculty, and nonacademic staff who either have managerial responsibilities or do not. For some security advice, it may also be advisable to craft separate messages for different user segments, such as by identifying specific needs of, say, the computer science department vs. the biology department – both of which use highly advanced technical equipment but of a different nature and to different purposes in teaching and research.

6 LIMITATIONS AND FUTURE WORK

Our interview study yielded data for understanding a wide range of behaviors within a small and nonrandom sample from one university. We are sharing these findings with the university IT team and will discuss the feasibility of our recommendations. Future work can follow up with quantitative surveys informed by our results to determine its representativeness and to help correct for any biases introduced by our use of IT workers' observations of others' activities vs. non-IT workers describing their own activities. Second, while we felt that we reached data saturation with our interview sample, i.e., participants began to simply repeat the same issues and offer no unique insights, we recognize that we may have inadvertently missed some voices that would have contributed to the study. We were able to secure the cooperation of only one professor due to most faculty's need to devote time to revising fall instruction to be remote, and we were not able to recruit any administrative assistants to faculty, both categories of university workers whose experiences should be further studied. Third, we usually were not able to secure the participation of more than one individual from a workgroup. A case study would be better suited for examining how inter-group culture and dynamics might contribute to account sharing and other cybersecurity practices. Fourth, we did not consider the impact of end user license agreements that legally govern how accounts and devices may be used. A survey of governing policies and terms and conditions would help to clarify any issues arising from these legal agreements.

7 CONCLUSIONS

In this paper, we described the results of a qualitative interview study with 23 staff, students, and faculty at a large U.S. university. We compared how different groups of employees (IT vs. non-IT, student vs. full-time) approach account sharing as a "normal and easy" workgroup practice in this setting. We contrasted our results with those in prior works and offered recommendations for security design and for IT messaging. Our findings that account sharing is perceived as low risk and that security is seen as secondary to other priorities offer insights into the gap between technical affordances and social needs in the contexts of education's paternalistic norms and of academic freedom.

ACKNOWLEDGMENTS

This work was sponsored by the U.S. National Science Foundation under grant no. CNS-1704087. Faklaris was also supported by the Center for Informed Democracy and Social Cybersecurity (IDeaS) at Carnegie Mellon University. The authors are grateful for the participation of so many

staff members despite increased workloads due to the pandemic and for the help of their anonymous reviewers in improving this paper for publication.

SUPPLEMENTAL MATERIALS

The subsidiary research questions, recruitment language, additional explanation of interview sections, structured interview protocol, text of sharing examples, pre-screening survey protocol, and lists of Dedoose codes and of accounts and devices reported used by participants are available at https://corifaklaris.com/files/campus_sharing_SM.zip.

REFERENCES

- [1] Mark S. Ackerman. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human-Computer Interact.* 15, 2-3 (September 2000), 179-203. DOI:https://doi.org/10.1207/S15327051HCI1523_5
- [2] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (December 1999), 40-46. DOI:<https://doi.org/10.1145/322796.322806>
- [3] Thomas J. Allen and Stephen I. Cohen. 1969. Information Flow in Research and Development Laboratories. *Adm. Sci. Q.* 14, 1 (1969), 12-19. DOI:<https://doi.org/10.2307/2391357>
- [4] Philip G. Altbach. 2001. Academic freedom: International realities and challenges. *High. Educ.* 41, 1 (March 2001), 205-219. DOI:<https://doi.org/10.1023/A:1026791518365>
- [5] D. Ashenden and D. Lawrence. 2016. Security Dialogues: Building Better Relationships between Security and Business. *IEEE Secur. Priv.* 14, 3 (May 2016), 82-87. DOI:<https://doi.org/10.1109/MSP.2016.57>
- [6] Zeynep Aycan. 2006. Paternalism. In *Indigenous and Cultural Psychology: Understanding People in Context*, Uichol Kim, Kuo-Shu Yang and Kwang-Kuo Hwang (eds.). Springer US, Boston, MA, 445-466. DOI:https://doi.org/10.1007/0-387-28662-4_20
- [7] S. Bartsch and M. A. Sasse. 2012. How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization. UCL Department of Computer Science, London, UK. Retrieved April 2, 2019 from <http://discovery.ucl.ac.uk/1389948/>
- [8] Konstantin Beznosov, Rodrigo Werlinger, and Kirstie Hawkey. 2009. An integrated view of human, organizational, and technological challenges of IT security management. *Inf. Manag. Comput. Secur.* 17, 1 (March 2009), 4-19. DOI:<https://doi.org/10.1108/09685220910944722>
- [9] Dieter Birnbacher. 2015. Paternalism in Education and the Future. In *The Nature of Children’s Well-Being: Theory and Practice*, Alexander Bagattini and Colin Macleod (eds.). Springer Netherlands, Dordrecht, 107-122. DOI:https://doi.org/10.1007/978-94-017-9252-3_7
- [10] David Michael Blomquist. 2020. Comparing Centralized and Decentralized Cybersecurity in State and Local Government. M.S. Utica College, United States — New York. Retrieved May 18, 2021 from <https://www.proquest.com/docview/2407282316/abstract/28997DC7A8DB4BD1PQ/1>
- [11] Jim Blythe, Vijay Kothari, Sean Smith, and Ross Koppel. 2018. Usable Security vs. Workflow Realities. In *Proceedings 2018 Workshop on Usable Security*, Internet Society, San Diego, CA. DOI:<https://doi.org/10.14722/usec.2018.23037>
- [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. *Int. J. Hum.-Comput. Stud.* 58, 5 (May 2003), 605-632. DOI:[https://doi.org/10.1016/S1071-5819\(03\)00024-7](https://doi.org/10.1016/S1071-5819(03)00024-7)
- [13] Amy Colbert, Nick Yee, and Gerard George. 2016. The Digital Workforce and the Workplace of the Future. *Acad. Manage. J.* 59, 3 (May 2016), 731-739. DOI:<https://doi.org/10.5465/amj.2016.4003>
- [14] 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 (CHI ’18)*, ACM, New York, NY, USA, 456:1-456:11. DOI:<https://doi.org/10.1145/3173574.3174030>
- [15] John W. Creswell and Cheryl N. Poth. 2020. *Qualitative Inquiry and Research Design*. SAGE Publications Inc. Retrieved April 22, 2020 from <https://us.sagepub.com/en-us/nam/qualitative-inquiry-and-research-design/book246896>
- [16] Gordon B. Davis. 2002. Anytime/anyplace computing and the future of knowledge work. *Commun. ACM* 45, 12 (December 2002), 67-73. DOI:<https://doi.org/10.1145/585597.585617>
- [17] Ingrid Erickson and Mohammad Hossein Jarrahi. 2016. Infrastructuring and the Challenge of Dynamic Seams in Mobile Knowledge Work. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work*

- & Social Computing (CSCW '16), Association for Computing Machinery, New York, NY, USA, 1323–1336. DOI:<https://doi.org/10.1145/2818048.2820015>
- [18] Chris Forman. 2005. The Corporate Digital Divide: Determinants of Internet Adoption. *Manag. Sci.* 51, 4 (April 2005), 641–654. DOI:<https://doi.org/10.1287/mnsc.1040.0343>
 - [19] Chris Forman and Nicolas van Zeebroeck. 2012. From Wires to Partners: How the Internet Has Fostered R&D Collaborations Within Firms. *Manag. Sci.* 58, 8 (April 2012), 1549–1568. DOI:<https://doi.org/10.1287/mnsc.1110.1505>
 - [20] Susan R. Fussell, Robert E. Kraut, Susan E. Brennan, and Jane Siegel. A Framework for Understanding Effects of Proximity on Collaboration: Implications for Technologies to Support Remote Collaborative Work 1.
 - [21] Frank L. Greitzer, Jeremy R. Strozer, Sholom Cohen, Andrew P. Moore, David Mundie, and Jennifer Cowley. 2014. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In 2014 IEEE Security and Privacy Workshops, 236–250. DOI:<https://doi.org/10.1109/SPW.2014.39>
 - [22] Carl Gutwin and Saul Greenberg. 1996. Workspace awareness for groupware. In Conference companion on Human factors in computing systems common ground - CHI '96, ACM Press, Vancouver, British Columbia, Canada, 208–209. DOI:<https://doi.org/10.1145/257089.257284>
 - [23] Carl Gutwin and Saul Greenberg. 1999. The effects of workspace awareness support on the usability of real-time distributed groupware. *ACM Trans. Comput.-Hum. Interact.* 6, 3 (September 1999), 243–281. DOI:<https://doi.org/10.1145/329693.329696>
 - [24] Carl Gutwin and Saul Greenberg. 2002. A Descriptive Framework of Workspace Awareness for RealTime Groupware. *Comput. Support. Coop. Work* (2002), 411–446.
 - [25] Carl Gutwin and Saul Greenberg. 2004. The importance of awareness for team cognition in distributed collaboration. In Team cognition: Understanding the factors that drive process and performance. American Psychological Association, Washington, DC, US, 177–201. DOI:<https://doi.org/10.1037/10690-009>
 - [26] 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. Association for Computing Machinery, New York, NY, USA, 1–12. Retrieved September 7, 2020 from <https://doi.org/10.1145/3173574.3174144>
 - [27] Christian Happ, André Melzer, and Georges Steffgen. 2016. Trick with treat – Reciprocity increases the willingness to communicate personal data. *Comput. Hum. Behav.* 61, (August 2016), 372–377. DOI:<https://doi.org/10.1016/j.chb.2016.03.026>
 - [28] Kirstie Hawkey, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne, and Konstantin Beznosov. 2008. Human, Organizational, and Technological Factors of IT Security. In CHI '08 Extended Abstracts on Human Factors in Computing Systems (CHI EA '08), ACM, New York, NY, USA, 3639–3644. DOI:<https://doi.org/10.1145/1358628.1358905>
 - [29] Jeff Hemsley, Ingrid Erickson, Mohammad Hossein Jarrahi, and Amir Karami. 2020. Digital nomads, coworking, and other expressions of mobile work on Twitter. *First Monday* (February 2020). DOI:<https://doi.org/10.5210/fm.v25i3.10246>
 - [30] Rich Henders and Bill Opdyke. 2005. Detecting intruders on a campus network: might the threat be coming from within? In Proceedings of the 33rd annual ACM SIGUCCS conference on User services (SIGUCCS '05), Association for Computing Machinery, New York, NY, USA, 113–117. DOI:<https://doi.org/10.1145/1099435.1099461>
 - [31] 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 (CHI '10), Association for Computing Machinery, New York, NY, USA, 383–392. DOI:<https://doi.org/10.1145/1753326.1753384>
 - [32] Mohammad Hossein Jarrahi, Gabriela Philips, Will Sutherland, Steve Sawyer, and Ingrid Erickson. 2019. Personalization of knowledge, personal knowledge ecology, and digital nomadism. *J. Assoc. Inf. Sci. Technol.* 70, 4 (2019), 313–324. DOI:<https://doi.org/10.1002/asi.24134>
 - [33] Joseph “Jofish” Kaye. 2011. Self-reported Password Sharing Strategies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11), ACM, New York, NY, USA, 2619–2622. DOI:<https://doi.org/10.1145/1978942.1979324>
 - [34] I. Kirlappos and M. A. Sasse. 2015. Fixing Security Together: Leveraging trust relationships to improve security in organizations. Proceedings of the NDSS Symposium 2015 2015. Retrieved September 9, 2020 from <http://dx.doi.org/10.14722/usec.2015.23013>
 - [35] Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. 2015. “Shadow Security” As a Tool for the Learning Organization. *SIGCAS Comput Soc* 45, 1 (February 2015), 29–37. DOI:<https://doi.org/10.1145/2738210.2738216>
 - [36] Iacovos Kirlappos and M. Angela Sasse. 2014. What Usable Security Really Means: Trusting and Engaging Users. In Human Aspects of Information Security, Privacy, and Trust (Lecture Notes in Computer Science), Springer International Publishing, Cham, 69–78. DOI:https://doi.org/10.1007/978-3-319-07620-1_7

- [37] Robert E Kraut, Robert S Fish, Robert W Root, and Barbara L Chalfonte. Informal Communication in Organizations: Form, Function, and Technology. 55.
- [38] Robert Kraut, Carmen Egidio, and Jolene Galegher. 1988. Patterns of contact and communication in scientific research collaboration. In Proceedings of the 1988 ACM conference on Computer-supported cooperative work (CSCW '88), Association for Computing Machinery, New York, NY, USA, 1–12. DOI:<https://doi.org/10.1145/62266.62267>
- [39] Airi M I 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 (CSCW '14), Association for Computing Machinery, New York, NY, USA, 499–504. DOI:<https://doi.org/10.1145/2531602.2531665>
- [40] Ahreum Lee, Austin L. Toombs, Ingrid Erickson, David Nemer, Yu-shen Ho, Eunhyung Jo, and Zhuang Guo. 2019. The Social Infrastructure of Co-spaces: Home, Work, and Sociable Places for Digital Nomads. Proc. ACM Hum.-Comput. Interact. 3, CSCW (November 2019), 142:1-142:23. DOI:<https://doi.org/10.1145/3359244>
- [41] Junchao Lin, Jason I. Hong, and Laura Dabbish. 2021. “It’s our mutual responsibility to share”: The Evolution of Account Sharing in Romantic Couples. Proc. ACM Hum.-Comput. Interact. 5, CSCW1 (April 2021), 160:1-160:27. DOI:<https://doi.org/10.1145/3449234>
- [42] Junchao Lin, Irene Yu, Jason Hong, and Laura Dabbish. 2020. “Did You Just Purchase a Butt Head on Amazon?": A Diary Study of Couples’ Everyday Account Sharing. In Conference Companion Publication of the 2020 on Computer Supported Cooperative Work and Social Computing (CSCW '20 Companion), Association for Computing Machinery, New York, NY, USA, 311–315. DOI:<https://doi.org/10.1145/3406865.3418340>
- [43] Panagiotis Louridas. 1999. Design as bricolage: anthropology meets design thinking. Des. Stud. 20, 6 (November 1999), 517–535. DOI:[https://doi.org/10.1016/S0142-694X\(98\)00044-1](https://doi.org/10.1016/S0142-694X(98)00044-1)
- [44] Thomas W Malone and Kevin Crowston. 1990. What is Coordination Theory and How Can It Help Design Codperative Work Systems? (1990), 14.
- [45] Alexandre Mas and Enrico Moretti. 2009. Peers at Work. Am. Econ. Rev. 99, 1 (March 2009), 112–145. DOI:<https://doi.org/10.1257/aer.99.1.112>
- [46] Cary Nelson. 2011. No University Is an Island: Saving Academic Freedom. NYU Press.
- [47] Lorelli S. Nowell, Jill M. Norris, Deborah E. White, and Nancy J. Moules. 2017. Thematic Analysis: Striving to Meet the Trustworthiness Criteria. Int. J. Qual. Methods 16, 1 (December 2017), 1609406917733847. DOI:<https://doi.org/10.1177/1609406917733847>
- [48] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. The Burden of Ending Online Account Sharing. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, Honolulu HI USA, 1–13. DOI:<https://doi.org/10.1145/3313831.3376632>
- [49] 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 Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), USENIX Association Berkeley, CA, Baltimore, Md., USA, 83–102. Retrieved February 26, 2019 from <https://www.usenix.org/conference/soups2018/presentation/park>
- [50] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don’t) use password managers effectively. 319–338. Retrieved July 15, 2021 from <https://www.usenix.org/conference/soups2019/presentation/pearman>
- [51] Jason Putter. 2006. Copyright Infringement v. Academic Freedom on the Internet: Dealing with Infringing Use of Peer-to-Peer Technology on Campus Networks Note and Comment. J. Law Policy 14, 1 (2006), 419–470. Retrieved May 20, 2021 from <https://heinonline.org/HOL/P?h=hein.journals/jlawp14&i=429>
- [52] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. 89–108. Retrieved September 11, 2020 from <https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles>
- [53] Malek Ben Salem, Shlomo Hershkop, and Salvatore J. Stolfo. 2008. A Survey of Insider Attack Detection Research. In Insider Attack and Cyber Security: Beyond the Hacker, Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith and Sara Sinclair (eds.). Springer US, Boston, MA, 69–90. DOI:https://doi.org/10.1007/978-0-387-77322-3_5
- [54] J.H. Saltzer and M.D. Schroeder. 1975. The protection of information in computer systems. Proc. IEEE 63, 9 (September 1975), 1278–1308. DOI:<https://doi.org/10.1109/PROC.1975.9939>
- [55] M. A. Sasse, S. Brostoff, and D. Weirich. 2001. Transforming the ‘Weakest Link’ — a Human/Computer Interaction Approach to Usable and Effective Security. BT Technol. J. 19, 3 (July 2001), 122–131. DOI:<https://doi.org/10.1023/A:1011902718709>
- [56] Steve Sawyer, Ingrid Erickson, and Mohammad Hossein Jarrahi. Infrastructural Competence. In DigitalSTS: A Field Guide for Science and Technology. Princeton University Press, 13. Retrieved from https://digitalsts.net/wp-content/uploads/2019/03/18_Infrastructural-Competence.pdf

- [57] 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 (November 2019), 83:1-83:25. DOI:<https://doi.org/10.1145/3359185>
- [58] Stacy Campbell. Cybersecurity in Higher Education: Problems and Solutions. *Toptal Insights Blog*. Retrieved January 13, 2021 from <https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education>
- [59] Will Sutherland and Mohammad Hossein Jarrahi. 2017. The Gig Economy and Information Infrastructure: The Case of the Digital Nomad Community. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW (December 2017), 97:1-97:24. DOI:<https://doi.org/10.1145/3134732>
- [60] Wali Ahmed Usmani, Diogo Marques, Ivan Beschastnikh, Konstantin Beznosov, Tiago Guerreiro, and Luís Carriço. 2017. Characterizing Social Insider Attacks on Facebook. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*, ACM, New York, NY, USA, 3810-3820. DOI:<https://doi.org/10.1145/3025453.3025901>
- [61] Geoffrey Vaughan. Creating Your Own Personal Threat Model for Everyday Security. Retrieved November 22, 2020 from <https://blog.securityinnovation.com/creating-your-own-personal-threat-model-for-everyday-security>
- [62] Jake Weidman and Jens Grossklags. 2018. What's In Your Policy? An Analysis of the Current State of Information Security Policies in Academic Institutions. *Res. Pap.* (November 2018). Retrieved from https://aisel.aisnet.org/ecis2018_rp/23
- [63] Jake Weidman and Jens Grossklags. 2019. Assessing the current state of information security policies in academic organizations. *Inf. Comput. Secur.* ahead-of-print, ahead-of-print (January 2019). DOI:<https://doi.org/10.1108/ICS-12-2018-0142>
- [64] 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 (NSPW '01)*, Association for Computing Machinery, New York, NY, USA, 137-143. DOI:<https://doi.org/10.1145/508171.508195>
- [65] 2017. 7 Types of Organizational Structures. *Lucidchart*. Retrieved May 18, 2021 from <https://www.lucidchart.com/blog/types-of-organizational-structures>
- [66] 2018. Revised Common Rule Q&As. *HHS.gov*. Retrieved September 14, 2020 from <https://www.hhs.gov/ohrp/education-and-outreach/revised-common-rule/revised-common-rule-q-and-a/index.html>
- [67] 2020. 2020 Data Breach Investigations Report. *Verizon Enterprise*. Retrieved May 28, 2020 from <https://enterprise.verizon.com/resources/reports/dbir/>
- [68] 2020. Ponemon Report 2020 Cost of Insider Threats: Global. *ObserveIT*. Retrieved May 29, 2020 from <https://www.observeit.com/2020costofinsiderthreat/>
- [69] BYOD vs. CYOD: What's Right For Your Business? Retrieved December 7, 2017 from <http://www.symantec.com/connect/blogs/byod-vs-cyod-whats-right-for-your-business>
- [70] Employees and Instructional Staff - How many people are employed by postsecondary institutions? Retrieved January 14, 2021 from <https://nces.ed.gov/ipeds/TrendGenerator/app/answer/5/30>
- [71] The Condition of Education - Postsecondary Education - Postsecondary Students - Undergraduate Enrollment - Indicator May (2020). Retrieved January 14, 2021 from https://nces.ed.gov/programs/coe/indicator_cha.asp
- [72] 1940 Statement of Principles on Academic Freedom and Tenure | AAUP. Retrieved May 20, 2021 from <https://www.aup.org/report/1940-statement-principles-academic-freedom-and-tenure>
- [73] Complexity and Information Systems: The Emergent Domain - Yasmin Merali, 2006. Retrieved May 20, 2021 from <https://journals.sagepub.com/doi/abs/10.1057/palgrave.jit.2000081>
- [74] Understanding UCSB's Federated IT Model. *UC Santa Barbara Information Technology*. Retrieved July 14, 2021 from <https://www.it.ucsb.edu/understanding-ucsbs-federated-it-model>
- [75] The Advantages and Disadvantages of Decentralized Information Security. Retrieved July 14, 2021 from <https://www.klogixsecurity.com/blog/the-advantages-and-disadvantages-of-decentralized-information-security>
- [76] What Is Sensitive Data? Sensitive Personal Data Definition & Types. | *Cipherpoint*. Retrieved July 15, 2021 from <https://cipherpoint.com/blog/what-is-sensitive-data/>
- [77] Compensation Force: 2016 Turnover Rates by Industry. Retrieved July 14, 2021 from <https://www.compensationforce.com/2017/04/2016-turnover-rates-by-industry.html>
- [78] A-26. Persons at work in nonagricultural industries by class of worker and usual full- or part-time status. Retrieved May 18, 2021 from <https://www.bls.gov/web/empisit/cpseea26.htm>
- [79] Table A-8. Employed persons by class of worker and part-time status. Retrieved July 14, 2021 from <https://www.bls.gov/news.release/empisit.t08.htm>
- [80] Penn State's College of Engineering Hit by Cyberattack - *The New York Times*. Retrieved July 14, 2021 from https://bits.blogs.nytimes.com/2015/05/15/penn-states-college-of-engineering-hit-by-cyberattack/?_r=0

- [81] Follow the Data: Dissecting Data Breaches and Debunking the Myths - Security News - Trend Micro USA. Retrieved November 24, 2020 from <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data>
- [82] The Surge of Cyber Threats: What Higher Education Needs to Know. SecureWorks. Retrieved January 13, 2021 from <https://www.secureworks.com/resources/rp-the-surge-of-cyber-threats-what-higher-education-needs-to-know>
- [83] Average hourly wages for selected occupational groups and areas for full-time workers by selected work levels, civilian workers. Retrieved September 9, 2020 from <https://www.bls.gov/mwe/avg-hourly-wages-for-fulltime-workers-by-work-levels.htm>
- [84] Why you need a security buddy (and how to find one) | CSO Online. Retrieved November 22, 2020 from <https://www.csoonline.com/article/2133470/why-you-need-a-security-buddy--and-how-to-find-one-.html>

Received January 2021; revised July 2021; accepted November 2021.