How Do Users Chain Email Accounts Together?

Lydia Kraus, Mária Švidroňová, Elizabeth Stobert

How Do Users Chain Email Accounts Together?

Lydia Kraus[1][0000−0002−1387−3578], Mária Švidroňová[2], and Elizabeth Stobert[3]

[1] Institute of Computer Science, Masaryk University
Brno, Czech Republic
lydia.kraus@mail.muni.cz
[2] Centre for Research on Cryptography and Security, Faculty of Informatics, Masaryk University
maria.svidronova@mail.muni.cz
[3] School of Computer Science, Carleton University, Ottawa, Canada
elizabeth.stobert@carleton.ca

Abstract. Recovery connections between email accounts can be exploited in manual hijacking attacks as has been shown in several incidents during the last years. Yet little is known about users' practices of chaining email accounts together. We conducted a qualitative interview study with 23 students in which they shared their email recovery and forwarding settings with us. Altogether, we collected and analyzed information about 138 different email accounts. We used this data to map email account topologies and analyzed these topologies for recurring patterns. We found that users often make poor configuration decisions in their email recovery setups, and often create patterns in their email recovery topologies that result in security vulnerabilities. Patterns such as loops (seen in more than a quarter of our topologies) could be easily exploited in a targeted attack. We conclude that users need better guidance about how to use email based recovery settings in a robust way.

Keywords: email recovery · email forwarding · fallback authentication · security · usability.

1 Introduction

Along with the increased use of email worldwide [16], email-based fallback authentication has gained in importance during the last decade [8, 14]. Yet little is known about users' real-world practices that accompany this "new" authentication scheme. Despite the usability advantages that this scheme offers [11], it also creates connections between accounts that can be leveraged by attackers. Incidents such as Wired writer Mat Honan's "epic hacking" [9] or the compromise of Twitter employees' accounts [10] show that adversaries are able to exploit connections between email accounts in targeted attacks. These *manual hijacking* [2] attacks usually start with a social engineering attack such as phishing and then continue by exploiting both the hijacked account and any linked accounts [2]. Manual hijacking is relatively rare, but can be devastating for end users as it typically concerns accounts that are of high value for their owners [2, 13].

Although manual hijacking has been known to both security researchers and end users for many years (the Mat Honan incident took place in 2012, and was widely covered in the media), little is known about users' practices of connecting accounts. Connections between email accounts are especially interesting, as email accounts are usually long-lived and of great importance because many online services require them for registration. While connected accounts do not directly constitute an attack vector, they may create links that can be exploited in a manual hijacking attack and make them more devastating.

To examine users' vulnerabilities to manual hijacking attacks, we investigated how users connect their email accounts via password recovery and forwarding options. Our research questions were: How do users use recovery and forwarding options to chain email accounts together? What are the connection topologies that they use, and what are the security implications resulting from different connection topologies?

We conducted a qualitative user study with 23 students from a major university in central Europe. In the study, we asked participants to log into each of their email accounts and to document the connections between accounts. As users have many online accounts [15] and remembering all of them can be a challenging task, we prompted participants to recall as many email accounts as possible with different kind of guides and questions. We asked participants to map the connection topology between their accounts, and interviewed them about their email protection and configuration decisions.

Our study is the first to provide a data set of email chain topologies. Altogether, we collected and analyzed information about 138 different email accounts and 27 topologies. Our results show that email account topologies are diverse, but that many include elements of line and loop topologies. Loop topologies are especially concerning, as they allow attackers who already have access to one account to easily gain access to a further account. We also found that users created other vulnerabilities in their topologies by placing the final recovery nodes in inaccessible accounts, or by using accounts owned by somebody else as a recovery option. They also tended to keep accounts with physical recovery options (which could be strong recovery options) separate from the rest of the recovery topology. Participants were often unaware of the connections between their accounts and only realized during the study that there are recovery links they are not happy with. We suggest users need additional support in using email-based recovery in such a way that it does not increase the attack surface for manual attacks.

2 Related Work

2.1 Manual Attacks and Account Hijacking

Our threat model follows the threat model of a manual hijacking attack, as defined by Bursztein et al. [2]: "Manual hijacking consist[s] of attack[s] that opportunistically select victims with the intent of monetizing the victim's contacts

or personal data; any sufficiently lucrative credential will suffice. These attacks are carried manually rather than automatically."

In general, manual hijacking attacks (such as email-based daisy-chaining attacks) mostly start with social engineering such as phishing [2]. Once one account is compromised, attackers first check whether the account is worth further investment, for instance, by checking whether it contains financial data, linked account credentials, or personal data [2]. Thereafter, the attack usually continues with account exploitation and actions to delay account recovery [2].

When it comes to account management, users have been shown to exhibit habits that make it easier for attackers to succeed in manual attacks. The literature suggests that password-reuse and variations are inherent parts of password creation and users' password management lifecycle [15]. Similarly, using password reset options is a part of users' coping strategies for managing multiple accounts [15]. Additionally, users balance password creation effort across accounts by spending more effort for more important accounts [15]. Research by Thomas et al. shows that users whose password has been leaked in a data breach, have a higher probability of being compromised, due to convenience habits such as password reuse [17].

Account hijacking can cause concrete and emotional harm, yet the majority of users who have not personally experienced this threat seem to be unconcerned about it [13]. Interestingly, research suggests that account hijacking is more widespread than is commonly assumed. In a study conducted by Shay et al., 30% of participants indicated that they had experienced account hijacking of email or social network accounts [13]. The study by Shay et al. further suggests that personal accounts of high value are usually the targets of account hijacking.

2.2 Email-based Identification and Authentication

Already two decades ago, email based identification and authentication (EBIA) had gained in popularity, mainly due to its usability and cost advantages as compared to PKI schemes [7]. Already at that time, major web service providers such as Amazon, Yahoo, and Apple had deployed this scheme [7]. In the last decade, service providers have further intensively started to promote password recovery options, for instance through recovery phone numbers, email addresses, or through social authentication [8, 14, 4, 12].

Compared to other fallback schemes such as SMS, designated trustee, or personal knowledge questions, EBIA offers several usability advantages such as high perceived ease of use and low authentication time [11]. Yet, its security is also dependent on the passwords that users choose and on the protection of the email servers [7]. Another issue is the email address lifecycle: an email address can be owned by different people over time and different email providers have different ways of dealing with terminated addresses [7].

Email based fallback authentication is double-edged sword. On the one hand, it creates connections between accounts which may be exploited by attackers, as shown by the account compromise of Wired-writer Mat Honan [9]. Through social engineering, the attackers were able to gain access to one account which

they then used to compromise other accounts via the password recovery option [9]. On the other hand, research by Google shows that account restoration through an email address was successful for 75% of accounts as compared to 14% of accounts which used secret questions [2].

Email based recovery is the most popular method observed at Google, but it's less secure and reliable than phone-based recovery as users sometimes mistype their secondary email address [2]. Moreover, users tend to forget to keep their recovery email up-to-date [2], which we observed as well in our study.

3 Methodology

To investigate connections between users' email addresses, we conducted a qualitative interview study, asking users about their email address configurations and the decisions and understanding that informed that setup. Our goal was to gain a deep understanding of how users configure their fallback authentication, and to be able to ask our participants to reflect and discuss the ways in which their account topologies are configured. Our study focused on three aspects of email linking: the connections between the accounts (i.e., the topologies), the characteristics of the accounts (and thus of each node in the topology), and participants' perceptions of their account topology.

3.1 Procedure

An overview of the study procedure is shown in Figure 1.

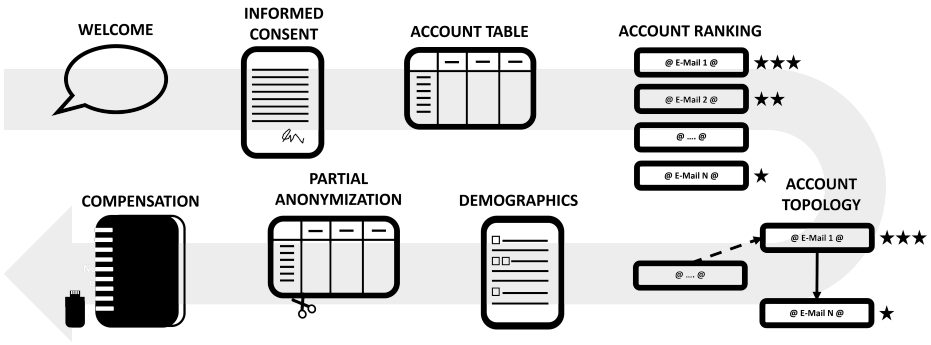

Fig. 1. Study procedure: after signing the informed consent, participants looked up recovery and forwarding settings of their accounts. Participants then ranked the accounts by importance and provided reasoning. Finally, participants created their account topologies and reflected on them. The study was concluded with a demographics questionnaire, partial anonymization of the account data, and the compensation for the participants.

In the first part of our study, we asked participants to recall as many of their email accounts as possible and to document the connections between these accounts in a printed table. Participants were given the table, and left to complete it individually. We allowed participants to supplement this data with information obtained directly from the account settings on their email address (participants were given the choice of accessing their accounts using a lab computer or bringing their own laptop). To assist participants in accessing the relevant information, we created several step-by-step guides for popular free email providers [1] as well as for the most popular providers in our country [3, 5]. This approach also helped participants recall forgotten accounts because they could sometimes be found in the recovery settings. Participants were instructed to write down a pseudonym for their email address and various properties of the account set up on the printed table. Knowing that it can be difficult for users to recall all of their accounts [15], we first let participants fill the table on their own and then prompted them towards remembering potentially forgotten accounts by asking whether they had considered different account categories, such as accounts used for communication, for online shopping, for social networking, for banking, or for online games.

Following completion of the account table, we asked participants to rank their accounts according to the subjective importance they would assign to each account. We interviewed participants about their perception of the strength of the password belonging to each account and whether they employ any additional measures (such as 2FA) to protect those accounts. We specifically did not ask participants for their passwords, and instead asked questions such as "do you think your password is unique?" or "does your password contain standard dictionary words?" to gain insights into the structure of the password without knowing the password itself.

We next asked participants to rank their accounts in order of highest to lowest importance. Participants wrote each account pseudonym on a coloured sheet of paper, and sorted those papers accordingly. We then interviewed participants about their reasoning behind the ranking and about the protection mechanisms that they deploy for each account.

Following the account rankings, we hung the coloured sheets on a whiteboard and asked the participant to draw the account connections according to the information recorded in the account table. We used this visualization of the account topology to foster further reflection on the topic, and we asked questions about participants' impressions of the map (topology), and their reasoning for how they had decided to set up recovery options.

The study concluded with a brief demographics questionnaire. We audio-recorded the interviews about the account ranking and the account topology. The account rankings and topologies (maps) were photographed for analysis. Participants completed the study in our lab, taking between 45 and 90 minutes to complete the entire procedure.

Our study was approved by Masaryk University's ethics commission. Since email addresses are personally identifiable information, we had participants phys-

ically remove their addresses (by cutting off the first column of the table) from the collected data at the end of the study.

3.2 Participants

We recruited 23 participants from our university campus in early 2020. Of those, 14 were male and 9 were female. Participants ranged between 19 and 26 years old with a mean age of 22 years. All participants were students. The majority of participants studied computer science (12, 52%), and the remaining participants came from a variety of other faculties (arts: 2, social studies: 3, science: 2, medicine: 1, law: 1, economics: 2).

3.3 Data Analysis

We used an inductive approach to analyze our qualitative data. We used the Grounded Theory approach of "all is data", and included both the interview transcripts and the account topology maps in our analysis.

We fully transcribed the interviews and translated them into English. One researcher then reviewed the transcripts line-by-line to identify themes in usage and password habits. These themes were used to create a code book (in which we listed and defined codes), which was used by a second researcher to systematically code the interviews in three rounds. After each round of coding the researcher checked for inconsistencies, and proceeded to the next round until all inconsistencies were resolved. The aim of our qualitative interview analysis was to identify account properties that would allow us to gain further insights into why the accounts are considered more or less important and how the accounts are protected.

For the topologies, we redrew all maps in a standard notation to facilitate the identification of patterns, and included account importance in the size of each node. We then conducted a qualitative analysis of the account topologies by identifying re-occurring patterns (such as line, loop, and star constellations) in the account maps. Maps and accounts were stored per participant and participants were given non-gendered coded names[4].

4 Account Types and Importance

Using the data from the account rankings together with the accompanying interviews, we were able to gain insight into users' perception and use of their email accounts.

We suspected that account properties may play a role when users are setting up recovery structures. Users treat accounts differently and spend more effort on more important accounts [15], which may in turn affect how they configure recovery options.

[4] The anonymized data set is available at: `https://crocs.fi.muni.cz/public/papers/ifipsec2021`.

Our study yielded a total of 138 accounts owned by 23 participants. Each user owned an average of 6 email accounts (min.= 3, max. = 10). We classified the accounts into four categories: private accounts, school accounts, work accounts, and somebody else's accounts. 67% of accounts (92 acc.) were private accounts – typically from popular free providers (such as Gmail or local account providers). 17% (24 acc.) were school accounts, i.e., accounts from the participant's university, and 13% (18 acc.) were work accounts, i.e., participants indicated that they were job-related. The final category, "somebody else's accounts", were those that are owned by another user and accounted for 3% (4 acc.) of all accounts. 21% (29 acc.) of all accounts listed in the study were inaccessible, i.e., the participant could not open them any more for whatever reason.

We calculated an importance index (II) for each account by normalizing the account ranking so that each rank takes a value between 0 and 1. Bottom-level ranked accounts have an importance index of 0, while top-level ranked accounts have an importance index of 1. Figure 2 shows a histogram of the importance indices. Participants made clear distinctions between between high- and low-importance accounts. Based on these rankings, we categorized accounts into high-importance ($II > 0.5$) and low-importance accounts ($II \leq 0.5$). 43% of accounts (60 acc.) in the study were high-importance, and 57% (78 acc.) were low-importance.

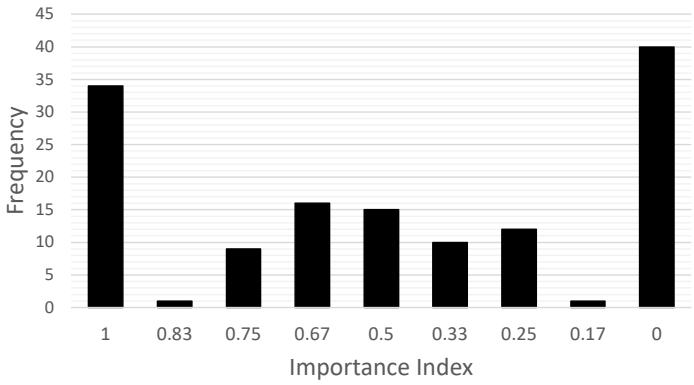

Fig. 2. Histogram of the accounts' importance indices (II). The histogram shows that users have a clear tendency to distinguish between high- and low-importance accounts.

4.1 High-importance Accounts

High-importance accounts are usually the target of manual hijacking attacks [2, 13]. In our study, high-importance accounts were most likely to belong to the *private* category (55%, 33 acc.), followed by *school* (19 acc., 32%), and *work* (8

acc., 13%). No account in the high-importance category belonged to the *somebody else's* category. Only one account ranked high-importance was inaccessible, and nine of these accounts were protected with 2FA.

Participants frequently characterized their high-importance accounts (19 acc.) by emphasizing the density of connections stemming from them. For example, Jaylen said: "In my personal emails, there is practically a lot of different personal information, practically a lot of people use it to contact me". Participants also described how their high-importance accounts are used frequently (13 acc.). These accounts are used "often" or "on a daily basis", as outlined by Kamryn: "So, um, it's an email I go to every day, every time I go to the Internet". Besides being linked to many accounts and being used often, participants further emphasized the *personal* nature of their high-importance accounts (11 acc.) and their importance as an information repository (9 acc.). As described by Cassidy "[the] highest level, that's my primary email, through which I handle all personal [things]".

Florencio, Herley, and van Oorschot [6] suggest that accounts should be classified according to the consequences that an attack on an account would yield, but it appeared that our participants used account properties to categorize the importance of their accounts. After the first round of reflection on the rankings, we further prompted participants to imagine what would happen if one of the accounts was hacked, but participants did not seem to harbour any further insights into their own behaviour in this way.

4.2 Low-importance Accounts

Low-importance accounts were also primarily categorized as *private* (59 acc., 76%), followed by *work* (10 acc., 13%), *school* (5 acc., 6%), and *somebody else's* (4 acc., 5%). More than a third of the low-importance accounts were inaccessible (28 acc., 36%). Six of these accounts were additionally protected by 2FA.

In the interviews, participants often characterized their low-importance accounts as being older (32 acc.), such as accounts that were created during childhood or youth. As indicated by Adrian: "it was the first email we just used to write to friends". Participants said that they used low-importance accounts less frequently (24 acc.), as described by Frankie: "I am not visiting this email so often and nothing terrible would happen if I forgot my login details or if they compromise it". A significant proportion of low-importance accounts were inaccessible (28 acc.): "I feel like it [the account] exists, but I have no idea what the password was there" (Harley). Low-importance accounts were also often associated with attacks or compromise (16 acc.), as described by Cassidy: "And there's just spam going on there, and I'm not watching it." Sometimes, low-importance accounts were created for a specific purpose (10 acc.), such as to preserve privacy when signing up to a new service, as described by Cary: "basically I started it just because of Facebook that in order ... I just had how to log on to Facebook."

As with the high-importance accounts, participants tended to classify the importance of these accounts according to their purposes and properties rather than according to what would happen if those accounts were compromised.

5 Account Topologies

Next, we analyzed the account topologies that we obtained from the printed table and that we visualized together with the participants in the third part of the study. Altogether, our data set contained 27 email account topology maps. Each map contained on average 3.57 accounts with a minimum of 2 accounts and a maximum of 8 accounts.

Out of 27 email topologies, we only found five which did not contain any apparent vulnerability. These five belonged to participants that had deployed additional two-factor authentication to protect the important accounts in their maps. An overview of issues that we encountered during the study can be seen in Table 1.

Eight topologies ended in an inaccessible account as a final node (30%). The remainder either finished at somebody else's account (3 acc., 11%) or placed the critical end node in low-importance accounts (4 acc., 15%). There were only a few forwarding connections in our data set and in only one chain (Rene) they impacted the recovery flow by forwarding emails (with deletion) from a recovery account to another account.

Interestingly, none of the participants used their school or work account account as a final node. This is a surprising finding, as those accounts can usually be physically recovered (e.g. by visiting the study office or a local admin) and would thus constitute a stronger restoration capability than private accounts or somebody else's accounts.

5.1 Topology Patterns

Using the well-known network topology model, we identified three topology categories: loop, star, and line topologies. We examined participants' account maps to identify what patterns were present. Each map could contain elements of more than one type of topology.

Seven participants' email chains contained a loop pattern. The classical loop pattern consists of two accounts that recover to each other. This creates a significant security vulnerability, as an attacker who has access to account A can easily gain access to account B. All an attacker needs to do is search in the settings of account A for recovery accounts and then try to reset the recovery account by the help of the already hijacked account.

A star topology pattern is a topology where multiple accounts recover to one single account, thus creating a single point of failure. Five participants' accounts contained this pattern. As long as the single point of failure is well-protected (e.g. by two-factor authentication (2FA)), this topology is not likely to create increased opportunities for manual hijacking accounts. However, the application of additional measures to the central node was relatively rare, and we only saw this in one user's topology in our study: Kendall linked six accounts to one single account and this account was 2FA protected (Table 1).

The line topology chains two or more accounts in sequence. Short line topologies of two accounts are the typical fallback set-up. In our study, we found 23

Table 1. Issues identified within each email chain, sorted by account chain length (L). Column 4 presents a summary of the recovery information flow between accounts of low and high importance and 2FA protected accounts, while column 5 presents topology and information flow related issues.

Participant	L	**Topology**	**Information Flow**	**Issue**
Cary	2	Line	high $\rightarrow$ *low*	Final node not controlled by user
Cassidy	2	Line	low $\rightarrow 2FA$	None (final node 2FA secured)
Cleo	2	Line	high $\rightarrow$ *low*	Final node of low importance
Finley	2	Loop	high $\leftrightarrow$ *low*	Loop increases attack surface
Frankie	2	Line	inacc. $\rightarrow$ *inacc.*	Both accounts inaccessible
Parker	2	Line	high $\rightarrow$ *low*	Final node not controlled by user
Rene	2	Line (fwd)	equal info low	Not relevant
Sage	2	Line	high $\rightarrow$ *inacc.*	Final node inaccessible
Sandy	2	Line (fwd)	equal info low	Not relevant
Adrian	3	Star	high,2FA $\rightarrow$ *low*	Final node of low importance
Cassidy	3	Line, Loop	low $\rightarrow$ *low* $\leftrightarrow$ *low*	Loop increases attack surface
Harley	3	Line	high $\rightarrow$ *inacc.*	Final node inaccessible
Kamryn	3	Line, Loop	inacc. $\rightarrow 2FA \leftrightarrow$ *high*	None (central node 2FA secured)
Kayden	3	Line	high $\rightarrow$ *low*	Final node of low importance
London	3	Line	high $\rightarrow$ *low* $\rightarrow$ *inacc.*	Final node inaccessible
Pat	3	Line	high $\rightarrow$ *inacc.*	Final node inaccessible
Rylan	3	Line, Loop	low $\rightarrow$ *high* $\leftrightarrow$ *low*	Loop increases attack surface
Sandy	3	Line	high $\rightarrow$ *low*	Final node not controlled by user
Frankie	4	Line, Loop	low $\rightarrow$ *high* $\leftrightarrow$ *high*	Loop increases attack surface
Jaylen	4	Line	high $\rightarrow$ *low*	Final node of low importance
Shannon	4	Line	low $\rightarrow$ *high* $\rightarrow$ *inacc.*	Final node inaccessible
Stacey	4	Line, Loop	2FA $\rightarrow 2FA \leftrightarrow$ *low*	None (central node 2FA secured
Marion	5	Star	high,low $\rightarrow$ *high*	OK, final node of high importance
Bailey	7	Ln., Lp., St.	Info flow in 5 directions	Loop increases attack surface
Jessie	7	Line	high $\rightarrow$ ... $\rightarrow$ *inacc.*	Final node inaccessible
Kendall	7	Star	2x high, 4x low $\rightarrow 2FA$	None (final node 2FA secured)
Rene	8	Line, Star	high $\rightarrow$ ... $\rightarrow$ *inacc.*	Final node inaccessible

instances of this pattern, mainly short sequences. However, we also found maps where participants had chained more than 2 accounts together – there were two participants with four or more accounts in a line (Jessie, Rene). In this category, there were also three participants who had a chain of accounts that ended in a recovery account belonging to somebody else (and was thus out of the control of the main account's user). Another pattern we saw in line topologies was that the final nodes (i.e., the accounts at the end of the chain) were often either of low-importance or inaccessible. From the account analysis, we know that low-importance accounts are more often older and inaccessible which can create a problem during account restoration.

5.2 Separate Accounts

To further understand the underlying patterns in participants' account topologies, we investigated which kind of accounts are kept separate from the rest of the chain. In total, 41 accounts were not involved in any chain. Among those accounts were 19 private accounts (46%), 15 school accounts (37%), and seven work accounts (17%). Together, school and work accounts constitute more than 50% of the separate accounts. This is especially noteworthy as those accounts can often be physically restored and should thus be more robust for account recovery after manual hijacking.

5.3 Recovery Use Motivation and Perceptions

In the last part of the study, we further asked users whether they set-up recovery on their own initiative or whether it was motivated by the email provider. An overwhelming majority (21 participants) indicated that the email provider prompted them to do so, as described by Cleo: "it kept popping up that you would secure your account, so I already said that well, so I'll take care of it, so I'll put it on the one, I'll put it on the email, on which I can basically sign up for."

This finding is unsurprising, as email providers have already started years ago to promote fallback authentication (see e.g. [8]), but it does demonstrate that users generally are not concerned with setting up fallback mechanisms, and that their motivation to do so is often externally imposed.

When asked about their perception of their own topology, most participants expressed significant observations resulting from the graphical depiction of their account setup.

Ten participants noticed aspects of their topology that they were not happy with. Some were concerned about a proper account recovery, like Shannon, who mentioned that "the only thing with the restoration in the [account] is that it could be there problem getting to that account." Others noticed security shortcomings in their topology set-up, like Cleo, who mentioned: "The old [account] is just as uninteresting, but now that I actually realized that I actually have the same passwords there."

Only seven participants indicated that there were no surprises in their account topologies. For instance, Cary said: "I guess I was aware that those are connected, and others aren't". Similarly, Jessie stated that there is "nothing I didn't know before".

6 Discussion

In this work, we explored users' vulnerabilities to account hijacking attacks by investigating how users chain email accounts together by using recovery options. We conducted a study with 23 participants, and identified three prevailing account topologies in which users structure their recovery accounts.

We found multiple aspects of our participants' email chaining to have significant security ramifications. The loop pattern (which was used by more than a quarter of our participants) was the most concerning. If a user's accounts are configured this way, an attacker who manages to compromise one account can easily hijack another. We also found that the final nodes of the recovery chains are often inaccessible (30% of all topologies), of low-importance (15% of all topologies), and sometimes owned by somebody else (11% of all topologies). All of these create problems for recovery, and the potential for failed recovery attempts if another account does get hijacked. Low-importance accounts are often created a longer time ago, are used less frequently, are often inaccessible, and sometimes used as spam collectors. This can create problems during account restoration as users may not be able to access them and email providers may even terminate access if the account has not been accessed for a while. Similarly, relying on recovery accounts owned by somebody else may create problems during account recovery as the recovery account may not be accessible in a timely manner (or at all).

We also interviewed participants about their understanding of their email topologies. We found that users do not seem concerned with security when configuring their fallback email accounts. Using email based recovery seems to be mainly encouraged by the email provider and users do not seem to spend much effort on creating robust links between their accounts. While account providers keep on reminding users to configure and maintain account recovery, they should also remind users to avoid insecure recovery practices, and encourage users to choose fallback addresses to which they expect to have lasting access. They should also recommend the use of additional security mechanisms (such as 2FA) on accounts that support others.

Limitations: The prevalence of manual hijacking attacks for the average end user is unclear. Mat Honan [9] and the Twitter employee compromise [10]) were both high-value targets, and the attacks on them were both devastating and well-publicized. While our work shows that email topologies actually exist, we cannot draw any conclusions about the likelihood that such a configuration might be actually exploited. However, the topologies that we identified contain weak points, about which users should be concerned.

We chose our methodology to allow us to closely examine users' email configurations and their understanding of those configurations. Our study examined only a small group of relatively young users, and a remaining question is how these findings generalize to a larger population. Yet, our results suggest that a larger scale study could give insight into vulnerabilities to manual hijacking attacks.

7 Conclusion

Our study of users' email configurations showed that many users' fallback emails are configured in a way that could potentially open them to vulnerabilities from manual hijacking attacks. We conducted a study with 23 students in which they shared their email recovery and forwarding settings with us. Our study showed that many users build (sometimes even sophisticated) chains that resemble diverse topology patterns such as loops, lines, and stars. However, these topologies seems to be rather a consequence of being prompted by email providers to set-up recovery accounts, than by intentional design with robustness in mind. We analyzed these patterns and their pitfalls and come to the conclusion that email providers should exercise more care when prompting users to set up email based recovery. Instead of just pointing users to use this feature, email providers and other security educators should also encourage users to protect their recovery accounts as well as their primary accounts (ideally with 2FA) and to avoid the use of recovery loops.

Acknowledgements This research was supported by ERDF project CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence (No. CZ.02.1.01/0.0/0.0/16_019/0000822). We would like to thank all of our participants for taking part in the study. Thanks also goes to Agáta Kružíková for help with study logistics. The user study was conducted while Lydia Kraus was a postdoctoral fellow at the Faculty of Informatics at Masaryk University.

References

1. Biswal, R.: Top 10 Best Free Email Service Providers 2020 (2020), https://web.archive.org/web/20200501082105/https://www.ecloudbuzz.com/best-free-email-service-providers/
2. Bursztein, E., Benko, B., Margolis, D., Pietraszek, T., Archer, A., Aquino, A., Pitsillidis, A., Savage, S.: Handcrafted fraud and extortion: Manual account hijacking in the wild. In: Proceedings of the 2014 Internet Measurement Conference. pp. 347–358 (2014)
3. Dobryemail.cz: Čím otevírají Češi e-maily a kde? (2017), https://dobryemail.cz/novinky-trendy/cim-oteviraji-cesi-e-maily-kde
4. Facebook Security: Introducing Trusted Contacts (2013), https://www.facebook.com/notes/facebook-security/introducingtrusted-contacts/10151362774980766/.

5. Fišer, M.: Nejoblíbenějším českým poskytovatelem e-mailu je podle průzkumu Seznam.cz (2009), https://www.novinky.cz/internet-a-pc/clanek/nejoblibenejsimceskym-poskytovatelem-e-mailu-je-podle-pruzkumu-seznamcz-40239742.
6. Florêncio, D., Herley, C., van Oorschot, P.C.: An administrator's guide to internet password research. In: 28th Large Installation System Administration Conference (LISA14). pp. 44–61 (2014)
7. Garfinkel, S.L.: Email-based identification and authentication: An alternative to PKI? IEEE Security & Privacy **1**(6), 20–26 (2003)
8. Google Help: Why add recovery options? (2012), https://www.youtube.com/watch?v=4SjJ2i1mc2Y
9. Honan, M.: How apple and amazon security flaws led to my epic hacking. Wired.com pp. 1–4 (2012), https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
10. Keizer, G.: Report: Hacker broke into Twitter e-mail with help from Hotmail (2009), https://www.computerworld.com/article/2525893/report-hackerbroke-into-twitter-e-mail-with-help-from-hotmail.html
11. Markert, P., Golla, M., Stobert, E., Dürmuth, M.: Work in Progress: A Comparative Long-Term Study of Fallback Authentication. In: Workshop on Usable Security (USEC) (2019)
12. NRJC: Outlook demanding my phone number. How do I continue using Outlook without giving my phone number. (2013), https://answers.microsoft.com/en-us/outlook_com/forum/all/outlook-demanding-my-phone-number-how-doi/95511277-0a17-46a0-9b17-f8470d1514f0
13. Shay, R., Ion, I., Reeder, R.W., Consolvo, S.: "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra": Experiences with Account Hijacking. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. p. 2657–2666. CHI '14, Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2556288.2557330
14. Smetters, D.: Don't get locked out: set up recovery options for your Google Account. (2013), https://blog.google/technology/safety-security/dont-get-locked-out-set-up-recovery/
15. Stobert, E., Biddle, R.: The Password Life Cycle: User Behaviour in Managing Passwords. In: 10th Symposium On Usable Privacy and Security (SOUPS) 2014). pp. 243–255 (2014)
16. The Radicati Group Inc.: Email Market, 2019-2023 (2019), https://www.radicati.com/wp/wp-content/uploads/2019/01/Email_Market,_2019-2023_Executive_Summary.pdf
17. Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., et al.: Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. pp. 1421–1434 (2017)