"I'm Surprised So Much Is Connected"

Hammann, Sven ; Crabb, Michael; Radomirović, Saša; Sasse, Ralf; Basin, David

Published in:
CHI 2022 - Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems

DOI:
10.1145/3491102.3502125

Publication date:
2022

Document Version
Peer reviewed version

"I'm Surprised So Much Is Connected"

A Study on Users' Online Accounts

Sven Hammann
ETH Zurich
Zurich, Switzerland
sven.hammann.90@gmail.com

Michael Crabb
University of Dundee
Dundee, Scotland
m.z.crabb@dundee.ac.uk

Saša Radomirović
Heriot-Watt University
Edinburgh, Scotland
sasa.radomirovic@hw.ac.uk

Ralf Sasse
ETH Zurich
Zurich, Switzerland
ralf.sasse@inf.ethz.ch

David Basin
ETH Zurich
Zurich, Switzerland
basin@inf.ethz.ch

ABSTRACT

A person's online security setup is tied to the security of their individual accounts. Some accounts are particularly critical as they provide access to other online services. For example, an email account can be used for external account recovery or to assist with single-sign-on. The connections between accounts are specific to each user's setup and create unique security problems that are difficult to remedy by following generic security advice. In this paper, we develop a method to gather and analyze users' online accounts systematically. We demonstrate this in a user study with 20 participants and obtain detailed insights on how users' personal setup choices and behaviors affect their overall account security. We discuss concrete usability and privacy concerns that prevented our participants from improving their account security. Based on our findings, we provide recommendations for service providers and security experts to increase the adoption of security best practices.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → **User studies**.

KEYWORDS

Account Graph, security setup, user interviews.

ACM Reference Format:
Sven Hammann, Michael Crabb, Saša Radomirović, Ralf Sasse, and David Basin. 2022. *"I'm Surprised So Much Is Connected"*: A Study on Users' Online Accounts. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3491102.3502125

1 INTRODUCTION

When accessing services online, people regularly use a large number of internet-based accounts and other access mechanisms such as smart phones and further access tokens. The resultant connections in a user's account setup are complex. For example, an account recovery email may create a link between an email account and a social network site; two-factor authentication can create a link between a physical device and a work email account. Users are also commonly logged into accounts on their personal devices, making additional connections between digital accounts and physical objects. Moreover, user accounts are connected to other aspects of the physical world; for example, people can write passwords down, and the real-world location of devices and their closeness to other objects can be used to unlock accounts. The connections between accounts, devices, and credentials are different for each user's account setup. Understanding the security risks that arise from these connections is a highly personal task that requires analyzing the setup of a given person individually.

The high degree of personalization of users' account setups also means that security advice must be personalized: Different advice is relevant for different users. For example, enabling two-factor authentication for a Google account would be important and recommended for a user who uses the associated GMail as her primary email account or makes extensive use of *Google Sign-In*, but it is much less relevant for a user who only uses her Google account to watch YouTube videos. These differences are disregarded when studying users' willingness to follow security advice.

Account access graphs [22] are a formalism to model the connections in a user's account setup and analyze their security implications. In this work, we employ this formalism to obtain a novel methodology for performing qualitative user studies and apply it in a user study with twenty participants. We obtain their account access graphs and leverage them to interview each participant about their account setup in semi-structured interviews. We use these interviews to understand the challenges that our participants face in creating secure setups, and the impact that decision made within one area of their security ecosystem have on their setup as a whole.

We expand upon previous work examining users' account setups in the following ways. Firstly, we develop a methodology to systematically elicit a user's account setup and subsequently provide actionable security advice. Secondly, we discover and highlight the structural features of users' account setups, e.g., account access patterns, cycles, and compartmentalization. These observations allow us to show that participants themselves are unaware of their account setup and underestimate the importance of critical accounts and devices. Previous work in this area focused on broad security challenges that are applied to large population groups. To our knowledge, this is the first study that attempts to understand the

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

granularity of online account security on an individual user level. This leads us to advocate further research into personalized security advice and investigations into automating this process to support more extensive studies.

2 RELATED WORK AND RESEARCH QUESTIONS

Studies related to ours generally fall into one of two categories. The first kind more broadly aims to understand users' motivations to follow security best practices, their security-related mental models, and their risk awareness. The second kind more narrowly focuses on specific aspects of account security, such as passwords and two-factor authentication.

This work bridges a gap between the motivation to follow security practices, and specific methods used to improve account security. We are not aware of previous studies focusing specifically on the connections between users' accounts and devices, such as those arising from recovery methods.

2.1 Account Security Methods

2.1.1 Passwords. The topic of user passwords and related risks and countermeasures has been studied extensively. For a literature review on the topic up to 2014, we refer the reader to Taneski et al. [39]. We next discuss some work that closely relates to the aspects we focused on in our study, in particular on password reuse.

Gaw and Felten [19] studied users' password management strategies, with a focus on password reuse. They found that participants used unique passwords for more important accounts and discussed users' perceived threat models, but with respect to attackers trying to compromise passwords specifically.

Das et al. [12] investigated partial password reuse and how an attacker can leverage a known password for guessing other passwords of the same user. They describe in detail the transformation rules users employ to generate new passwords from existing ones, a topic that is also mentioned by our participants.

Pearman et al. [29] conducted a large-scale *in situ* study of users' password behaviors, obtaining detailed data about password reuse. They did not find a correlation between using password managers and password reuse, suggesting that their participants did not use randomly generated passwords. They found correlations between website categories and password reuse, with decreased reuse on government websites and increased reuse on shopping and job search websites. They conjectured that the difference was due to perceived account importance, and noted that it was *somewhat surprising considering that shopping website passwords may protect sensitive credit card data and that job- and work-related sites may contain [...] payroll and employment information. [29]* This is another indicator that users may not accurately assess the importance of their accounts.

Lyastani et al. [26] explicitly studied the relationship between using password managers and password reuse in a study with both qualitative and quantitative elements. They pose the question why users of password managers still reuse passwords. Our study provides some insight into this: some participants felt uncomfortable only using randomized passwords, and others used password managers as a digital notebook on a separate device rather than having their passwords synchronized across all their devices.

Pearman et al. [30] conducted an interview study on the use of password managers, finding that users reuse passwords, despite using a browser-based password storage feature.

2.1.2 Two-factor authentication. We next discuss work related to the usability of two-factor authentication and how its adoption could be increased, a topic on which we provide recommendations.

Redmiles et al. [32] conducted a study on messages asking users to enable two-factor authentication. Their participants both critiqued existing messages and designed new ones. They preferred simple and clear messages, including information about the required time investment for setup. Participants also mentioned they were more likely to use two-factor authentication for just their more important accounts.

Albayram et al. [4] investigated how video tutorials on two-factor authentication can increase users' willingness to adopt the technology. Interestingly, one of their participants gave the following reason for not enabling two-factor authentication after watching the video: *"I do not want [...] sites I use to have my cell phone number, as I don't feel like I can trust them with it." [4]* That is, their participant was unaware of solutions that do not require the phone number, similar to our participants. The work by Redmiles et al. [33] mentioned previously also shows that privacy concerns can be a barrier for the adoption of two-factor authentication.

De Cristofaro et al. [14] performed a comparative usability study of three two-factor authentication solutions: codes generated by security tokens, received via email or SMS, or generated by smartphone apps. Their participants were already two-factor authentication users. They found that two-factor authentication was overall perceived as usable by their participants. Their participants mentioned troubles with SMS-based authentication when abroad, similar to what we observed.

2.2 Motivation to Follow Security Advice

Despite long-running efforts by the security community, challenges still exist in getting people to follow security advice. It is common for users to see themselves as low-risk targets for their accounts to be compromised [13]. Additionally, users struggle to see the benefits of following security advice when it is given at a broad, general level [16]. Participation in generic security training does not necessarily lead to the adoption of more secure behavior [8]. Questions still exist on how to engage users best to see the need to adopt reasonable security practices.

A common reason for not adopting security advice is the perceived cost/benefit ratio that following advice creates. Taking proactive security actions is seen as having too high a cost by users [42], with generic advice regularly ignored due to the unknown individual cost-benefit [15]. Users' decision to focus on usability over security is not unfounded, with the simple act of unlocking a phone taking, on average 2.9% of all time that a person may interact with a smartphone [23]. For users of security tools such as password managers, convenience rather than improved security is seen as the primary reason for continued usage [15]. Methods to identify the

explicit challenges within a single security setup may be a potential method to alter individual users' perceived cost-benefit.

The generic one-size-fits all approach to providing security advice is not conducive to producing change [34]. Providing guidance at a very broad level has even created challenges in consensus within the security community as to the best advice that users can follow to stay safe online [35]. Giving security advice at this level also creates challenges due to factors such as an individuals socioeconomic status and how this may alter their willingness to follow advice [31].

2.3 Security on an Individual User Level

Security advice is commonly offered at a broad level for large population groups. This creates challenges in an individual's willingness to follow the advice [8] and does not account for the wide range of factors that individuals will consider [31]. Presenting users with the ability to see real benefits from changing their own practice may have potential [16] as an alternative method of providing security advice. For security advice to be given at a per-person granularity, understanding the security of a given person must first be achieved. We use this to motivate our initial research question in this work where we ask ***RQ1:*** **What does a typical user account setup look like and what potential weaknesses exist in it?**

Security advice is generally given within compartmentalized areas (like password strength or two-factor authentication) [3, 36]. Whilst this type of advice is beneficial and can provide guidance for people on how to improve the general security of their account setups, it is incapable of protecting against security threats that exist due to the *connections between elements* in a particular account setup. As current security advice may be unable to provide guidance at this level of granularity, we ask ***RQ2:*** **What awareness do users have of the weaknesses in their account setups and what are the individual barriers to solving these challenges?**

3 ACCOUNT ACCESS GRAPHS

The theoretical foundation of this work is the model of *Account Access Graphs* by Hammann et al. [22]. This formalism models users' account setups as graphs, with vertices representing accounts, devices, and credentials. Edges (with color) model dependencies for granting account access, where the same edge color is used for conjunction (all necessary) and different edge colors are used for disjunction (alternative), see Example 1 for more details. Account access graphs also enable the automated security analysis of users' account setups. We present the definitions this work relies on.

Definition 1 ([22]). *An* account access graph *is a directed graph* $G = (V_G, E_G, C_G)$*, where* V_G *are vertices,* C_G *are colors, and* $E_G \subseteq V_G \times V_G \times C_G$ *are directed colored edges.*

Example 1. *Figure 1 shows an account access graph that features an email account, a phone, text messaging (SMS), a password, a fingerprint device locking mechanism, and a PIN code with correspondingly named vertices. The vertices are shaded in different colors depending on their type. Accounts are blue, credentials are red, devices are yellow, and biometrics are green. We distinguish between access to the locked phone and access to the unlocked phone. We decorate a locked device vertex with a rectangular outline and diagonal chords in each corner. The graph indicates that there are two ways to access the services of the unlocked phone, indicated by two different edge colors. To access the unlocked phone, the locked phone is necessary and either a fingerprint (*Finger*) or a PIN code (*PIN Phone*).*

*The locked phone provides access to incoming text messages (*SMS*), that is, the phone's lock screen displays the full text message. The dashed edge from* SMS *to* Mail *indicates that access to the email account can be recovered with a text message. Standard access to the email account is obtained with a password (*pwd*).*

The unlocked phone provides access to an open session of the email account. We denote this by Mail basic *since some security-critical features, such as changing the password, may be unavailable from an open session. Accessing such features explicitly requires entering credentials to access the* Mail *vertex.*

A black edge indicates a single credential or an account that is sufficient for access. For example, access to Mail basic *can be obtained* either *through* Mail or *through* Phone.

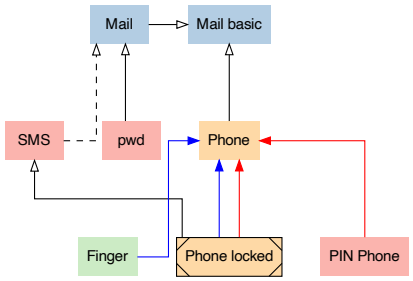

Figure 1: An access graph with four different types of vertices. A black edge denotes a sufficient condition for access. For other edge colors, the same colors denote conjunction (all necessary for access) and different colors denote disjunction (alternative). Dashed edges indicate recovery methods.

We use account access graphs to model the account setups of our participants, and as a basis for automated analysis. To this end, we have developed a front-end tool (available at [2]) in preparation for this study to complement the existing back-end [22]. This tool facilitates entering users' account setup data to then visualize and automatically analyze the resulting account access graphs.

We have performed both manual and automated analysis to discover security weaknesses in our participants' account access graphs. The manual analysis focused on standard notions, such as password reuse [12, 19, 26, 29] and lack of two-factor authentication [4, 14, 32]. The automated analysis focused on the discovery of *backdoors*, a notion introduced in [22], which we explain next.

An account has a backdoor if it can be accessed more easily by means of a *recovery* method than by *primary* authentication methods. A backdoor arises in scenarios where an attacker with specific capabilities can exploit one or more recovery methods, but no primary authentication methods, to compromise an account. Thus backdoors are defined relative to an attacker model. This notion is transitive; for example, a backdoor for a single sign-on account also constitutes a backdoor for the connected accounts.

We only give an informal definition of backdoors. The formal definition in [22] makes use of additional concepts such as *scoring schemes*, which are not directly relevant to this work.

Definition 2. *An account has a* backdoor with respect to an attacker *A if A can compromise the account using at least one recovery method, either directly or provided by a connected account, but not using only primary authentication methods.*

We next explain the different attacker models that we used to define backdoors. Our automated analysis marks an account vertex if at least one such backdoor is present.

- A *text message attacker* can compromise text messages directly (without access to the phone). A text message attacker models, for example, an attacker who can perform SIM swap attacks [5, 25]. In such an attack, the attacker obtains access to the victim's phone number by impersonating the victim to their mobile phone provider, thereby obtaining a new SIM card for the victim's phone number.
- A *password attacker* can compromise passwords. A backdoor with respect to a password attacker could for example mean that two-factor authentication can be circumvented using only a password.
- A *weak-secrets attacker* can compromise credentials labeled as *weak secrets*. In our model, weak secrets include in particular security questions as well as patterns that must be drawn to unlock a device (e.g., a smartphone).
- A *device-theft attacker* can compromise (steal) physical devices, but cannot compromise any secrets. A backdoor with respect to a device-theft attacker means that an attacker who has obtained one of the user's devices can access the account without knowing its password, e.g., through password reset using an open email account session on a phone without a locking mechanism.

An account's backdoor thus means that its *recovery method(s)*, or those of connected accounts, makes the account vulnerable to a *wider range* of attack vectors than its primary authentication method.

Example 2. *In Figure 1, the* Mail *account requires a password as its primary authentication method and a text message (*SMS*) as its recovery method. Thus, it has a backdoor with respect to a text message attacker. Moreover, the* SMS *recovery method is also a backdoor with respect to a device-theft attacker, as text messages are accessible from the locked phone. Thus, the account is vulnerable to SIM swap attacks and theft in addition to the primary authentication method's vulnerability to password compromise.*

4 METHODOLOGY

We carried out semi-structured interview sessions to understand typical user account setups and their users' potential weaknesses. We also used these interviews to discover users' awareness of these weaknesses and the barriers that exist in solving associated challenges. Our interviews were structured into two stages. First we obtained information about account graph information. Afterwards, we conducted a discussion with participants that was structured around an analysis of their account graph information.

This work was approved by our institution's Institutional Review Board (IRB). Participants' names were never included in their data. At the start of each study session, participants were informed of their rights and responsibilities, including that they may withdraw from the study at any time. Participants were asked whether they agree to an audio recording of the second part of the interview to assist in data analysis. They were informed that the recording stays on an off-line device, and that the transcript is stored off-line on the interviewer's computer as well as on the secured server of our research institute. 18 out of 20 participants agreed to the recording. At the interview's end, participants were given a supermarket voucher (roughly $20 USD) as a thank you for taking part.

4.1 Obtaining Account Graph Information

In the first part of the interview, participants were asked about their accounts and connections. This part of the interview relied on self-reported information only that participants reported. Account and connection information was entered into the tool described in Section 3. We now describe the approach in more detail.

Device Information: Participants were asked which devices they use to connect to the internet, such as computers, smartphones, or tablets. For each device the participant uses, we asked how that device can be unlocked, i.e., whether it requires a password, a PIN, or biometrics such as a fingerprint or FaceID.

Global Account Management: Participants were then asked about their password management strategy. Participants were asked if they used a password manager, or what alternative methods they used to store their passwords, e.g., in a browser. Participants were then asked about their email accounts, since these are often connected to many other accounts. Participants were not required to disclose which service providers they use for email, but were asked to give each email account an identifier during the interview.

Individual Account Access: For each account, participants were asked whether login requires a password and/or a second factor. Participants were also asked how they could reset the password if they forgot it. If the participant was unsure how the recovery process for one of their accounts works, the interviewer asked them if they can obtain this information by looking at their account settings on their own devices. The interviewer did not tell participants that they had to attempt password resets, but they could do so voluntarily. In some cases, the participant provided additional information in the second interview part, leading to slight changes to their account access graph.

Primary Access Accounts: Participants were asked if they have accounts that they use to log in to other services, explicitly asking if they use their Google or Facebook accounts for this purpose. Participants that did use this technique were asked about the accounts that they use to assist with single sign-on. The Google account was already covered in the email section if the participant used GMail. If they mentioned GMail in this part but did not explicitly mention that one of their used email accounts is the GMail account, the interviewer added this information. This ensured that the Google account was modelled properly as both a GMail account and an account used for single sign-on. Participants who were uncertain about whether they used single sign-on were asked to look this up by checking connected applications on their accounts.

Persistent Account Logins: For all accounts with at least one outgoing connection, the interviewer also asked whether the participant is usually logged in, i.e., has an open session on any of their devices. In some cases, the participants noted that this varies over time and the device was modelled to be connected to the account even if the participant was not always logged in.

'Leaf Vertices' Accounts: Participants were then asked about additional accounts that are more likely to be leaf vertices in the graph, i.e., that are not used to recover or log in to another account. For these kinds of accounts, the goal was *not* to gather information about every single account the participant owns. This would not have been feasible within a reasonable time frame. We aimed to estimate which of the participant's accounts and devices provide access to many other accounts, but the exact numbers were not important. To this end, participants were asked whether they have accounts in categories such as social media, web shops, and banking.

Account Setup Behavior: When participants had multiple email addresses, they were asked which one of them they are most likely to register as a recovery method when they set up a new account at a service. When the participant mentioned that they use single sign-on, the interviewer asked them for example services for which they use this option. They were also asked which option they are most likely to use, e.g., if a service provider offered single sign-on with different providers or offered both single sign-on and the option of registering a separate account. The interviewer then included generic vertices in the account access graph, such as a Default vertex to capture the participant's behavior they described as most likely when registering at a new service. Note that this default behavior was entirely self-reported, unlike the connections between participants' actual accounts. Thus, we did not overly emphasize default vertices in our results.

Additional Information: Before finishing the first part, the interviewer asked the participant whether there was an account they considered important, which they had not talked about, or whether they can think of more accounts with unusual setups for authentication or recovery. If the participant mentioned any accounts at this stage, the interviewer also asked about how these accounts can be accessed and recovered. Between the first and second parts of the interview, the interviewer ran an automated analysis on the obtained account access graph to detect backdoors with respect to the specific attacker models described in Section 3.

4.2 Discussion on Account Graph Analysis

In the second part of the interview, participants were asked to reflect on the overall analysis of their account access graph. This part was audio recorded for each participant that explicitly agreed to this. The goal in this part of the study was to discuss individual weaknesses in each participant's setup. Even though no rules were formalized in our process for the second part, the interviewer informally followed the guidelines described next.

Explanation of the Account Graph: The interview's second part started with the interviewer showing individual participants a visualization of their account access graph. Any accounts with *backdoors* that were discovered by the automated analysis were marked red and highlighted to participants. While these provided an entry point into the discussion, the interviewer also discussed potential weaknesses that were noticed by manually inspecting the graph. The interviewer had the required expertise on account security to perform such a manual analysis. The combined automated and manual analysis aimed to discover a wide range of potential security weaknesses. However, it was not designed to exhaustively discover every single weakness.

Password Protected Accounts: The interviewer pointed out when an account with many outgoing edges, such as an email account, was only protected with a password. In these cases, the interviewer asked whether this password was used for other accounts. If the participant did reuse the password for such an account, the interviewer steered the conversation to the risk arising from password reuse. In particular, the interviewer asked whether the participant has seen *haveibeenpwned.com*, or a similar website or tool that can be used to determine whether a password has been exposed in a password database breach. Participants were also asked if they were aware that password reuse had an associated risk. If participants were aware, they were asked why they follow this practice, and they were advised to use unique passwords at least for their accounts with many outgoing edges. If participants were unaware of the risks, the risk of credential stuffing attacks using password database breaches was explained.

Two Factor Authentication: When a connected account belonged to a service that offers two-factor authentication, participants were asked if they were aware of this option and why they chose to use or not use this service. The purpose of this discussion was to understand the participant's barriers in using two-factor authentication given the additional context of an important account. If the participant was unaware of two-factor authentication options, the interviewer explained them, in particular text messages and authenticator apps such as Google Authenticator. If the participant was aware of the option using text messages, but not authenticator apps, the interviewer explained the differences.

Additional Security Topics: Each participant's account graph is unique and we intentionally did not constrain the topics covered in the interview's second part. This allowed the interviewer to touch on the different unique circumstances encountered in each participant's account access graph. In particular, some participants made interesting comments in the first part with respect to their thought process on how they have setup their accounts. The interviewer followed up on these comments in the second part to discuss them in the recorded part of the interview.

4.3 Interview Analysis Method

Our results were analyzed using open coding [41]. Coder training and briefing sessions were carried out to familiarize coders with the methodology that was used. We detail this below.

(1) **Generating Interview Transcripts:** Audio recordings from the second stage of our interviews were transcribed by the lead author. As we had a mixture of sessions that were conducted in English and German, transcripts were created in the language the interviews were created in. Final quotes are all shown in English with translations made by the interviewer. Original language transcripts are provided [2] in line with existing style guidelines [20].

(2) **Developing the Initial Code Book:** A subset of 5 transcripts were coded by the first author and 3 different transcripts were coded by the second author. This was carried out as a first round of coding. Both authors used an inductive coding technique [40] with themes then generated as emergent categories [21]. The two authors then carried out a virtual discussion regarding their different approaches to coding, noting similarities in the generated codes and themes and discussed differences. Discussion continued until agreement was achieved, and a preliminary code book was created consisting of 34 codes and 9 themes. A second phase of discussion was carried out to refine our codebook further, creating a final book of 20 codes and 4 themes. As part of this discussion we found that code saturation had been reached after analyzing a subset of transcripts, and creating a codebook with our whole corpus was not needed [17].
(3) **Corpus Analysis:** The entire corpus was then analyzed within a second round of coding. This included transcripts that had been analyzed in the previous stage. All authors took part in this activity and first became familiar with the initial code book. Each transcript was analyzed, separately, by two authors. Individual transcript coding was compared between authors and agreement sought for individual codes. Any disagreements between coders were discussed in detail until a resolution could be found. All authors then discussed analysis with the aim of condensing the overall number of codes in areas where similarity was present [38].

As the generation of codes was part of the overall evaluation process and not the end product, inter-coder reliability metrics are not recommended in this situation [27]. However, to aid in analysis quality we used multiple coders [10, 21]. 2 participants declined to be recorded for Part 2, but were included in analysis for Part 1.

5 RESULTS

5.1 Participants

Participants were recruited to take part in this work through an online research platform[1] and through posters that were placed within two university campuses. Our recruitment method stated that we were carrying out a study on security risks in user accounts and that participants should:

- Actively use internet services, such as web shops, social media, and online banking
- Be fluent in English or German
- Own at least one portable device with internet connection, such as a laptop or smartphone (which should be brought to the study)

Twenty participants took part in the study. 12 were female and 8 were male. Their ages ranged from 19 to 40, with a mean of 25.5. 4 reported to study computer science. 12 reported to be interested in information security topics, but not professionally or in their studies, and 2 reported interest in IT topics, but not security specifically. One participant reported no particular interest in IT topics, and another participant reported to be between the last two options (no particular interest, and interest in IT, but not security specifically). Interviews lasted between 60-90 minutes and were carried out in February and March 2020 after obtaining approval of our IRB. Each interview was conducted by the same interviewer to ensure consistency in the process. We refer to our participants as P1, ..., P20. Note that P3 and P19 did not agree to the recording and thus were not quoted.

[1] https://marktplatz.uzhalumni.ch/

5.2 Account Graph Details

We give here a brief overview over all participants' account graph features. All interviewed participants use smartphones in addition to a laptop or desktop computer. Table 1 summarizes the data we discuss and is elaborated on in the following.

The *Vertices* column indicates the number of vertices in each participant's account access graph that were elicited during the interview. As discussed in Section 6.1, the actual number of vertices is likely to be higher, since the interview did not aim for completeness.

Several participants had cycles in their account access graph. The *Elements in Cycles* column shows the size of each cycle. 0 indicates that there is no cycle, while more than one number indicates that there is more than one cycle. As seen in Table 1, five participants have one cycle in their account setup and two participants have two cycles. Five of these cycles provide sufficient access to each vertex in the cycle, that is, each vertex in the cycle is sufficient to access the next vertex without any other authentication factors. In three of these cases, this is the consequence of two email providers being used as recovery email addresses for each other. In the other two cases, a password manager provides access to a cloud service, which in turn provides access to the password manager.

The *Components* column indicates the number of connected components in the graph. Many participants' graphs consist of a single connected component. The reasons for several components may be the lack of detail provided or an intentional separation.

A few participants do not use any kind of password manager, indicated by *no* in the Password Manager column. However, many make only *partial* use of it, as they still access some accounts with passwords not stored in the password manager. Our definition of password managers is broad and includes any tool that allows the user to store and retrieve passwords without memorizing them.

The *Open Sessions* column indicates the number of accounts that one of the participant's devices has an open session with. However, we only elicited this information for accounts that could potentially be used to access other accounts, such as email accounts or accounts used for single sign-on.

As can be seen from the next three columns in Table 1, all but two participants use text messages (SMS) as a second authentication factor or a recovery factor for at least one account. Almost half of the participants allow SMS previews to be displayed on the lock screens. For participants whose account access graphs did not contain SMS at all, SMS-related entries are indicated by "n/a".

The last column, *Central Vertices*, indicates the types of vertices that are most critical for providing access to other vertices in a participant's graph as determined by a centrality score[2]. More precisely, they show the types of vertices with a score that is within

[2] The *centrality score* of a vertex is its share of all the possible ways to provide access to vertices in the access graph. See Section 6.1 for a formal definition and examples.

Table 1: Summary of participants' account graph features. *: the cycles are overlapping.

Participant	Vertices	Elements in Cycles	Components	Use of Password Manager	Open Sessions	Lockscreen prevents SMS Preview	SMS for 2FA	SMS for recovery	Central Vertices
1	50	4	1	yes	2	yes	no	yes	Computer
2	45	0	2	no	4	no	no	yes	Phone
3	32	0	4	no	1	no	yes	yes	Password
4	44	0	1	partial	4	n/a	n/a	n/a	Computer
5	33	0	3	no	1	no	yes	no	Password, Old Password
6	58	3;5	1	yes	5	n/a	n/a	n/a	Password for PwdManager
7	59	0	1	yes	4	yes	yes	yes	Computer
8	37	4	1	yes	3	no	no	yes	Phone
9	43	6	1	partial	4	yes	yes	yes	Password
10	53	0	3	yes	4	yes	yes	yes	Computer
11	41	0	1	partial	4	yes	no	yes	Computer
12	49	0	2	partial	6	yes	yes	yes	Phone
13	30	0	2	yes	4	no	yes	no	Phone, PwdManager
14	42	0	3	yes	3	yes	yes	yes	Phone
15	44	0	1	yes	3	yes	yes	yes	Phone
16	35	2	2	partial	2	no	yes	yes	Computer
17	33	0	2	partial	2	no	yes	no	Phone
18	35	0	1	partial	2	no	no	yes	Finger, Tablet, Computer
19	52	4; 6*	1	yes	6	yes	no	yes	All Devices, Account
20	51	3	1	partial	2	yes	yes	yes	Old Password

5% of the graph's highest score. Note that we do not distinguish between locked and unlocked devices in this column.

For fourteen out of the twenty setups, a device (phone, laptop, tablet, or computer) is the most central vertex, the phone being the most central in eight of these. In three of the remaining six setups, the central password vertex is a source vertex that provides access to an email or service provider vertex with many outgoing edges. In P18's setup, shown in Figure 3 on page 10, the central vertex is a fingerprint that provides access to all of the participant's devices (phone, tablet, and laptop). P6, shown in Figure 2 on page 10, P9, and P19 each have a central vertex that provides access to a large cycle (of 5 or 6 vertices). Moreover, P19's setup is special in that there are two overlapping cycles. In P19's setup , all highly ranked vertices directly or indirectly provide access to at least one of the two cycles. All vertices in the cycles also received comparatively high centrality scores.

5.3 Interview Results

Our final code book contained 20 codes across 4 themes. We present our themes below. We provide quotes that provide a representative overview of participants' perspectives on account security.

5.3.1 Account graph structure. Participants discussed items that relate to the structure of their online security setup.

Separation and Sharing: 5 participants mentioned that they consciously separate their accounts, e.g., into work-related and not work-related. This affected on which devices they were logged in to those accounts, commonly with the goal of reducing spam and notification load. P8 justified this approach, stating that *"if something is important, I would connect it to [one email address], something that just needs an email to log in, I would connect to [another email address]."* P6 followed a similar approach, having an email account for things that were described as *"important,"* a second email account for things that were *"related to university,"* and a final account for things that were *"more creative, I would say, social media and stuff."*

Routines and Preferences: 5 participants discussed their routine relating to their accounts and which devices they are logged in on. For example, P11 described that *"usually I just use my laptop and my phone [...] using the university's computer, which is not that common, [...] I always make sure that I'm logged out,"* and P15 mentioned being *"always logged in"* to their email account. P10 explained that they used their tablet only rarely and thus consciously were not logged in on many accounts there, concluding *"my configuration follows my routine, basically."*

Digital Management: 5 participants discussed digital security management techniques and tools they currently employ. P7 used two-factor authentication *"if I'm logging in to a new device, not on my devices, but if I'm logging in on a separate computer."* P15 applied a mixed password generation strategy; their password for their email account *"was suggested by the Phone, by the App [...] it's really long, and diverse, so I will not remember it,"* while their password for a social media account was *"not randomly generated, but different from the other ones."*

Non-digital Management: 12 participants discussed non-digital security management techniques. P4 described that they were selectively *"writing [passwords] down with pen and pencil, usually I know where I need to log in to, like if I go traveling,"* while P1 *"didn't want to write them down [GER]."* With respect to choosing passwords, P20 explained that they have *"a very complex basis, and then a specific one [for each website] [GER]."* P10 similarly described that they had a *"structure [...] numerical and alphabetical, and in the end, maybe just a slight change of the symbol or something [...] I wouldn't say like, algorithm."*

5.3.2 Awareness and understanding of security problems and solutions. Participants discussed different aspects relating to their awareness of security problems, such as password reuse risk, and solutions like two-factor authentication and password managers.

Lockout Risks: 6 participants expressed concerns related to the risk of locking themselves out of their devices or accounts. With respect to usernames and passwords, P5 mentioned *"that one could forget the email address, that could be more likely [GER]*, while P11 described that they do not use randomly generated passwords because they *"wouldn't feel comfortable in not having this power over my accounts."* Two-factor authentication leading to lockout over a longer time was discussed by P8, who had moved between countries, *"I lost my [...] country's phone number, and when I entered my email [...] I need to have the SMS, and I couldn't receive the SMS, so I was locked out for 30 days on both my emails,"* and P20 noted: *"I had an authenticator for a while, for example for [a gaming platform], and it took two months until I could enter again because I changed my mobile phone [...] [GER]."*

Security Risks: 10 participants commented on security risks arising from password reuse, weak passwords, or security questions. P4 was aware that reused passwords were *"not so secure,"* and P7 used one password *"for almost everything else,"* wanting *"something different"* for their most important email account. Participants understood that some security questions could be brute-forced, with P2 describing that one such question related to *"the color of the first car that we owned [...] but of course it's another thing that there's not a lot of colors."* P11 thought that it was *"so easy to find such information"* related to security questions.

Security Mechanisms: 9 participants mentioned whether they are aware of some security mechanism or tool. P12 discussed the *"option to use, for example, TOTP,"* referring to the time-based one-time passwords used by many two-factor authentication apps. P4 described physical security keys as *"devices that can just like plug in to your computer."*

Influence of Others: 5 participants explained that other people, most commonly family members, made them aware of a particular security problem or solution. P2 discussed a reliance on their sister for information: *"she's a computer scientist, she also helped me with how to [set up two-factor authentication]."* P15 followed a similar process regarding passwords, saying that they are *"[...] randomly generated, because my brother told me to [...] it was something because it was good to do, but also he insisted on this thing."*

Security Mental Models: 10 participants expressed security beliefs or ways they think about their account security. Participants had different opinions about the security of certain practices. P11 described that *"thought that [writing down a password] wouldn't be that safe, anyway, so it's always better to just trust your mind and the security system each platform has,"* while P12 believed that *"the physical copy is actually the safest of my password managers."*

Risk Implications of Connections: 13 participants discussed how they believe the connections between their accounts and devices are associated with risks. P8 expressed surprise at their access graph, saying that *"everything is almost accessible if they have your phone."* P15 expanded on this, saying that *"that there are so many connections"* but they were *"not aware of the risks."* P16 thought of one of their email accounts *"as more of a risk, since there one has the app on the mobile phone where one does not have to log in [GER]."* P17 identified that *"when the mobile phone is turned on, and the person knows how the pattern works, then this is a big security risk for me [GER]."*

Misconceptions and Inefficient Use of Tools: 8 participants made comments that showed a misconception they had about a security concept, or described using a tool in an inefficient or ineffective manner. P4 *"thought you would have to use [two-factor authentication] every time [you log in], or something, and then it's annoying."* P6 had trouble shifting their own viewpoint to an attacker's, asking about two-factor authentication, *"if I'm logged in all the time, what's really the difference?"*

Noticing or Recovering from an Account Breach: 3 participants described how they would notice or recover from an account breach. P7 noted that *"these days"* if someone else were to login to their bank account, *"the bank will instantly notify you, and your money is kind of protected."* P16 described a similar belief, saying that they have *"never had the problem that someone debited or transferred money off my account, and I would notice it within a day, so that's not such a great risk [GER]."*

5.3.3 Improving Account Security. Participants discussed various aspects relating to their overall account security and the challenges associated with improving this.

Account Importance: 8 participants discussed the importance that they attach to specific accounts. P7 described that they *"wouldn't really worry about somebody logging in to"* their account at a hotel booking service, but *"what I would worry about is my bank."* P8 described reusing passwords for *"the stuff that I don't care about,"* while *"the things that are important to me have different passwords."* P18 similarly said *"I do reuse passwords, I just make sure that the [accounts] that I know are connected to a lot of different things are unique."* Participants explained how much they would care about account breaches, such as P7, *"I of course don't want anyone to access my email, but I feel like, worse comes to worst, somebody does actually [access it], there's nothing that I'm afraid they might read, I don't have anything like that,"* or P14, who *"wouldn't really care"* if their shopping or social media accounts got hacked.

Usability and convenience: 13 participants mentioned either concrete usability concerns or more generic convenience concerns with respect to security mechanisms. In particular, participants discussed usability of two-factor authentication with P2 describing that *"if you change your number, maybe you have to go back and change your number in the account."* P4 described that they have been *"moving a lot, so I got different phone numbers from different countries [...] if I'm in a different country I won't receive the [two-factor authentication] message."* P14 reused a single password for all their accounts despite having heard of the risks, explaining *"one just doesn't get around to doing it, because convenience wins out [GER]."*

Accepting defaults: 5 participants expressed that they prefer default configurations, independent of whether they are secure or not. P7 described that they *"feel like all of my accounts are protected [...] there's nothing that's gone wrong with any of my accounts, so it's just an extra hassle if I have to do [set up 2FA],"* but later also mentioned an account for which two-factor authentication was *"by default set up,"* for which they did not disable it. Similarly, P20 explained *"if an app or platform asks me upon installation if I want*

to use two factors, I usually say yes, but if it does not ask explicitly, I don't [GER]."

5.3.4 Attacker models. Participants mentioned both concrete *attack personas*, which we labeled with the first two codes that follow, and more general *attack vectors*, labeled with latter codes.

Service and application providers: 9 participants discussed concerns in sharing their personal data with a cloud service provider or web applications. P6 described that they *"don't really like to have all my data in the cloud,"* and switched from one browser to another because *"you can control more"* with respect to data sharing. In contrast, P17 had *"no concerns with respect to this"* when using social login, explaining *"it's good that I can pay with my data [...] then I get ads that actually interest me [GER]."*

Friends and family: 4 participants mentioned how they feel about friends or family members potentially accessing their accounts. P1 mentioned they don't like to write down recovery codes: *"If they're just lying around, then family members can access them, too [...] I don't have the feeling that they're trying to hack me, but the thought that the codes are just lying around makes me uncomfortable. [GER]."* P7 shared some accounts with colleagues, but made sure to use a different password for their personal account: *"I'm definite they wouldn't misuse it, but I don't want to take any chance."*

Physical device security: 6 participants discussed whether they were concerned about others physically accessing their devices. P11 mentioned not saving too many passwords on their laptop because they *"don't want to let things too easy for someone else"*. P1 had an additional security PIN required for accessing apps on their phone because *"it is unlocked on occasion, and then one cannot simply enter [the apps] [GER]."*

Targeted attacks: 5 participants mentioned reasons why they would consider a targeted attack on their accounts likely or unlikely. P5 wondered if they *"might be too paranoid,"* because they were *"not some politician who has important things [GER]."* P9 said that they *"don't have that much wealth to make people want to hack my account."* P20 had been targeted before: *"the reason why my [social media account] got hacked, I won tickets [for an event] and that was announced on the radio [GER]."*

Attacker capabilities: 5 participants expressed beliefs on what an attacker might be able to do. P2 doubted the effectiveness of even a strong password against a dedicated attacker, *"I just increased the degree of difficulty [...] for the password, but of course if there is a hacker he could find other ways to go into that."* P2 also thought about what an attacker might know when answering security questions: *"I didn't write the name of my best friend, I just wrote the name of the first friend I ever had, which also not a lot of people know."* P11 expressed doubts about the effectiveness of their computer's PIN: *"if someone steals [my computer], this person probably knows how to access things, I don't know how safe this PIN really is."*

6 DISCUSSION

6.1 User Account Structure

RQ1: What does a typical user account setup look like and what potential weaknesses exist in it?

We modeled our participants' account setups as account access graphs as a basis for answering this research question. The 20 account access graphs elicited by interviewing our participants have between 30 and 59 vertices. However, as we were more interested in structural features rather than exact numbers, we did not require participants to mention all of their accounts.

Figures 2 and 3 are simplified versions of P6's and P18's account access graphs, whose structural features we describe next. These graphs combine most of the structural features we have observed in the elicited graphs. The semantics of different kinds of vertex and edge styles is as in Example 1.

Account Setup Structure. The first structural features we examined were how our participants' accounts are generally accessed and recovered. In particular, we examined what common *patterns* exist, where many different accounts are accessed in a similar manner.

We consider two kinds of patterns: Those reported by our participants directly, and those we identified in the graphs ourselves. An example of the first kind of pattern is the blue 3D-box-shaped vertex Default in Figure 3. The participant did not name specific accounts for this vertex, but indicated the use of accounts that only had a password but no recovery method. Similarly, using the Mail account for single sign-on was identified by the participant as a pattern for Serious accounts.

We identified patterns ourselves by considering different vertex types: passwords, email accounts, other accounts, and devices. We consider three or more credentials or accounts to have the same access pattern if they are of equal type and are accessed by equal (non-empty) combinations of types of credentials. A typical such pattern is the use of some kind of password manager to store passwords. This pattern can be seen in the red 3D-box-shaped pwds vertices in Figures 2 and 3. We bundle accounts, devices, and any other credentials that are accessible with the same pattern as follows. We contract the vertices that have the same access pattern and indicate in the resulting 3D-box-shaped vertex the number of contracted vertices. Figure 2 shows 3 different access patterns that we identified for P6. P6 reported on 16 passwords, contracted into the vertex pwds, all of which are accessed using a password manager. P6 mentioned 7 different accounts, each of which is accessed with a password and recoverable using an email account, and 3 email accounts that are accessed and recoverable in the same way.

Central vertices. The next structural feature we analyzed was which vertices are the most central in our participants' graphs in terms of providing access to other vertices. The centrality scoring method we used is based on access sets defined in [22]. An access set for a vertex v is a minimal set of vertices that is sufficient to (transitively) obtain access to v.

Example 3. *In Figure 3, one (of many) access sets for the vertex Social 2 is the singleton set {Social 1}, because access to Social 1 suffices to gain access to Social 1 basic, whence access is obtained to Social 2. Every access set for the Bank vertex in the same graph includes the vertex PIN B, since access to Bank is only possible through the phone and with that PIN. As there is no vertex providing access to PIN B, this vertex must occur in every access set for Bank. One such access set is the set of vertices {PIN B, Finger, Phone locked}.*

We define the *centrality score* of a vertex by counting the number of times a vertex occurs in the access set of another vertex. The

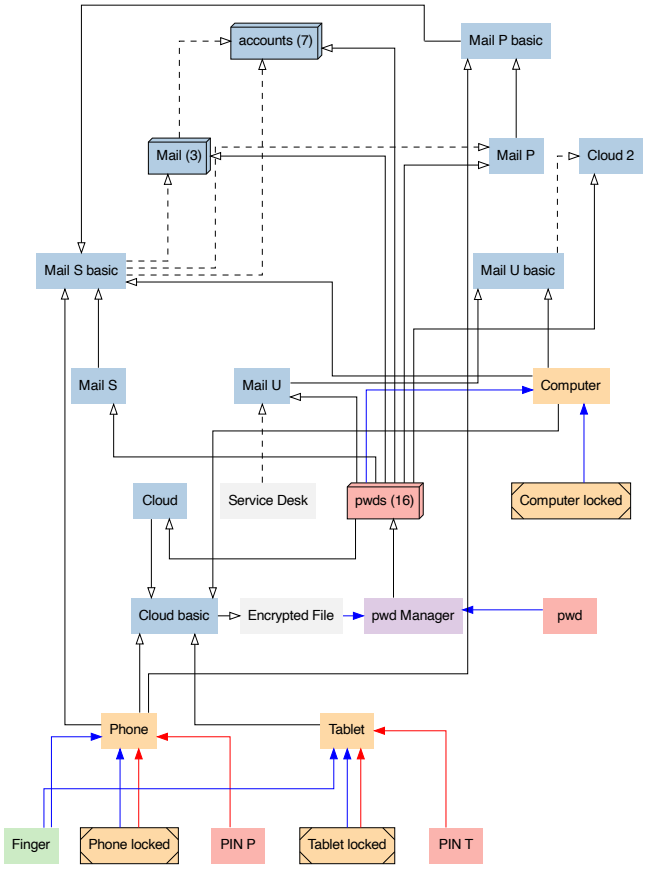

Figure 2: Simplified Access Graph of participant P6. Some accounts have been removed. 3D-box-shaped vertices contract vertices with the same access pattern.

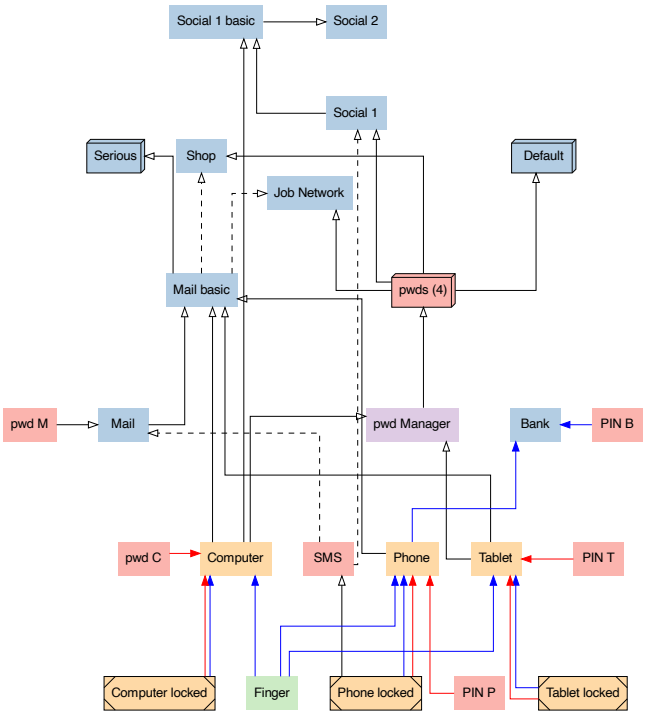

Figure 3: Simplified Access Graph of participant P18. Some accounts have been removed. 3D-box-shaped vertices are contractions of vertices with the same access pattern.

vertex's occurrence is weighted inversely proportional to the number of vertices occurring in the access set. Thus every vertex has a score of at least 1 as it constitutes its own access set.

Example 4. *The centrality score of vertex Social 1 in Figure 3 is 3, since it occurs in the access set for itself, for Social 1 basic, and for Social 2. The score for PIN B is* $2\frac{1}{6}$*, because it provides access to itself (1), and occurs in three access sets for Bank, once with Phone, weighted 1/2, and twice with two other vertices, each weighted 1/3.*

Vertices that receive high centrality scores indicate critical parts of the user's setup. If these vertices were protected poorly, this would result in a weakness in the setup.

Passwords are used as an authentication factor for most accounts, so **password managers or vertices providing access to them are central vertices.** For example, in Figure 2, the vertex pwd has the highest centrality score. This is a decryption password for an Encrypted File stored in the Cloud storage. We discuss the reason for pwd's high score in the context of cycles below.

While we found that **most participants stored some of their passwords in a password manager, several participants did not store all of them.** For example, in P18's setup (Figure 3), the password pwd M for the Mail account is not stored in the pwdManager. This is consistent with previous studies showing that users do not necessarily take full advantage of password managers [26, 30].

In many participants' setups, a device is the most central vertex under our centrality scores. Our participants' devices commonly provide access to many accounts by means of open sessions or through passwords saved on the device. Most participants' devices were protected with a locking mechanism. The most common locking mechanisms were PINs and fingerprints. The Finger vertex of the graph in Figure 3 is the most central vertex because it unlocks any of the three devices. The next most central vertices in this graph are Computer and Tablet. In comparison, the Phone is not as central because it does not provide access to the password manager.

Cycles. A structural feature closely related to central vertices are cycles. Cycles occur, for example, when multiple accounts can be used directly or indirectly to recover each other. Vertices that are contained in a cycle or provide access into a cycle can have comparatively high centrality scores, particularly when access to one of the cycle's elements provides access to the whole cycle. The reason is that such a cycle with several incoming and outgoing links acts like a hub connecting all incoming paths to all outgoing paths. If the cycle includes or provides access to a critical vertex such as a password manager, then all vertices that are part of the cycle or provide access into the cycle obtain high centrality scores. The accounts that are part of such a cycle must therefore all be

well-protected. Cycles can, primarily, reveal the weakest points for all accounts within an account ecosystem. They also have the potential to reveal multiple connected accounts as a result of users consciously separating work and personal life [6, 9].

Several participants' account access graphs contained cycles, for example due to email accounts recovering each other or passwords saved in cloud storage. P6's graph in Figure 2 contains two cycles: Mail S basic → Mail P → Mail P basic → Mail S basic, and pwd Manager → pwds → Cloud → Cloud Basic → Encrypted File → pwd Manager. All vertices in these cycles are sufficient to provide access to the next vertex in the cycle, except for the access provided to the password manager, which, in addition to Encrypted File, requires pwd. This explains why pwd, the password for the password manager, has by far the highest centrality score: Most of the access paths to passwords and accounts in this graph are contingent on pwd. In contrast, Encrypted File, unlike the password, is accessible through multiple devices that have open sessions to the Cloud storage, denoted by Cloud basic.

Compartmentalization. Several participants' account graphs consist of multiple connected components. In the second part of the interview, we learned that **some participants consciously separated their accounts with the goal of reducing spam and notification load**, e.g., into work-related and other. In particular, they were logged in to different accounts on different devices, and connected accounts to different email accounts. For example, P8 stated that *"if something is important, I would connect it to [one email address]; something that just needs an email to log in, I would connect to [another email address]."* P6 followed a similar process, describing their use of the three email accounts shown in Figure 2 as follows: One email account is for things that were described as *"important,"* a second email account for things that were *"related to university,"* and a final account for things that were *"more creative, I would say, social media and stuff."* P10 explained that they used their tablet only rarely and thus consciously was not logged in on many accounts there, concluding *"my configuration follows my routine."*

While multiple connected components in an account access graph indicate compartmentalization or missing information, we can see that they are insufficient to detect the quoted participants' compartmentalization strategies. This is because their strategies do not aim for a clean separation across their account setup, but only for a separation of particular items meeting their individual criteria.

Weaknesses in users' account setups. We briefly outline the most common weaknesses that we discovered by automatically and manually analyzing our participants' account access graphs, as described in Sections 4.1 and 4.2. Our automated analysis discovered backdoors with respect to text message attackers, as many participants used text-message-based account recovery, leaving them vulnerable to SIM Swap attacks [5, 25]. Furthermore, it discovered backdoors with respect to device-theft attackers, as some participants who used such a recovery method either did not have a locking mechanism on their phone at all, or enabled text message preview on the locked phone. That is, anyone with physical access to the phone would have direct access to the recovery codes sent to the phone. We did not find backdoors with respect to weak secret attackers; while security questions were used as recovery methods in a few participants' setups, they often served only as a single step in a multi-step recovery process.

Our manual analysis showed that participants did not use two-factor authentication unless it was mandatory, as is the case for many online banking accounts. While using only a single authentication factor might not directly constitute a critical weakness, it does become critical when this factor is a reused or weak password. Therefore, using two-factor authentication is security advice commonly given by experts [7, 16, 24]. In particular, some participants had email accounts that were central to their setup, and with email providers that offered two-factor authentication, but the participants had not enabled it.

During the interviews, we also found that our participants fully or partially reused passwords, exposing themselves to risk from password database breaches [28]. Some participants even reused their password for accounts that provide access to many other accounts, such as their email accounts. Note that we elicited password reuse in the second part of the interview only, so the graphs do not differentiate between unique and reused passwords.

6.2 Awareness of Account Weaknesses

RQ2: What awareness do users have of the weaknesses in their account setups and what are the individual barriers to solving these challenges?

Our analysis of participants' individual account graphs illustrates features (e.g., compartmentalization and cycles) that are unique within an individual's own setup. However, our participant's account seutps also share common features. In this section we provide security recommendations that are based on our analysis of participants' account setups and our subsequent discussions with participants on the challenges they face in managing the security of their setups.

Recommendation 1: Users may have an incomplete view of their online account setup and personalized security advice could be used to overcome this. All participants had an incomplete view of their account setup. Thus, they underestimated the importance of their central accounts, such as their email accounts and their devices. When asked what they found surprising about the study, P15 replied *"I'm surprised that so much is connected, especially to my [email account] [GER],"* with P8 adding that *"everything is almost accessible if they have your phone physically."* This misunderstanding leads to participants insufficiently securing important accounts, as we show in the next section.

It has been pointed out before that not every piece of security advice is equally relevant to every user, e.g., by Reeder et al. [36]. Our results suggest that we should go even further, and that *security experts* should seek out opportunities for *personalized security counseling* rather than trying to craft advice for the general population. While our process of interviewing users may not scale to a larger population, we believe that large parts of our process could be automated, especially if the main goal is to give advice rather than to obtain interview data. Such automated tools could then provide personal security advice at scale.

During our interview sessions, we were able to give participants security advice that was tailored to their specific setup and experience, unlike generic advice that is commonly given. In particular,

we could single out accounts that were central to each participant's setup, providing access to many other accounts. When these accounts were just weakly protected, such as with a reused or weak password, we gave advice on how to better protect this account specifically. Future work should focus on the ability to automate the collection of the data required to determine a user's online account setup, and in methods to then give users advice based on any weaknesses that are determined.

Note that tools currently offered by service providers, such as Google Security Checkup [1], only consider the part of a user's account setup that is connected to that service provider. Therefore, such tools cannot give personalized security advice that considers the user's entire setup. Bespoke tools that offer broader security advice based on a user's full account infrastructure (e.g., [11]) should be prioritized as a future method to improve the security guidance that is given to end users.

Recommendation 2: Users struggle to see the links created between accounts due to password reuse and work is required to highlight password database breaches to assist in mitigating this problem. Multiple participants reused passwords only for accounts they considered relatively unimportant. P8 described reusing passwords for *"the stuff that I don't care about,"* while *"the things that are important to me have different passwords."* P18 similarly said *"I do reuse passwords, I just make sure that the [accounts] that I know are connected to a lot of different things are unique."* It has been observed that password reuse is acceptable for lower-valued accounts [18, 37]. However, our participants' perceptions of their accounts' importance were not always accurate.

Some participants consciously favored convenience over security, considering their accounts insufficiently important to warrant extra effort. P14 reused a single password for all their accounts despite having heard of the risk, explaining *"one just doesn't get around to doing it [setting up unique passwords], because convenience wins out."* Participants that *reused passwords* were not too concerned with attacks because they believed that they had to be *targeted*, thinking of an attacker as someone who had decided in advance to hack them specifically. Our participants were also largely unaware of password database breaches [28]. The interviewer showed *haveibeenpwned.com* to participants who reused passwords, and the vast majority were unaware of the site or similar tools. This suggests that *security experts* should increase *awareness of password database breaches* and resulting password reuse risk. They should also *explain the untargeted nature of credential stuffing attacks*, emphasizing that an attacker does not have to consciously pick a user as their target.

Recommendation 3: Users are likely to adopt default security advice as long as it does not greatly impact their current mental model of accessing systems. Enabling methods such as 2FA on accounts likely to be central within users' account graphs would be beneficial. In our study, participants mentioned concrete obstacles, in particular with respect to adopting two-factor authentication. Multiple participants had usability or privacy concerns about using their phone number for text-message-based two-factor authentication. P8, who had moved between countries, described resulting usability problems as follows: *"I lost my [...] country's phone number, and when I entered my email [...] I need to have the SMS, and I couldn't receive the SMS, so I was locked out for 30 days on both my emails."*

Participants expressed a higher willingness to keep a default configuration than to actively switch to another. P7 explained *"I feel like all of my accounts are protected [...] there's nothing that's gone wrong with any of my accounts, so it's just an extra hassle if I have to [set up two-factor authentication],"* but later also mentioned an account for which two-factor authentication was *"by default set up,"* for which they did not disable it. P20 explained *"if an app or platform asks me upon installation if I want to use two factors, I usually say yes, but if it does not ask explicitly, I don't [GER]."* Participants were happy to use two-factor authentication as a secure default that is set up at registration, while they would not go through the steps to set it up afterwards.

Service providers should should should offer two-factor authentication as the *default option* during registration and inform users clearly that they can *configure trusted devices* for which the second factor is not required.

6.3 Limitations

Our study was advertised as a *User Study on Security Risks in Accounts for Internet Services*. As with every study with voluntary participation, there is a self-selection bias that may lead to participants that have an above average interest in the discussed topic. This is likely the reason for the high number of participants who reported an interest in information security. Participants were required to actively use internet services and own at least one portable device with an Internet connection. The study was also advertised in places, both online and physical, that are to a large part, but not exclusively, frequented by university students from our local area. Thus, even though we did not specifically ask about this, we assume that a large fraction of our participants are students from this population group. However, we know from statements during the interviews that some participants were not students.

Despite these limitations, our study provides valuable insights into users' thought processes with respect to their online account setups. In fact, our participants' interest in the topic was likely a reason for the wide range of topics covered in our data, and was conducive to obtaining accurate account access graphs. Due to the qualitative nature of our study, we do not claim that our results are generalizable over a larger population, and thus consider the limited demographic spread among our participants acceptable. Note that only one fifth of our participants studied computer science, none of them with a focus in information security. Thus, our participant sample is meaningful for studying the behavior of interested, yet non-expert, users.

7 CONCLUSION

We developed a novel methodology, leveraging user account graphs, for systematically eliciting a user's online account setup. We used our methodology in a study with 20 participants and obtained for the first time insights into the complexity of users' unique account setups. We observed structural features within account setups, like account access patterns and cycles, and used these to demonstrate the importance of central accounts and devices within the individual users' online security ecosystem.

Our interviews provided not only an understanding of the structure of our participants' account setups; the graphical representation of the participants' elicited account setups shown to them facilitated a discussion that additionally provided insights into their beliefs, opinions, and mental models regarding these setups. This allowed us to relate our findings to previous work across diverse topics including password best practices, adoption of two-factor authentication, users' attacker models, and security advice.

Our findings suggest that personalized security analysis and advice holds much potential. However, to achieve it at scale, our process requires more automation support and we must further improve our understanding of users' account setups through larger-scale studies using quantitative metrics. In particular, we seek to learn how account setups compare between different demographics, what the prevalent account security management strategies are, and how they manifest themselves in an account setup.

REFERENCES

[1] 2021. Make your account more secure. https://support.google.com/accounts/answer/46526. Accessed: 2021-09-06.

[2] 2021. Supplementary material: Account graphs, coded transcripts, and front-end tool. https:doi.org/10.1145/3491102.3502125.

[3] Yasemin Acar, Christian Stransky, Dominik Wermke, Charles Weir, Michelle L. Mazurek, and Sascha Fahl. 2017. Developers Need Support, Too: A Survey of Security Advice for Software Developers. In *2017 IEEE Cybersecurity Development (SecDev)*. 22–26. https://doi.org/10.1109/SecDev.2017.17

[4] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA). *International Journal of Human–Computer Interaction* 33, 11 (2017), 927–942. https://doi.org/10.1080/10447318.2017.1306765

[5] Nathanael Andrews. 2018. Can I Get Your Digits: Illegal Acquisition of Wireless Phone Numbers for Sim-Swap Attacks and Wireless Provider Liability. *Nw. J. Tech. & Intell. Prop.* 16 (2018), 79.

[6] Wei Bai, Ciara Lynton, Charalampos Papamanthou, and Michelle L. Mazurek. 2018. Understanding User Tradeoffs for Search in Encrypted Communication. In *2018 IEEE European Symposium on Security and Privacy (EuroS P)*. 258–272. https://doi.org/10.1109/EuroSP.2018.00026

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

[8] Ashley A. Cain, Morgan E. Edwards, and Jeremiah D. Still. 2018. An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications* 42 (2018), 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

[9] Marta E. Cecchinato, Abigail Sellen, Milad Shokouhi, and Gavin Smyth. 2016. Finding Email in a Multi-Account, Multi-Device World. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1200–1210. https://doi.org/10.1145/2858036.2858473

[10] Sarah P Church, Michael Dunn, and Linda S Prokopy. 2019. Benefits to qualitative data quality with multiple coders: Two case studies in multi-coder data analysis. *Journal of Rural Social Sciences* 34, 1 (2019), 2.

[11] Michael Crabb, Melvin Abraham, and Saša Radomirović. 2021. "I'm Doing the Best I Can.": Understanding Technology Literate Older Adults' Account Management Strategies. In *11th International Workshop in Socio-Technical Aspects in Security and Trust*. 11th International Workshop on Socio-Technical Aspects in Security.

[12] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The tangled web of password reuse.. In *NDSS*, Vol. 14. 23–26.

[13] Sanchari Das, Andrew Dingman, and L Jean Camp. 2018. Why Johnny doesn't use two factor a two-phase usability study of the FIDO U2F security key. In *International Conference on Financial Cryptography*. Springer, 160–179.

[14] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2014. A Comparative Usability Study of Two-Factor Authentication. *NDSS Workshop on Usable Security (USEC 2014)* (2014).

[15] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences* 7, 1 (2017), 1–20.

[16] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 59–75.

[17] Uwe Flick. 2013. *The SAGE handbook of qualitative data analysis*. Sage.

[18] Dinei Florêncio, Cormac Herley, and Paul C Van Oorschot. 2014. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *23rd USENIX Security Symposium (USENIX Security 14)*. 575–590.

[19] Shirley Gaw and Edward W Felten. 2006. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*. 44–55.

[20] Joseph Gibaldi, Walter S Achtert, and Modern Language Association of America. 2003. *MLA handbook for writers of research papers*. Modern Language Association of America New York.

[21] Graham R Gibbs. 2018. *Analyzing qualitative data*. Vol. 6. Sage.

[22] Sven Hammann, Saša Radomirović, Ralf Sasse, and David Basin. 2019. User Account Access Graphs. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. ACM, New York, NY, USA, 1405–1422. https://doi.org/10.1145/3319535.3354193

[23] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 213–230.

[24] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 327–346.

[25] Kevin Lee, Ben Kaiser, Jonathan Mayer, and Arvind Narayanan. 2020. An Empirical Study of Wireless Carrier Authentication for SIM Swaps.

[26] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. 2018. Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. In *27th USENIX Security Symposium*.

[27] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 72 (Nov. 2019), 23 pages. https://doi.org/10.1145/3359174

[28] Dennis Mirante and Justin Cappos. 2013. Understanding password database compromises. *Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02* (2013).

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

[30] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium On Usable Privacy and Security (SOUPS 2019)*. 319–338.

[31] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. Association for Computing Machinery, New York, NY, USA, 666–677. https://doi.org/10.1145/2976749.2978307

[32] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. 2017. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages.. In *Thirteenth Symposium On Usable Privacy and Security (SOUPS 2017)*.

[33] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 272–288.

[34] Elissa M. Redmiles, Michelle L. Mazurek, and John P. Dickerson. 2018. Dancing Pigs or Externalities? Measuring the Rationality of Security Decisions. In *Proceedings of the 2018 ACM Conference on Economics and Computation* (Ithaca, NY, USA) *(EC '18)*. Association for Computing Machinery, New York, NY, USA, 215–232. https://doi.org/10.1145/3219166.3219185

[35] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security Privacy* 15, 5 (2017), 55–64. https://doi.org/10.1109/MSP.2017.3681050

[36] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64.

[37] Elizabeth Stobert and Robert Biddle. 2014. The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. 243–255.

[38] Heather L Stuckey. 2015. The second step in data analysis: Coding qualitative research data. *Journal of Social Health and Diabetes* 3, 01 (2015), 007–010.

[39] Viktor Taneski, Marjan Heričko, and Boštjan Brumen. 2014. Password security-No change in 35 years?. In *37th International Convention on Information and Communication Technology, Electronics and Microelectronics*. IEEE, 1360–1365.

[40] David Thomas. 2003. An inductive approach for qualitative analysis. (2003).

[41] Sarah J Tracy. 2019. *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. John Wiley & Sons, Oxford, UK.

[42] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. 2018. " I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security*.