A Mixed-Methods Study on User Experiences and Challenges of Recovery Codes for an End-to-End Encrypted Service

Sandra Höltervennhoff[L] Noah Wöhler[C] Arne Möhle[T] Marten Oltrogge[C]
Yasemin Acar[PW] Oliver Wiese[C] Sascha Fahl[C]

[L]*Leibniz University Hannover*
[C]*CISPA Helmholtz Center for Information Security*
[P]*Paderborn University*
[W]*The George Washington University*
[T]*Tutao GmbH*

Abstract

Recovery codes are a popular backup mechanism for online services to aid users who lost their passwords or two-factor authentication tokens in regaining access to their accounts or encrypted data. Especially for end-to-end encrypted services, recovery codes are a critical feature, as the service itself cannot access the encrypted user data and help users regain access. The way end-users manage recovery codes is not well understood. Hence, we investigate end-user perceptions and management strategies of recovery codes. Therefore, we survey users of an end-to-end encrypted email service provider, deploying recovery codes for accounts and encrypted data recovery in case of authentication credential loss. We performed an online survey with 281 users. In a second study, we analyzed 196 support requests on Reddit. Most of our participants stored the service provider's recovery code. We could identify six strategies for saving it, with using a password manager being the most widespread. Participants were generally satisfied with the service provider's recovery code. However, while they appreciated its security, its usability was lacking. We found obstacles, such as losing access to the recovery code or non-functioning recovery codes and security misconceptions. These often resulted from users not understanding the underlying security implications, e.g., that the support cannot access or restore their unencrypted data.

1 Introduction

Online accounts are commonly protected with authentication mechanisms using passwords and two-factor authentication. To protect user data further from unauthorized access by the service provider or other third parties, some apps and online services encrypt user data or use end-to-end encryption for communication purposes. Encryption keys are often derived based on users' passwords [1]–[5] using some form of password-based key derivation [6]–[9].

While deploying cryptography to restrict access to user data, most services also aim to support users who have forgotten or lost their login credentials in recovering their accounts or access to encrypted data. Otherwise, users may be locked out of their accounts and data permanently. Recovery codes can act as a feasible and secure fallback key for these services. They are most widespread as two-factor authentication (2FA) fallback [10], [11], but they can also function as recovery feature to access encrypted accounts in case of password loss [1], [12]–[14]. While a variety of other popular account recovery schemes exist, e.g., email recovery, SMS recovery, or security questions, all of them are not only susceptible to attacks [15]–[18] but also require the service provider to be able to access the account data. These measures are not feasible for service providers that encrypt the user data without having a backup key. However, for services deploying recovery codes, users must store their recovery codes securely as they hold significant value to potential attackers, bypassing the standard authentication process and granting access to user accounts. Recent reports highlight the significance of recovery codes, as evidenced by the activities of thieves who intentionally focus on iPhone users. Their objective involves tampering with the stolen devices to establish or modify the 28-character recovery codes, ultimately enabling unauthorized access to the victim's Apple ID account [19].

Since the management of recovery codes has not been studied in the past, in this work, we conduct a mixed-method study to investigate end users' awareness and management of their recovery codes and the challenges they face. We cooperate with an end-to-end encrypted email service that utilizes recovery codes as the only account and encrypted data recovery option. The email service deploys recovery codes for both 2FA and password loss. We survey users of the email service regarding their experiences and approaches to managing their recovery codes. We further qualitatively analyze support requests on Reddit from users of the email service regarding account and encrypted data recovery to identify misconceptions and challenges regarding the recovery code.

In the course of this work we address the following research questions:

RQ1 *"Are users aware of the existence and importance of recovery codes?"* Recovery codes often are an essential, if not

the only, way of retaking an account after the compromise or loss of the primary authentication method. End-users should be aware of their existence and important nature. We are interested in whether users know the impact of losing their recovery codes for recovering their encrypted user data.

RQ2 *"What strategies for handling recovery codes do users deploy?"* Due to their criticality, end-users should handle recovery codes with diligent care. We investigate how users approach account recovery and store and manage their recovery codes. We discuss confidentiality, integrity, and availability of the strategies we identified.

RQ3 *"What obstacles do users face when using recovery codes?"* The storage and management of recovery codes are not necessarily hassle-free. We explore which obstacles and misconceptions users face regarding their recovery code.

2 Background

In this section, we will explain methods commonly used for account recovery, as well as introduce our email provider and its implementation of recovery codes.

2.1 Recovery schemes

If users forget their passwords or lose their devices, recovery schemes help them to regain access to their accounts or encrypted data. It helps them to recover their accounts, cryptographic secret keys, or cryptocurrencies. The security model of a specific application or service limits the possible recovery schemes. For example, a trusted third party, e.g., the service providers themselves, can support users to recover their objectives and give them access to their accounts.

There are different principles for designing recovery schemes:

1. Special registration/access: The user and (trusted) service provider can establish a secure recovery channel in advance. For example, the user can register a recovery email address, a phone number or trusted device. If users lose access to their account, they can convince the service provider or administrator about the account's ownership by replying to a phone call, SMS, or email. For example, social media account providers often use this scheme [20]–[22]. If users register a trusted device, they can regain access to an account by having access to the device, e.g. a smartphone.

2. Secret knowledge: The user and service provider can share a secret in advance, e.g., a password/code or security questions.

3. Ad-hoc schemes: In case of no preparation, more informal and ad-hoc recovery schemes are possible. For instance, users can verify their identity using their official ID card or contact the service provider.

The security model of end-to-end encryption excludes a trusted third party having access to users' (plain) secret keys and thus restricts possible recovery options. Without a trusted third party, users can only recover secrets based on another secret known by them. Therefore, users have to back up their secret keys themselves.

2.2 Our Partner

We cooperated with Tuta, an email provider that provides end-to-end encryption for their email users. In addition to password-based authentication, users can add a second factor for authentication. The security model of Tuta is similar to end-to-end encryption, as they exclude themself as a trusted third party. Therefore, the users' mailboxes are encrypted on their servers, and the service provider cannot access the (plain) decryption keys. On account creation, users create a public key pair on their device (or in their browsers). The account password does not only enable the login but protects the private key on the server. As our email provider does not know the password, the dual use of the user's password limits the possible recovery schemes.

Therefore, the recovery scheme of Tuta is a recovery code. The recovery code is a locally generated string with 16 words, each of 4 characters. It is shown to users during account registration, and they are prompted to store it securely, e.g., on a sheet of paper. The recovery code dialog is shown in Figure 1. It is a typical key recovery scheme used in other end-to-end encryption applications, e.g., password managers like NordPass and Dashlane [12], [13], or messengers like Keybase [23]. Users of Tuta need either one out of two factors (password or recovery code) if they do not use 2FA or two out of three factors (password, 2FA, or recovery code), with 2FA activated, to recover their accounts and their secret keys.

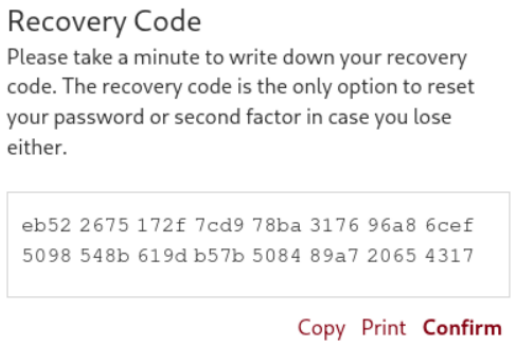

Figure 1: The recovery code pop-up shown to Tuta users. The pop-up illustrates the purpose and criticality of the code and encourages users to store the code.

3 Related Work

In this section, we discuss related work regarding account recovery methods and recovery research with a special focus on the usability of account recovery.

In 2006, Brainard *et al.* introduced and designed a new recovery method, in which a pre-chosen helper can generate a temporary passcode via a hardware token, and discussed the security of their approach [24]. In a similar vein, Schechter *et al.* presented an account recovery method, in which account recovery codes are gained from trusted individuals appointed beforehand. They found that users often forgot which confidants they chose [25]. Rabkin examined the backup authentication mechanism of banking sites. They found that personal security questions were often utilized and illuminated usability and security weaknesses [26]. In 2015, Bonneau *et al.* analyzed Google data on personal knowledge questions for backup authentication and found that their security is lacking [18]. Through a survey and interviews, Hang *et al.* examined backup authentication methods for smartphones. They found that although most users were satisfied with their backup methods, some users had difficulty recovering their phone [27]. In 2016, Stavova *et al.* conducted an experiment to analyze two account recovery mechanisms for usability, backup codes, and trusted people. Most of the participants found backup codes to be easier but regarded the trusted people approach as more secure [28]. Parkin *et al.* analyzed university helpdesk log data of password resets and conducted succeeding interviews. They found that many participants found the password policies to be too restrictive [29].

Through a survey, Huh *et al.* researched the impact of a password reset email from LinkedIn, sent after experiencing a data breach. They found that less than half of the participants reset their password, and many only did so long after receiving the email [30]. In 2019, Maqbali *et al.* presented a model for password recovery processes, evaluated existing recovery approaches, and gave recommendations for improving them [31]. Neil *et al.* analyzed account remediation advice from 57 websites and found that advice was often incomplete. Popular websites or those that previously experienced a data breach generally performed better [32]. In 2023, several works covered recovery of 2FA. Ghorbani Lyastani *et al.* investigated uniformity of multi-factor authentication (MFA) implementations, they found that the setup of a recovery option was seldom enforced. The recovery option most often provided was one-time recovery codes [33]. Gerlitz *et al.* went through the 2FA account recovery processes of 78 services. They found a vast heterogeneity of practices with respect to implementing 2FA and processes for recovering from loss [10]. Amft *et al.* also investigated MFA deployment of recovery methods. They found recovery codes and contacting the support the most mentioned methods for MFA recovery [11].

In addition, there is also work on different attack vectors for account recovery. In 2014, Javed *et al.* presented a new attack method against a social authentication method "Trusted Friends" as implemented by Facebook [34]. Guri *et al.* discussed information disclosure of private data during account recovery attempts on popular websites and resulting attack vectors [35]. Gelernter *et al.* described a new password reset man-in-the-middle attack. They checked password reset functions of popular sides against it and found many to be vulnerable [36]. In 2018, Li *et al.* investigated employed recovery methods and found that most websites use email as a recovery method. They further assessed possible email recovery attack scenarios and found most websites vulnerable [15].

While there are many studies regarding account recovery, only a few investigate the actual deployment and usage in companies or on websites. We close this research gap, by presenting insights about a recovery method deployed by an actual email provider. Our work focuses on a specific implementation of a recovery code as the only fallback method for an encrypted service. We take a mixed-method approach towards users' handling and their view on recovery codes.

4 Methodology

Below, we describe our methodology for the survey with users of Tuta and the qualitative analysis of Reddit threads regarding account recovery. We also detail the coding process and analysis of the qualitative and quantitative data before discussing ethics and the limitations inherent to our research approaches.

4.1 Online Survey with Users

To investigate our first two research questions, we conducted an online survey with (n = 281) Tuta users. In this section, we detail the study procedure and structure of the survey we conducted.

4.1.1 Survey Procedure

We created the questionnaire according to our research questions and pre-tested the questionnaire with team members and personal contacts in cognitive interviews [37]. While going through the questionnaire with them, we focused on possible (mis)interpretations of questions, biases, phrasing, and given response choices. We iteratively revised, reordered, and rewrote questions after each of the conducted cognitive interviews (n = 14).

Having converged on a satisfactory version of the questionnaire, we then shared it as an addendum to a monthly newsletter of Tuta that is sent to each user in the form of an email. We only required that participants had received the newsletter, meaning that they were a user of Tuta in some capacity, that they were at least age 18, and that they were comfortable using English. The survey was created and shared

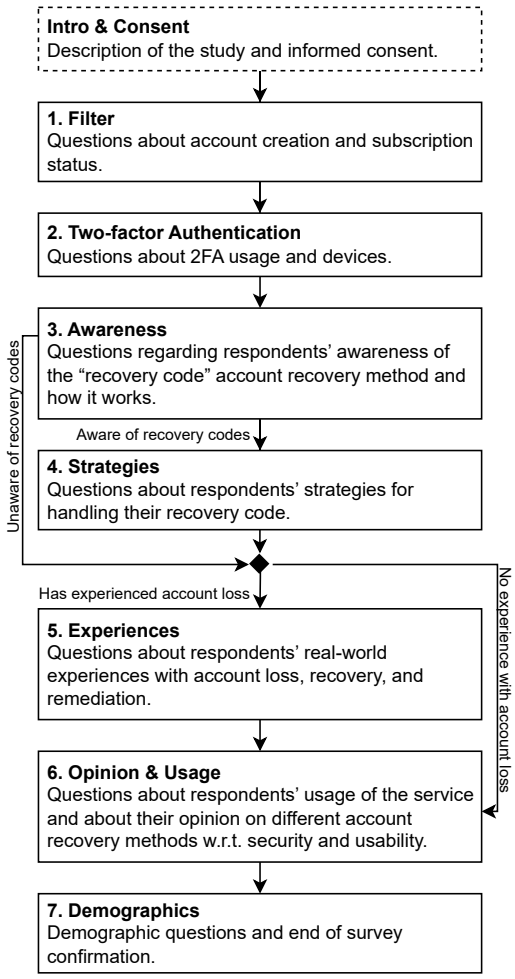

Figure 2: Overview of the survey flow and topics. The survey consisted of seven topics covering awareness of recovery codes, storage and management strategies, experiences with recovery codes, opinions and account usage, and demographic information.

in the November 2022 newsletter, and data collection was continued through February 2023.

4.1.2 Survey Structure

The survey included eight sections in total and was presented to all participants in the same order. Some questions or entire sections were skipped according to the answers given so as to not confuse participants or collect subpar data, as shown in Figure 2. The survey was delivered exclusively in English, although a few participants chose to answer free text questions in German.

1. Filter This section contains two general questions about account creation for Tuta and whether the participants have a paid Tuta subscription to display additional answer options later and to better contextualize written responses to free text questions.

2. Two-factor Authentication. This section explores our participants' 2FA usage, i. e., whether they have two-factor authentication enabled for Tuta and what method they use.

3. Awareness This section intends to gain insights into participants' awareness of Tuta's recovery method using recovery codes. Specifically, the first question asks how they would approach recovering their account if they lost their password. The second question asks a similar question regarding losing their second factor if they previously indicated using 2FA for Tuta. We then ask them whether they feel well informed about Tuta's recovery method and whether they know what a recovery code is used for. If they indicate that they know about recovery codes, they are shown some more questions about their understanding of their functionality.

4. Strategies In this section, we ask participants about their strategies for dealing with their recovery code. Being one of the central questions that motivated this survey, this open-ended question asks them to elaborate on their reasons for proceeding in such a way.

Secondly, we are interested in how long it would take them to access their recovery code in an everyday situation given their chosen strategy.

5. Experiences This section goes into participants' experiences with actual Tuta account loss and subsequent recovery. We are interested in how many participants had already used the recovery method, whether they were successful, and if not, whether they had lost data and how they dealt with losing access.

6. Opinion & Usage After a brief high-level explanation of how Tuta's recovery method works, we ask participants how they would judge the privacy-accessibility trade-off of the method. We then ask whether they have heard about or used six different recovery methods that are used by various services with varying incidences. In an optional step, participants are asked to order the methods they have heard about in terms of security and usability. We are also interested in whether they are satisfied with Tuta's current recovery method and whether they would like to see others implemented. Lastly, we ask how frequently participants use Tuta, their main use cases, the amount of critical data they store in Tuta, and who they think has access to their unencrypted inbox.

7. Demographics This last section contains demographic questions and finally the option to submit one's answers.

4.1.3 Coding and Data Analysis

Our survey was started by 333 participants, from which 281 completed it. As we did not find any inconsistencies in the data, we consider all 281 answers valid. We analyzed all open-ended questions using an iterative open coding approach [38]–[40]. For each open-ended question, a pair of two researchers independently coded all responses. They then talked about

each answer, compared codings, discussed the assigned codes, and arrived at a final set of codes. Three researchers were involved in the whole coding process. As the discussions, in which all disagreements for the dataset were resolved, were crucial for forming our results, we refrained from reporting an intercoder agreement [41]. We then established one codebook for each question by listing all the assigned codes, adding a description to each, and lastly merging codes that we deemed similar enough. The codebooks were then used for grouping results and for reporting in Section 5.1.

When reporting percentages in the results sections, we normalized through all participants who saw the respective question. Regarding the two questions where participants ranked the recovery methods, we normalized the data by min-max normalization, as participants were only shown the methods they knew. Thus, each participant ranked a different quantity of methods.

4.2 Recovery Support Discussions on Reddit

To get deeper insights into the challenges and misconceptions related to recovery codes, we conducted a qualitative analysis of related online discussions in the Tuta's support forum on Reddit. We choose Reddit threads, as analyzing users' support requests directly would break data protection policies, especially as it is not transparent which of those users consented to data collection. Tuta only offers customer support for paid users, therefore, the subreddit is a valuable alternative for free users to ask questions.

We gathered all posts in the subreddit that were returned searching for the term "recovery" in April 2022. This was done using Reddit's official API[1] via the PRAW library[2]. The search resulted in a dataset of 233 posts in total that potentially pertained to account recovery.

In a first pass, teams of two researchers assessed the relevance of each post, meaning that they are connected to Tuta's account recovery. All posts that were deemed relevant were then coded in an iterative open coding approach [38]–[40]. Our analysis referred to the main posts and any remarks from the thread owners in the comment sections. Each Reddit post was coded by two researchers. Conflicts were resolved in a subsequent step by discussing and merging, removing, or adding codes for new themes. A total of three researchers were involved in the coding. As for the survey, we did not calculate an intercoder agreement, as it could not reflect on the crucial team discussions and iterations.

4.3 Ethics

Both experiments were designed in due consideration of the ethical principles of the Menlo report [42] and approved by the ethical review board of our institution. We further adhered to the EU's General Data Protection Regulation (GDPR). For the survey, we made sure that participants were aware of the contents, the purpose, and the risks of participating in the study before choosing whether they wanted to participate. Therefore, we obtained informed consent from each participant by having them fill out a mandatory form confirming that they were at least 18 years old, comfortable participating using English, that they had no unanswered questions regarding the study, and that they were aware that they may stop participating and/or revoke the given consent at any time. In order not to annoy users by sending out unsolicited invitations to the survey via direct email or other channels, we chose to attach a summary and a link to the survey to Tuta's newsletter to reach a large number of active users. We did not offer our participants any compensation and advertised an estimated survey completion time of 10 to 20 minutes.

4.4 Limitations

For each of our mixed-methods approaches, different limitations apply. The survey may suffer from several biases typical for this sort of online study, such as self-reporting bias, over- and underreporting, sampling bias, and, to a lesser extent since responses are anonymous, social-desirability bias. Our sample further consists of active users of one privacy-centered email provider, which is not representative of email users or privacy-conscious users in general. Security- and privacy-interested users were likely more inclined to participate in our survey, which means that our results should be seen as an upper bound for the reported awareness numbers and as a lower bound for the reported, e.g., account recovery experience numbers. We did not compensate our participants for taking part in the survey, as Tuta is committed to its users' anonymity, but the legal framework of our university does not allow us to compensate participants anonymously.

The analysis of Reddit threads might include mostly free users, as paid users enjoy priority email support and could ask or voice their frustrations there. Regarding account recovery, however, there is no difference in the process, except that paid users have the option to prove past payments via receipts to transfer their email alias to a new account.

5 Results

In this section, we report on our survey results with 281 Tuta users and our analysis of 196 Reddit threads regarding account recovery.

5.1 Online Survey with Users

We conducted a survey with Tuta users aimed to investigate the handling and utilization of recovery codes, as well as uncover obstacles and opinions. Our 281 participants completed the survey in 13.0 minutes (median time). As participants

[1] https://www.reddit.com/dev/api/
[2] https://github.com/praw-dev/praw

Table 1: Demographics for all 281 valid participants from the survey study with Tuta users.

Demographics	Value	Percent
Gender:		
Man	211	75.1%
Woman	37	13.2%
Genderqueer	8	2.8%
Age:		
18-24 Years	40	14.2%
25-34 Years	83	29.5%
35-44 Years	51	18.1%
45-54 Years	46	16.4%
55-64 Years	24	8.5%
64 and Older	21	7.5%
Education:		
Bachelor Degree	89	31.7%
Master Degree	80	28.5%
Secondary School	33	11.7%
Trade/Technical/Vocational	19	6.8%
Associate Degree	7	2.5%
Professional/Doctoral Degree	27	9.6%
Other	9	3.2%
Employment:		
Employed Full-Time	126	44.8%
Employed Part-Time	12	4.3%
Self-Employed/Freelancer	37	13.2%
Out of Work	21	7.5%
Student	35	12.5%
Retired	20	7.1%
Other	11	3.9%

were given the option to not answer questions, not all results will sum up to 281 answers.

Demographics Many of our participants were rather young and identified mostly as male. As shown in the demographics in Table 1, most of our participants had a bachelor's degree (89, 31.7%), master's degree (80, 28.5%), or completed secondary school (33, 11.7%).

While most (137, 48.8%) of our participants used Tuta for up to four years, 90 participants (32 %) stated to use Tuta for up to one year and are, thus, relatively new to the email provider. Further, 46 participants (16.4%) stated using Tuta since more than four years. Regarding payment, 201 participants (71.5%) paid for their account, while 77 participants (27.4%) used a free account. Most of our participants were regular users, as 175 participants (62.3%) stated to use Tuta daily, followed by 52 (18.5%) who used the email provider four to six times a week. The use of 2FA was relatively balanced, as 142 participants (50.5%) opted for having 2FA and 127 (45.2%) stated to not have 2FA (seven participants were unsure).

Regarding their main usage of Tuta, 189 participants (67.3%) used it for everyday communication. Second most frequently selected, by 131 participants (46.6%), was signing into sensitive services. Explicitly receiving or sending confidential documents was specified by 115 (40.9%) and 111 participants (39.5%) respectively. Other reasons were less prevalent, like using the service for work (69, 24.6%).

An extended demographic table and a full list of what critical data participants reported to store in their accounts can be found in Appendix Table 3 and Table 4.

> Demographics.
>
> - We surveyed 281 users of the end-to-end encrypted mail service Tuta.
> - Most participants used Tuta several times a week.
> - Our participants used Tuta for every day communication, but also for sensitive data or signing into sensitive services.

Recovery Code Awareness. To investigate the awareness of our participants regarding the recovery code, we first asked open or general questions regarding account recovery without mentioning the recovery code explicitly. Most of our participants felt at least moderately well-informed about account recovery by Tuta, with 118 (42%) feeling very well-informed. Only 34 (12.1%) felt not well-informed at all.

Asked how they were informed, most participants (122, 43.4%) stated that it was during signup, 80 (28.5%) read it in the website's FAQ, and 74 (26.3%) while they set up 2FA. Further information channels, e.g., blog posts, or social media, were each selected by at most 20 participants. Some participants (43,15.3%) were not sure how they were informed or felt that they were not informed at all (25, 8.9%).

Asked how they would recover from a password loss, 139 (49.5%) stated that they would use the recovery code. Moreover, 40 participants (14.2%) stated that they would use a password manager, either indicating that a password loss was unlikely or that the password was backed up there. Twelve participants (4.3%) mentioned password backups outside a password manager, e.g., writing it down offline. To that end, 23 (8.2%) felt very confident that they could not lose their password. Measures only taken after the loss of the password were also mentioned. Some participants (27, 9.6%) hoped that the support could help them. Clicking on the "forgot password" interface was mentioned by twelve participants (4.3%) and searching for website instructions by eight (2.8%). Two participants (0.7%) talked about security questions and 14 participants (5.0%) about backup emails. Interestingly, the latter two options are not available for Tuta. Ten participants (3.6%) stated that they never checked or thought about this scenario, and nine participants (3.2%) stated that there would be no recovery. All answers are visualized in Figure 3.

A similar picture emerged when we asked the 142 participants using 2FA for Tuta about their account recovery procedure when losing their 2FA mechanism. Of these participants, 80 (56.3%) mentioned recovery codes. Backup of the 2FA app, hardware device or secret key was mentioned by 26 participants (18.3%), while 19 participants (13.4%) stated that they would contact the support. Five participants (3.5%) were unaware on how to recover their account.

Subsequently, we explicitly asked participants about the recovery code and whether they are aware of its usage. This

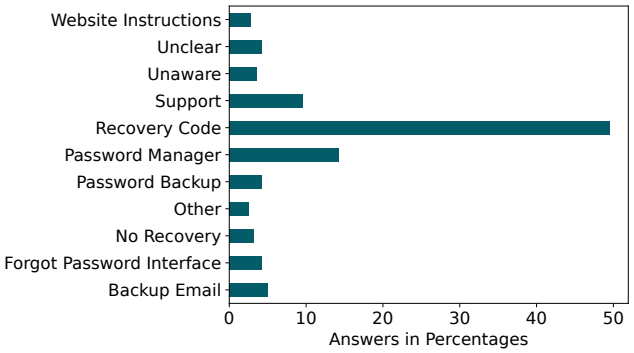

Figure 3: Self-reported strategies of our participants for recovering their account and encrypted data in case of password loss. Not all strategies are applicable for Tuta. They illustrate misconceptions of Tuta users regarding the purpose and the capabilities of the recovery code.

question was answered in the affirmative by 229 participants (81.5%). Further, 26 participants (9.3%) were not sure or denied. We excluded these participants for further questions directly targeted at the recovery code. To investigate participants' comprehension of the importance of the recovery code, we asked whether they believed that Tuta's support team would be able to help with recovery if users lose both password and recovery code. The majority (148, 64.6%) did not believe that the support could help, but 51 (22.3%) were not sure, and 29 participants (12.7%) believed so. All participants who answered the question in the affirmative were asked what they thought could be recovered by the service. Half of those participants (15, 51.7%) selected the ability to use the account's email address, which is at least correct for paying customers that can prove their account ownership. Indeed, eleven of these participants were paying users. However, restoring the mailbox content was selected nine (31.0%) times, restoring list of contacts seven (24.1%) times, and calendar events six (20.7%) times. All of which is not possible. Nine participants (31.0%) were not sure about the question and two (6.9%) stated that none of the above options could be recovered.

To inquire the 281 participants about their threat model and comprehension of the end-to-end encrypted service, we asked who they thought had access to their unencrypted inbox and got diverse answers. While 123 (43.8%) selected that only they have access, 155 (55.2%) believed other institutions or people to have access. Most (65, 23.1%) participants selected law enforcement or intelligence agencies, followed by 55 (19.6%) selecting Tuta, indicating that they do not fully understand the cryptographic implications for Tuta. Only seven (2.5%) selected family or friends, which might be legitimate access, if the password is passed onto them.

Recovery Code Awareness.

- Most participants felt well-informed about account recovery and are aware of the recovery code.
- Participants most often stated to use the recovery code or a password manager in case of password loss, but some also mentioned measures only taken after password loss, e.g. hoping that the support can help.
- About half of our participants believed other authorities to have access to their unencrypted inbox.

Recovery Code Management. The biggest obstacle to using a recovery code is its secure storage without losing it. Therefore, we asked all 229 participants who knew about the recovery code how they handled and stored it after signing up. In 78 cases (34.1%), participants stated that they saved the recovery codes in a password manager. Further digital storage options were saving the recovery code in a file or as PDF (29, 12.7%), including screenshots and photos, or uploading it to a cloud or online storage (9, 3.9%). Further, 19 participants (8.3%) saved the recovery code on other hardware or devices, e.g., a second computer, their server, or a USB stick. Participants also stored the code offline, as 32 (14.0%) wrote it down and 25 (10.9%) printed the recovery code. Only 34 participants (14.8%) mentioned that they saved the recovery code in at least two different locations or utilized more than one strategy, e.g., saving it offline and putting it in a password manager. Seven participants (3.1%) did not write the recovery code down or could not remember anymore. The frequency of all strategies is shown in Figure 4. We could not uncover a strategy for 35 participants (15.3%), as they stated that they copied or saved their recovery code, but were unspecific about the location, e.g., participants often only mentioned a "safe place".

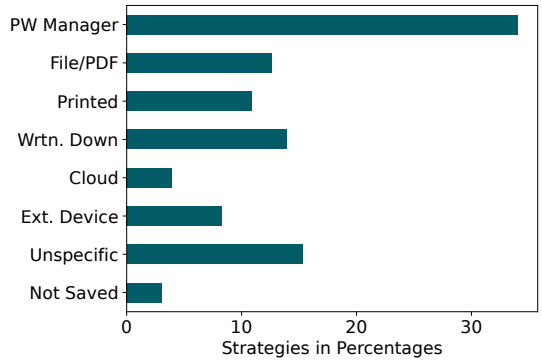

Figure 4: Self-reported strategies of our participants for storing and managing recovery codes for their Tuta accounts. Some participants (34) reported having a backup of the recovery code or using multiple strategies.

Some participants further elaborated on their storage, as 34 participants (14.8%) emphasized that the digital storage location would be encrypted. In the same vein, seven participants (3.1%) tried to somehow obscure the nature of the recovery code, e.g., storing the note of the recovery code without any context, so that a stranger could not recognize its use.

Asking the 229 participants about the time required for

reaching their recover code if needed, most participants (103, 45.0%) stated that they could access their recovery code immediately. Whereas, 64 participants (27.9%) would need up to ten minutes, 19 (8.3%) up to an hour, and eight participants (3.5%) up to five hours. Up to a day or longer was only selected by 19 participants (8.3 %). The distribution of time to access the recovery code across the strategies we uncovered is shown in Figure 5.

Interestingly, when asked if they knew how they could view or regenerate their recovery code in their account, only 145 (63.3%) answered in the affirmative, 84 (36.7%) were not sure or unaware. We consider the latter numbers a great proportion for such a crucial function, possibly indicating that some users only interact superficially with the recovery code.

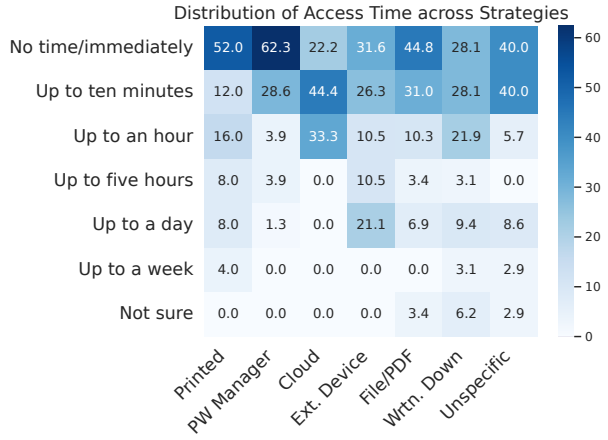

Figure 5: Distribution of time to access the recovery codes based on self-reported data for the six recovery code management strategies we identified. Each row is normalized for all participants who reported a specific strategy. Printing recovery codes on paper or storing them in a password manager provided the fastest accessibility for most participants.

> Recovery Code Management.
>
> - We identified six recovery code management strategies. The most prominent strategy was to store the recovery code in a password manager.
> - Most participants stated that they could access the recovery code immediately or in a very short time.
> - Only 145 of 229 participants knew how to view or regenerate the recovery code in their account.

Recovery Experiences. Most of our participants had not yet tried to recover their Tuta account. Only 29 (10.3%) answered this question in the affirmative. To recover their accounts, 15 of them used a recovery code. Three participants eventually found their password or had it backed up, e.g., in a password manager. One participant reached out to the support, due to being mislabeled as a spammer. Another participant lost their account as they had not accessed their free account for over six months. We could not identify a strategy for three participants. Asked whether their recovery attempt was successful, 20 answered in the affirmative, while seven lost their account, of which two have stated to have entered the recovery code unsuccessfully. One participant was not sure. Two of the participants that lost access regarded the data that was lost as sensible or valuable, three did not, and two were not sure. The emotions from the seven participants without successful account recovery were diverse. One participant stated that they "*Didn't stress over it*" (p232), while other participants, were more frustrated. Two participants elaborated on the problem of being hacked, with no means of getting the account back.

> "*[It] made me realise how dangerous [the] recovery system is, if [the] account gets compromised. No chance of recovery then! End of the Road!*" - p332

We asked all participants who tried to recover their account in the past, successfully or not, whether they changed their strategy. About half of the participants stated that their strategy remained the same. Five participants made sure to back up their password (e.g., in a password manager) or note down their recovery code. Two participants stated that they would be even more attentive. Measures only taken by single participants were the use of their own domain, regular logins, and even the reuse of the password to better remember it. One participant mentioned that they would now rely on another email provider. Participants were also affected in their opinion on Tuta. One participant who could recover their account mentioned that it "*built [their] confidence in [Tuta] and [it was] why [they] eventually switched from free to a subscription*" (p147). Another participant who could not recover their account felt the opposite: "*I don't trust [Tuta] anymore - I only think of it as an ephemeral account that may disappear at any moment.*" (p218)

> Recovery Experiences.
>
> - 29 participants tried to recover their Tuta account, 20 were successful.
> - About half of the 29 participants stated that their strategy changed after the recovery attempt, e.g., they made sure to backup their password.

Opinions on Recovery. We were not only interested in the participant's handling of their recovery code but also in their opinion about it in comparison with other recovery methods. The majority of the 281 participants (198, 70.5%) were satisfied with Tuta's recovery option, 50 participants (17.8%) were neither dissatisfied nor satisfied, and only 16 (5.7%) were dissatisfied. Asked to judge the trade-off made by Tuta's recovery code between privacy and possibly irrevocable access loss, most (185, 65.8%) participants tended to find privacy (considerably) more important to them. Only 33 participants (11.7%) tended to find account access more important and 58 (20.6%) found both equally important. While most participants found privacy more important, nevertheless the consequences of account loss were rated severe by 194 (69%) participants. Only 37 (13.2%) believed them to be minor to none.

To understand the sentiments regarding the recovery code in contrast to other methods, we gave participants a list of recovery methods and asked them to select all of which they have heard of and subsequently to select all that they have used before. In general, participants most often utilized email recovery (232, 82.6%), followed by 195 participants (69.4%) using security questions and 158 (56.2%) using SMS recovery. Critically, previous research has shown that these three methods are all vulnerable [15], [18], [43]. Recovery codes were selected by 154 (54.8%)[3]. The answers are visualized in Appendix Figure 8.

In a follow-up question, we showed all recovery methods that the participant had heard of before and let them order these regarding security. Most participants regarded the recovery code as secure and sorted it into first or second place, as depicted in Figure 6. Only very few participants thought of it as a less secure method. For other methods, participants' voting was diverse, but trusted devices and personal identification also showed a tendency to be regarded as secure. Security questions, email recovery, and SMS recovery were most often considered insecure, but could also be found at the top of the list a few times. When asked to sort these recovery methods for usability, recovery codes did not perform nearly as well. While some participants considered it somewhat usable, others regarded its usability as even less favorable. On the contrary, email recovery followed by trusted devices was regarded as the most usable.

Finding other options more usable, it is not surprising that participants wished for alternatives. Their answers regarding preferences of other recovery methods implemented by Tuta were diverse, as shown in Figure 7. While 66 participants (23.5%) did not want a mechanism other than the recovery code and 14 (5.0%) preferred no recovery at all, preferences by other participants were versatile, with 153 participants (54.4%) wishing for another or additional feature. Most commonly selected were trusted devices by 57 participants (20.3%), email recovery by 49 (17.4%) and security questions by 45 (16.0%). Additionally, participants wished for SMS recovery (35, 12.5%) and personal identification (31, 11.0%).

> Opinions on Recovery.
>
> - Most participants were satisfied with the recovery code.
> - Participants generally rated the recovery code as secure, but not as usable as other methods.
> - About half of our participants wished for alternative recovery options like trusted devices, email recovery, or security questions.

[3] As more participants stated saving their Tuta recovery code in an earlier question than answered in this question to use recovery codes, we assume that participants selected their recovery methods apart from Tuta.

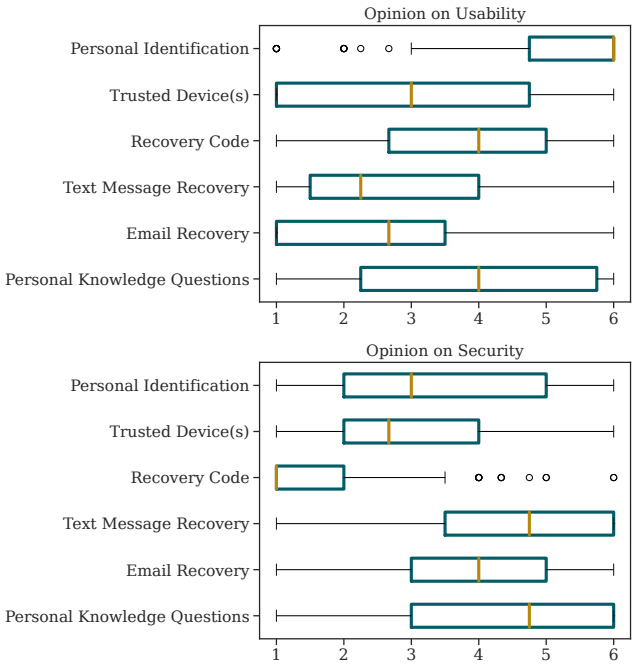

Figure 6: Self-reported usability and security ratings of recovery procedures our participants knew of. A method which was ordered into first place is denoted as 1, a method which was deemed as less secure/usable in comparison to the other methods is denoted as 6.

5.2 Reddit Thread Analysis

Users who lost their Tuta account might not get the newsletter anymore. We indeed found only a few of our survey participants to have lost access to their accounts in the past. Therefore, we conducted a second study, analyzing Reddit threads, to enrich our dataset with user sentiments, obstacles, and misconceptions concerning recovery codes.

Of 233 Reddit threads that were returned searching for "recovery", we found 196 to be related to our research. The relevant posts had a median number of six comments (mean $= 7$, $\sigma = 6$). We found three different themes within the

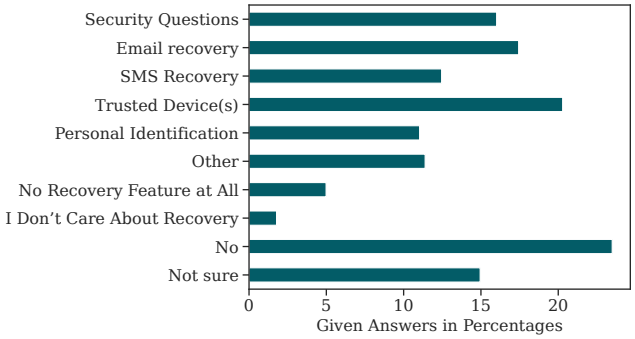

Figure 7: Self-reported preferred alternatives to recovery codes.

threads. First, support requests, mostly consisting of users having trouble during login (148 threads). Second, opinions and sentiments regarding the recovery code deployed by Tuta (24 threads). And third, questions about the recovery code, e.g., about its security (40 threads). The themes could could also co-occur.

Login Problems and Support Requests Most of the threads we found relevant addressed login problems or requests regarding account recovery support. First, 33 thread owners reported that they could not access their accounts shortly after creation. These accounts most likely got blocked, e.g., for spam protection, or as the users defied the terms of services, and were therefore not recoverable by normal means. As this is not indicated during login, to regain access, 18 users stated that they had unsuccessfully tried the recovery code, and only one user stated that they had not written down the recovery code: "*[S]ince I know my credentials, I thought I would never need it.*" (t198)

In addition, 23 threads were created by users that had their free account disabled per Tuta policy, as they did not interact with the account for six months. While most users understood that they lost their account access because of their inactivity, for some users the implications were not clear, e.g., three users stated that they had tried their recovery code without success, while five users stated that they had lost their recovery code. While many of the threads of both aforementioned scenarios mention a recovery code, e.g., a user stating that they could not log in using the recovery code, the account loss had other underlying causes, as the account was blocked or deleted. We will therefore disregard these threads for further analysis.

Since we focus our research on recovery codes, we consider those support requests most relevant that were related to users being unable to access their account due to losing their passwords (53) or recovery codes (48). Both scenarios co-occurred in 37 threads, meaning that the users had lost both. Threads mostly gave no precise information about how users lost their recovery code. If anything was mentioned, it was most often the loss of data, e.g., because of a factory reset or a broken hard drive. A few users stated that they had not saved the recovery code, with one user being sure that they would never lose their password. Another user was uncomfortable with writing the recovery code down and providing "*any kind of access into [their] account for outsiders.*" (t157) Two users lost access as they had trouble with their password manager that they used to store their recovery code and two users were not aware of the existence of a recovery code.

Interestingly, in 31 threads, users still had their recovery code, but asked for help as it was not functioning, while in 18 threads, users reported having trouble with their password. Some users indicated to be sure that they had saved the correct recovery code, or they expressed negative sentiments: "*[W]hy would they provide me with a recovery phrase to keep safe that doesn't work [...]?*" (t116) Two users were confused by the whitespace every four characters when the recovery code was displayed and believed the format to be the problem. Further, two users asked if the recovery code would change after usage or would become invalid with time. One of these two later figured out that they confused "1" and "I" while entering the code.

Table 2: Crosstable for all reported lost or nonfunctional credentials by Reddit users. Some users lost both their passwords and the recovery codes. Some users found that their password or recovery code were non-functional.

	Lost2FA	NonfunctRC	LostRC	NonfunctPW	LostPW
LostPW	1	13	37	0	53
NonfunctPW	0	15	2	18	
LostRC	6	0	48		
NonfunctRC	0	31			
Lost2FA	9				

PW = password, RC = recovery code

Nine users lost their password and 2FA device, or their recovery code and 2FA device, and were thus not able to log in. Co-occurrence between lost and non-functioning credentials can be found in Table 2.

When losing their credentials or finding them non-functional, a few users elaborated on sending proof of their account ownership or the credentials to Tuta, believing that Tuta could reset their account. Further, 17 users, who could no longer log in, still had an active session, e.g., because they were still logged in in the app. They unsuccessfully hoped for means to recover the account or extract their password, as they still had access to their mailbox. Further support requests we found were about help regarding 2FA, lost email addresses, or because the users believed to be hacked.

> Login Problems and Support Requests.
>
> - 148 Reddit threads covered some kind of support requests or login problems.
> - 53 thread owners lost their password and 48 their recovery code, 31 thread owners still had their recovery code, but found it to be non-functional.
> - A few thread owners elaborated on sending ownership proofs to Tuta or hoped that an active session could help with account recovery.

User Opinion. Most of the posts that related to users' opinions on the recovery method discussed its features and technical details. Seven posters mentioned that they would prefer an option to disable recovery altogether. This mostly stemmed from various misconceptions which implied that the existence of a recovery code would compromise security. The mental model some posters seemed to have of a recovery code was that of an additional password that they would have to remember and whose contents they should be in control of:

> "*The user has no control on the length or content of the recovery code while it is essentially an additional password forced on to the user.*" - t233

Other users thought their recovery code would be more prone to being stolen by malware than their password, as the recovery code is displayed on the screen in plain text upon registering a new account. They suggested hiding the recovery code by default and only showing it if the user chooses to. Three posters did not like the idea of there being a second secret, in addition to their password, that is capable of decrypting their private key, thus giving them access to their stored encrypted data.

One user suggested splitting up the recovery code into parts and distributing these code parts amongst trusted people. In a similar vein, six users suggested adding alternatives for the current recovery code, e.g., their proposals comprised security questions, or Tuta sending out recovery emails or SMS, as one user stated:

> "*My best guess for not implementing [additional recovery methods] [...] is due to security concerns, but security means data integrity and availability but in this case I'm loosing both.*" - t226

One poster suggested regular prompts to test the recovery code, so users would not be caught off guard by its loss.

User Opinion.

- We found 24 threads touching upon the posters opinion on the recovery code.
- Seven thread owners wanted to deactivate the recovery code completely.
- Some thread owners suggested adjustments to the recovery code or alternative recovery options.

Questions and Comprehension. We identified several misconceptions in the threads of 20 users, often related to implementation details and handling of the recovery code, e.g., a user trying to create a recovery code manually and asking about the rules for creation, a user stating that they never set a recovery code, or another user believing that they need the recovery code to change their password.

Regarding questions, ten users asked questions regarding the security of the recovery code. Recurring questions were whether a password change automatically triggers the creation of a new recovery code, and how the recovery code is stored, including concerns that Tuta had access to it.

Moreover, 14 thread owners asked about how to locate and re-access the recovery code in their accounts. Reasons to access the recovery code were, e.g., not writing down their recovery code at account creation or losing their copy of the recovery code. One user asked if the recovery code could be reset, as they opened their copy within an untrusted program, or if they could otherwise delete their account and register a new one.

Questions and Comprehension.

- We found 40 threads containing misconceptions or comprehension questions.
- Thread owners had several misconceptions or questions regarding creation and functionality of the recovery code, e.g., 14 thread owners asked how to re-locate the recovery code.

6 Discussion

In this section, we discuss our findings in the context of our participants' security comprehension of recovery codes, the sentiments about recovery, and our research questions.

6.1 Misconceptions Around Account Recovery

Tuta is an email provider focusing on security-savvy users with a high need for data privacy. Hence, our participants likely represent an upper bound regarding security and privacy awareness and needs. However, we argue that security awareness does not necessarily imply a better understanding of underlying security mechanisms. While security was important for most participants, we found that not all participants had a detailed understanding of the provided security features. This was even more obvious in the Reddit discussions, where we found various misconceptions regarding account recovery. While both studies suggest that at least some of the Tuta users aimed for a trustworthy or secure solution, not all understood the cryptographic implications. Our findings are consistent with a study from Usman *et al.*, that conducted an interview study with users of the end-to-end encrypted email service Proton Mail. They found that about half of all participants were unaware of how Proton Mail secures the user data but placed their trust in the provider's security [44].

We assume that the usage frequency and motivation with which the email service is used might impact the users' understanding or behavior in the context of recovery codes. While we invited our survey participants through the email service's newsletter, leading to potentially more interested and active users, the Reddit threads, also comprised of inactive users, resulted in novel misconceptions or obstacles.

6.2 RQ1: "Are users aware of the existence and importance of recovery codes?"

Most users in our survey reported being aware of the recovery code and felt well-informed about account recovery. However, their awareness of the recovery code was sometimes only superficial, as many users did not know how to regenerate it, and several Reddit threads indicated that users lost their recovery code. Users could be easily misled in their assessment because the recovery code does not influence their daily life. They might engage with the code only once while saving it and never question any details or forget its location afterward.

Moreover, some users thought they could not lose their password at all. This overconfidence could lead to a decreased awareness of their recovery code.

Another important aspect is that users already had previous experiences with account recovery processes. Some survey participants stated they would use backup email or security questions to recover their account, although Tuta does not deploy these options. Similarly, survey participants and Reddit users hoped the support could help them regain access or stated they would use the "forgot password" button to recover their accounts and data. These results illustrate that some users have a pre-formed understanding of account recovery that can even superpose their actual experiences while setting up their Tuta account. Ultimately, these users are not aware of the true criticality of their recovery code as the only recovery feature, if they are aware of the recovery code at all.

To make matters worse, some users struggled to understand the implication of using an end-to-end encrypted service, as they erroneously thought that Tuta could access their unencrypted mailbox, making a recovery without providing a recovery code only dependent on the graciousness of the support. This sentiment is reinforced by the use of the term recovery code across various websites, but normally with different nuances, e.g., users often get several recovery codes that can only be used once before they are invalid. Two studies from Gerlitz *et al.* and Amft *et al.* both investigated MFA recovery features deployed on popular services [10], [11]. While they found that recovery codes were a frequent 2FA recovery feature, for many services they could regain access without having the recovery code, even if websites stated otherwise. Such variation in the implementation of recovery codes can contribute to users' confusion about a recovery code's concrete capabilities and functionalities. Especially for users who do not understand the encryption scheme of a service, these findings can endorse their belief that storing the recovery code is not that important, as account access can be regained anyway. Hence, we strongly suggest explaining the principle of account recovery sufficiently and emphasizing when a recovery code is the only option to regain access to the account or data, e.g., by an additional popup that has to be confirmed.

6.3 RQ2: "What strategies for handling recovery codes do users employ?"

We identified six recovery code management strategies, utilizing digital and analog storage options. Most often, participants stored the recovery code inside a password manager. Some participants also indicated that they have a backup of the recovery code, usually implying that they utilized at least two of the six strategies.

All six recovery code management strategies have different advantages and disadvantages regarding confidentiality, integrity, and availability. In the recovery code context, confidentiality means protecting against unauthorized access, i.e., from strangers or close relatives, and against phishing and hacking. Integrity implies the protection against transmission errors, e.g., typos. Availability means that the user can easily access the recovery code and does not lose it. Moreover, the recovery code should still function as a password backup, meaning the recovery code and password are in different places. Especially since, in our case, recovery codes are the last option to decrypt the mailbox when users lose access to their passwords.

We assume the password manager is a secure place that protects the recovery code against (most) unauthorized access, yielding good confidentiality. The availability must be viewed in a more differentiated manner: If users need their recovery code, they can easily find and use it and will likely have a backup of their password manager. However, the password and recovery code are in the same place. If users lose access to their password, they also lose access to their recovery code. If the second factor is not stored in the password manager, the recovery code can still operate as a 2FA backup, but also weakens the 2FA security policy. An adversary with access to the password manager does not need the second factor.

Other participants stored the recovery code as a (PDF) file. Compared to a password manager, a file might have more disadvantages in terms of confidentiality and availability. Storing the recovery code as an image also reduces integrity, as typos can be made when typing out the code. Users can store the file on a separate device, e.g., a USB stick, but finding the device with the recovery code later may prove more complicated. Moreover, the storage on which the recovery code is saved might break or be lost. To strengthen confidentiality, the recovery code can be encrypted. However, users would need to store and back up the decryption key.

A file or even the password manager stored in the cloud has advantages for availability but raises alarm bells for the confidentiality of the recovery code. Especially a recovery code as an image can easily be uploaded to the cloud by accident. E.g., the Photos app stores photos on Apple devices. Users must remember that the recovery code is in the Photos app when activating the iCloud for photos, or the image of the recovery code is automatically stored in iCloud [45]. Storing recovery code in the cloud requires an individual and carefully considered risk analysis.

Moreover, all previously mentioned strategies are also (in various dimensions) prone to digital adversaries. Circumventing this, some participants kept a paper version of the recovery code, utilizing one of the two strategies to write it down or print it. On the one hand, this strategy can protect the recovery code against strangers' attacks and digital adversaries, leading to some advantages for confidentiality. On the other hand, users might be vulnerable to close relatives or physical threats. Users must be organized to find the location of their recovery code after a long time, making availability critical. If users write down the code, they might make typos and irretrievably

destroy the integrity. As with images, typos can also occur while entering the code during the recovery process.

Critically, as we have just discussed, none of the six strategies is flawless. As a password manager has many advantages, it might be sensible to utilize this strategy, but only if a backup of the password manager or the recovery code is stored in a different location. However, weighing all strategies against each other and considering the individual circumstances is a burden for the user and a non-trivial problem. We assume users might choose a suboptimal solution if their threat model is underdeveloped.

6.4 RQ3: "What obstacles do users face when using recovery codes?"

While most of our participants were satisfied with the recovery code, we observed several obstacles, especially in the Reddit posts. Several users lost their recovery code, often together with their password, making account recovery impossible. Two users lost account access as they had problems with their password manager, demonstrating that this is a realistic scenario and rendering backups particularly important. In this context, it is important to consider that a proprietary backup of the password manager is of no use if, e.g., the user has forgotten their master password.

Moreover, some users found their recovery code to be non-functional. For a start, it is opaque for users whether the account is blocked, deleted, or they have forgotten their password, as they are only shown that they have entered invalid login credentials. The recovery code is not designed to help with blocked or deleted accounts. It just appears to be non-functioning, but because of users' lack of situational awareness, it can still cause frustration. We also found less clear causes for a non-functional recovery code. We assume that users made mistakes transferring their codes, which is especially likely if they wrote down their code by hand, as it is long and unwieldy. Moreover, one Reddit user mistook letters in the recovery code for one another. Other Reddit users were confused by the whitespace after every fourth letter. While this representation renders the code easier to read, it also illustrates the importance of presenting the recovery code in an unambiguous format with sufficient explanation. Simple measures like an easy-to-read font might help distinguish all letters clearly. Furthermore, we suggest exploring the option of testing the recovery code every so often, an approach, e.g., deployed by Signal for their PIN [46]. Currently, many users only interact with the recovery code once and only find out too late if they have lost their code or copied it wrong, which might be prevented by those reminders. In this vein, promising results were found by Bailey *et al.* Their study about Signal PINs indicated that 76% of their participants kept the feature enabled, and many at least occasionally tested their PIN [47].

In some cases, understanding of the recovery scheme was also a problem. A few Reddit users had questions regarding the security or distrusted the recovery code in such a way that they did not only not save the code but even would have liked the feature removed. They found the risk of storing their recovery code too high, fearing to compromise their privacy or security. For some, their distrust and lack of understanding of the recovery feature extended to distrust of the service. While Tuta discloses their implementation of security mechanisms, this seems not to reach all users. As Usman *et al.* found that mental models for security mechanisms for users of secure email providers were often at most vague, it is important to reach those users with simple and comprehensible communication [44]. Moreover, it would be worthwhile to explore possibilities to diminish misunderstandings and build trust by, e.g., letting trusted entities verify the recovery scheme.

6.5 User Sentiments towards Recovery

For a successful deployment of a recovery scheme, user sentiments are crucial. Our survey participants were generally satisfied with the recovery code approach and liked the trade-off between security and the possibility of regaining account and data access. They knew an account loss would have severe consequences but rated privacy as more important. However, it is also evident that recovery codes were not regarded as the most usable tools. Moreover, some of the survey and Reddit users who lost their accounts expressed quite negative sentiments, especially when they did not understand why their recovery code seemed to be non-functional. Contrary to previous research findings that poor usability can significantly restrict the adoption of security tools [48]–[51], we conclude that Tuta users were mostly fine with the overhead of storing the code – if it was functional and locatable when needed.

Still, bad usability might incite users to use less secure mechanisms against their better judgment when not forced to use a secure recovery method. We observed that many of our survey participants wished for alternatives for the recovery code, including insecure security questions, email, and SMS recovery. Trusted devices, however, were the most desired. Many participants regarded them as secure and quite more usable than recovery codes. An advantage of trusted devices is that they can be used just like recovery codes for encrypted services, e.g., the password manager LastPass deploys an approach where a recovery code is generated and saved on a trusted device or browser without the users' intervention [52]. As various websites deploy different approaches for trusted devices, it is worthwhile to conduct further research and investigate their implementation and security.

6.6 Generalizability

Our study is limited to end-users using Tuta, thus, our findings are not generalizable without further ado. Still, we assume that the user base of different secure mail services is generally similar. We confirmed some of the findings reported by

Usman *et al.* in their study on Proton Mail users, e.g., we also observed our participants to be generally wary or privacy affine [44]. Compared to conventional mail services, secure mail providers are only a niche. But they still have millions of users and their user bases are growing [53], [54].

While we argue that deploying recovery codes as a decryption key fallback will mostly affect security-savvy users and therefore reflect our user base, recovery codes are also often used for 2FA recovery. 2FA is targeted at the average user, with various websites nowadays strongly encouraging or even enforcing 2FA [55], [56], thus, rendering it an increasingly important topic. Therefore, our results should be probed in future work for a more general end-user sample. We assume that less tech and security-savvy users would use other strategies than the password manager more often, as the general adoption is less common [48], [57], [58]. One study indicated, that users might rather utilize the strategies of taking a photo with their cell phone or writing the code down. [59]. It is also possible that a greater proportion might not save the recovery code at all.

Further, we found similarities to cryptocurrency wallets, as seed phrases utilized in this context can take a similar function to recovery codes. Previous research indicates, that not all users are aware of the importance of their recovery information or know about its functionality, similar to our findings. For mobile cryptocurrency wallets, Voskobojnikov *et al.* found that some users lost or never saved their seed phrase or were unsure how to use it [60] and Krombholz *et al.* found that many users did not back up their crypto wallet or were not aware whether they had a backup [61]. Research also indicates that better guidance is needed to support those users [62].

7 Conclusion

We conducted a mixed-method study about recovery codes deployed by an end-to-end encrypted email provider. We surveyed 281 users and analyzed 196 Reddit threads. Most of our participants knew the recovery code and were willing to use it. They were generally satisfied with the recovery code and appreciated it for its security, but found its usability lacking. We identified six different strategies for storing recovery codes. While saving the recovery code in a password manager was most common, we found none of the strategies to be optimal for confidentiality, integrity, and availability. Moreover, a lack of understanding of the cryptographic implementation could hamper user behavior or cause distrust. We also found some obstacles, e.g., participants lost their recovery code or found it non-functional. Since a loss of the recovery code has severe consequences for users of end-to-end encrypted services, we recommend more research to better support users with the recovery process and how to store their recovery code.

Acknowledgments

We would like to thank all of our participants for partaking in our survey. We also thank the anonymous reviewers for their valuable feedback. In loving memory, the first author wants to thank August Boldering for his steady help and treasured support over all the years. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

Financial Conflicts

Arne Möhle is CEO of Tuta. While Arne was involved in motivating this work, formulating research questions, and the study design and piloting, he did neither contribute to the data analysis, nor the results, discussion, or conclusion writing.

Availability

To improve the reproducibility of our work, we provide a replication package containing our codebooks, the survey questions, and a list of the Reddit posts we analyzed. Please find the replication package at: https://doi.org/10.25835/wasieu9f.

References

[1] *Secure email: Tutanota free encrypted email.* https://tutanota.com/, Accessed: 2023.

[2] *Proton Mail: Get a private, secure, and encrypted email account | Proton*, https://proton.me/, Accessed: 2023.

[3] *#1 Password Manager & Vault App with Single-Sign On & MFA Solutions - LastPass*, https://www.lastpass.com/, Accessed: 2023.

[4] *Security - KeePass*, https://keepass.info/help/base/security.html#secdictprotect, Accessed: 2023.

[5] *Password Manager for Families, Businesses, Teams | 1Password*, https://1password.com/, Accessed: 2023.

[6] B. Kaliski, *PKCS# 5: Password-Based Cryptography Specification Version 2.0*, 2000.

[7] N. Provos and D. Mazières, "A Future-Adaptable Password Scheme," in *USENIX Annual Technical Conference, FREENIX Track*, USENIX, 1999.

[8] C. Percival and S. Josefsson, *The scrypt Password-Based Key Derivation Function*, 2016.

[9] A. Biryukov, D. Dinu, D. Khovratovich, and S. Josefsson, *Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications*, 2021.

[10] E. Gerlitz, M. Häring, C. T. Mädler, M. Smith, and C. Tiefenau, "Adventures in Recovery Land: Testing the Account Recovery of Popular Websites When the Second Factor is Lost," in *Proc. 19th Symposium on Usable Privacy and Security (SOUPS'23)*, USENIX, 2023.

[11] S. Amft, S. Höltervennhoff, N. Huaman, *et al.*, ""We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments," in *Proc. 30th ACM Conference on Computer and Communication Security (CCS'23)*, ACM, 2023.

[12] *What is a Recovery Code and why it's important?* https://support.nordpass.com/hc/en-us/articles/360002445318-What-is-a-Recovery-Code-and-why-it-s-important-, Accessed: 2023.

[13] *Keep Your Dashlane Account Safe with a Recovery Key*, https://www.dashlane.com/blog/dashlane-account-recovery-key, Accessed: 2023.

[14] *Set account recovery methods in case you forget your Proton password*, https://proton.me/support/set-account-recovery-methods, Accessed: 2023.

[15] Y. Li, H. Wang, and K. Sun, "Email as a Master Key: Analyzing Account Recovery in the Wild," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, IEEE, 2018.

[16] K. Lee and A. Narayanan, "Security and Privacy Risks of Number Recycling at Mobile Carriers in the United States," in *2021 APWG Symposium on Electronic Crime Research (eCrime)*, IEEE, 2021.

[17] K. Lee, B. Kaiser, J. Mayer, and A. Narayanan, "An Empirical Study of Wireless Carrier Authentication for SIM Swaps," in *Proc. 16th Symposium on Usable Privacy and Security (SOUPS'20)*, USENIX, 2020.

[18] J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, "Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google," in *Proceedings of the 24th International Conference on World Wide Web*, 2015.

[19] J. Rossignol, *Apple Responds to Report About Thieves Permanently Locking Out iPhone Users*, https://www.macrumors.com/2023/04/19/apple-responds-to-iphone-theft-recovery-key-report/, Accessed: 2023.

[20] *About account security*, https://help.twitter.com/en/safety-and-security/account-security-tips, Accessed: 2023.

[21] *I can't log in*, https://help.instagram.com/374546259294234/?helpref=hc_fnav, Accessed: 2023.

[22] *How do I log in to Reddit if I forgot my password and haven't set up an email address?* https://support.reddithelp.com/hc/en-us/articles/360043047152-How-do-I-log-in-to-Reddit-if-I-forgot-my-password-and-haven-t-set-up-an-email-address-, Accessed: 2023.

[23] *Your Keybase Account*, https://book.keybase.io/account, Accessed: 2023.

[24] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: somebody you know," in *Proc. 13th ACM Conference on Computer and Communication Security (CCS'06)*, ACM, 2006.

[25] S. Schechter, S. Egelman, and R. W. Reeder, "It's Not What You Know, but Who You Know: A Social Approach to Last-Resort Authentication," in *Proc. CHI Conference on Human Factors in Computing Systems (CHI'09)*, ACM, 2009.

[26] A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook," in *Proc. 4th Symposium on Usable Privacy and Security (SOUPS'08)*, USENIX, 2008.

[27] A. Hang, A. De Luca, E. Von Zezschwitz, M. Demmler, and H. Hussmann, "Locked Your Phone? Buy a New One? From Tales of Fallback Authentication on Smartphones to Actual Concepts," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, ACM, 2015.

[28] V. Stavova, V. Matyas, and M. Just, "Codes v. People: A Comparative Usability Study of Two Password Recovery Mechanisms," in *Information Security Theory and Practice*, Springer, 2016.

[29] S. Parkin, S. Driss, K. Krol, and M. A. Sasse, "Assessing the User Experience of Password Reset Policies in a University," in *Technology and Practice of Passwords*, Springer, 2016.

[30] J. H. Huh, H. Kim, S. S. Rayala, R. B. Bobba, and K. Beznosov, "I'm too Busy to Reset my LinkedIn Password: On the Effectiveness of Password Reset Emails," in *Proc. CHI Conference on Human Factors in Computing Systems (CHI'17)*, ACM, 2017.

[31] F. A. Maqbali and C. J. Mitchell, "Web Password Recovery: A Necessary Evil?" In *Proceedings of the Future Technologies Conference (FTC) 2018*, Springer, 2019.

[32] L. Neil, E. Bouma-Sims, E. Lafontaine, Y. Acar, and B. Reaves, "Investigating Web Service Account Remediation Advice.," in *Proc. 17th Symposium on Usable Privacy and Security (SOUPS'21)*, USENIX, 2021.

[33] S. Ghorbani Lyastani, M. Backes, and S. Bugiel, "A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites," in *Proc. 30th Annual Network and Distributed System Security Symposium (NDSS'23)*, The Internet Society, 2023.

[34] A. Javed, D. Bletgen, F. Kohlar, M. Dürmuth, and J. Schwenk, "Secure Fallback Authentication and the Trusted Friend Attack," in *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, IEEE, 2014.

[35] M. Guri, E. Shemer, D. Shirtz, and Y. Elovici, "Personal Information Leakage During Password Recovery of Internet Services," in *2016 European Intelligence and Security Informatics Conference (EISIC)*, 2016.

[36] N. Gelernter, S. Kalma, B. Magnezi, and H. Porcilan, "The Password Reset MitM Attack," in *Proc. 38th IEEE Symposium on Security and Privacy (SP'17)*, IEEE, 2017.

[37] S. Presser, M. P. Couper, J. T. Lessler, *et al.*, "Methods for Testing and Evaluating Survey Questions," in *Methods for Testing and Evaluating Survey Questionnaires*. John Wiley & Sons, Ltd, 2004, ch. 1, pp. 1–22.

[38] J. Corbin and A. Strauss, "Grounded theory research: Procedures, canons and evaluative criteria," *Qualitative Sociology*, vol. 13, no. 1, pp. 3–21, 1990.

[39] K. Charmaz, *Constructing Grounded Theory*. SAGE Publications, 2014.

[40] A. Strauss and J. M. Corbin, *Grounded theory in practice*. SAGE Publications, 1997.

[41] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice," *ACM on Human-Computer Interaction*, vol. 3, no. CSCW, 72, pp. 1–23, 2019.

[42] E. Kenneally and D. Dittrich, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," *SSRN Electronic Journal*, 2012.

[43] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon, "Mind your SMSes: Mitigating social engineering in second factor authentication," *Computers & Security*, vol. 65, pp. 14–28, 2017.

[44] W. Usman, J. Hu, M. Wilson, and D. Zappala, "Distrust of big tech and a desire for privacy: Understanding the motivations of people who have voluntarily adopted secure email," in *Proc. 19th Symposium on Usable Privacy and Security (SOUPS'23)*, USENIX, 2023.

[45] *Set up and use iCloud Photos*, https://support.apple.com/en-us/108782, Accessed: 2024.

[46] *Signal PIN*, https://support.signal.org/hc/en-us/articles/360007059792-Signal-PIN, Accessed: 2023.

[47] D. V. Bailey, P. Markert, and A. J. Aviv, ""I have no idea what they're trying to accomplish:" Enthusiastic and Casual Signal Users' Understanding of Signal PINs," in *Proc. 17th Symposium on Usable Privacy and Security (SOUPS'21)*, USENIX, 2021.

[48] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, "Why people (don't) use password managers effectively," in *Proc. 15th Symposium on Usable Privacy and Security (SOUPS'19)*, USENIX, 2019.

[49] S. Das, G. Russo, A. C. Dingman, J. Dev, O. Kenny, and L. J. Camp, "A Qualitative Study on Usability and Acceptability of Yubico Security Key," in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, ACM, 2018.

[50] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *Proc. 8th Usenix Security Symposium (SEC'99)*, USENIX, 1999.

[51] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons, *Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client*, arXiv preprint arXiv:1510.08555, 2016.

[52] *What is a Recovery One Time Password in LastPass?* https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/FAQ_ROTP.html&_LANG=enus, Accessed: 2023.

[53] A. Yen, *There are now over 100 million Proton Accounts*, https://proton.me/blog/proton-100-million-accounts, Accessed: 2024.

[54] *Celebrate with us: Tutanota reaches 10 million users!* https://tuta.com/blog/10-million-users, Accessed: 2024.

[55] *Protecting your personal info with 2-Step Verification*, https://support.google.com/accounts/answer/10956730?hl, Accessed: 2024.

[56] N. Gleicher, *Expanding Facebook Protect To More Countries*, https://about.fb.com/news/2021/12/expanding-facebook-protect-to-more-countries/, Accessed: 2024.

[57] I. Ion, R. Reeder, and S. Consolvo, ""...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices," in *Proc. 11th Symposium on Usable Privacy and Security (SOUPS'15)*, USENIX, 2015.

[58] N. Alkaldi and K. Renaud, "Why do people adopt, or reject, smartphone password managers?" In *Proc. 1st European Workshop on Usable Security (EuroUSEC'16)*, The Internet Society, 2016.

[59] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A Usability Study of Five Two-Factor Authentication Methods," in *Proc. 15th Symposium on Usable Privacy and Security (SOUPS'19)*, USENIX, 2019.

[60] A. Voskobojnikov, O. Wiese, M. Mehrabi Koushki, V. Roth, and K. (Beznosov, "The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets," in *Proc. CHI Conference on Human Factors in Computing Systems (CHI'21)*, ACM, 2021.

[61] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, "The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy," in *International Conference on Financial Cryptography and Data Security*, 2016.

[62] A. Mai, K. Pfeffer, M. Gusenbauer, E. Weippl, and K. Krombholz, "User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach," in *Proc. 16th Symposium on Usable Privacy and Security (SOUPS'20)*, USENIX, 2020.

A Appendix

A.1 Measurement of User Behavior

A.1.1 Measurement Methodology

In order to gain initial insights into how users interact with recovery code reminder dialogs, we performed a small measurement study with users of Tuta. We required that users of the service explicitly opt in to interaction data collection before any of their data would be sent to the servers.

For the study, a dialog, prompting to write down the recovery code, is presented in the user's newsfeed after the first log-in to the app or after first logging in since the dialogue's creation. Our measurement approach could not differentiate between newly registered and returning users. The dialog text states that the recovery code is the only option to reset the password or second factor in case of their loss. If the user clicks "Display recovery code", they are prompted to enter their password. The recovery code is then shown alongside three actions as depicted in Figure 1.

Each of the action buttons records an extra interaction on the server to be able to measure how exactly users interact with their recovery code. The "Copy" button copies the recovery code to the clipboard for the user to paste it anywhere, e.g., into a password manager entry. The "Print" button opens the platform's print dialog for the user to print their recovery code and store it physically. This action is not available in the service's mobile apps. If the user manually selects the recovery code, this is also recorded as an action, as it likely means that they are going to copy it to their clipboard as well. Lastly, the "Confirm" button acknowledges and closes the dialog, after which it is not shown to the user again.

A.1.2 Measurement Results

During the time-frame of our measurement, 56.790 users that agreed to the data collection and that logged-in to Tuta or created a new account opened the newsfeed of their mail account. They thus were shown the recovery code reminder dialog. From those, 32.784 users clicked on the dialog button and entered their password to display a pop-up with their recovery code. 9.396 users closed the dialog directly. The rest did not interact with the dialog. As our measurement not only included new users but also existing users, they might have already saved their recovery code before.

From the 32.784 users that opened the pop-up to display their recovery code, 7.546 users opted to copy the code to the clipboard, probably to paste and store it into some file or password manager. Apart from this, we measured 2.136 users selecting the recovery code. It is likely, that some of these selection-processes were aimed to copy the recovery code and save it to a place of the user's trust. Further, 1.873 users clicked on the dialog button to print and physically save their recovery code. After finishing their task, 28.093 users clicked on the confirm button and thus left the dialog.

A.2 Figures

Type of Document	Value	Percent
Confidential/Sensitive Work-Related Documents	65	26.75%
Scans of Identification Documents	82	33.74%
Salary/Income Related Documents	82	33.74%
Tax Related Documents	73	30.04%
Health Related Documents	79	32.51%
Contract Documents	74	30.45%
Time-Critical Files	44	18.11%
Receipts	133	54.73%
Log-in Related (e.g., One-Time PWs, Log-in Links)	81	33.33%
Calendar Events	88	36.21%
Contact Information	119	48.97%
Credentials	49	20.16%
Coupons, Vouchers, Keys	55	22.63%
Other	17	7.00%
Not Sure	5	2.06%

Table 4: The general storage of critical data inside a Tuta account has varied between participants, 95 participants (33.9%) reported storing none or only little, 100 (35.6%) stored some, and 74 (26.4%) much critical data. Participants selected a multitude of options on what type of critical data they process or store in their Tuta account. Most often, they selected to process or store receipts, like invoices or delivery receipts, and contact information.

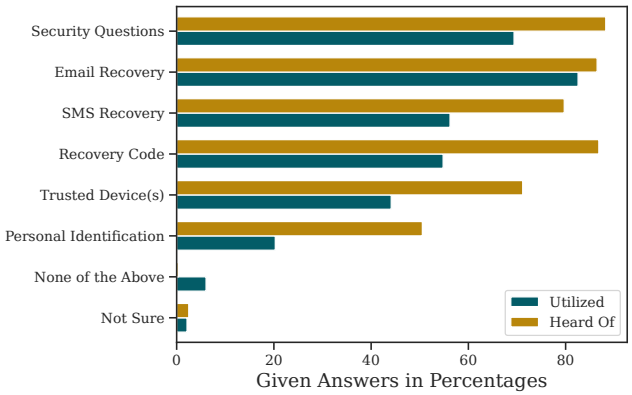

Figure 8: The participants selected all recovery methods that they had heard of before and that they had already used themselves. Altogether, most participants (110, 39.1%) have heard of all six or at least five methods (77, 27.4%). Further, 41 participants (14.6%) heard of at least four methods and 44 (15.7%) of three or less.

Demographics	Value	Percent
Gender:		
Man	211	75.1%
Woman	37	13.2%
Genderqueer	8	2.8%
Age:		
18-24 Years	40	14.2%
25-34 Years	83	29.5%
35-44 Years	51	18.1%
45-54 Years	46	16.4%
55-64 Years	24	8.5%
64 and Older	21	7.5%
Education:		
Bachelor Degree	89	31.7%
Master Degree	80	28.5%
Secondary School	33	11.7%
Trade/Technical/Vocational	19	6.8%
Associate Degree	7	2.5%
Professional/Doctoral Degree	27	9.6%
Other	9	3.2%
Employment:		
Employed Full-Time	126	44.8%
Employed Part-Time	12	4.3%
Self-Employed/Freelancer	37	13.2%
Out of Work	21	7.5%
Student	35	12.5%
Retired	20	7.1%
Other	11	3.9%
Start with Tuta		
Up to One Month	8	2.8%
Up to Six Months	27	9.6%
Up to One Year	55	19.6%
Up to Four Years	137	48.8%
Longer Than Four Years	46	16.4%
Not Sure	5	1.8%
Usage Frequency		
Daily	175	62.3%
4-6 Times a Week	52	18.5%
2-3 Times a Week	20	7.1%
Once a Week	17	6.0%
Once a Month	8	2.8%
Less Than Once a Month	3	1.1%
Not Sure	2	0.7%
Payment		
Paid Account	201	71.5%
Free Account	77	27.4%
Not Sure	1	0.4%
MFA Usage		
Yes	142	50.5%
No	127	45.2%
Not Sure	7	2.5%
Usage Areas (Multiple Choice)		
Everyday Communication	189	67.3%
Work	69	24.6%
Sending Confidential Documents	111	39.5%
Receiving Confidential Documents	115	40.9%
Signing into Sensitive Services	131	46.6%
Manage Calendar Events/Invites	70	24.9%
Manage Contacts	57	20.3%
Other	24	8.5%
Not Sure	2	0.7%

Table 3: Extended demographics for all 281 valid participants from the survey study with Tuta users.