Adventures in Recovery Land: Testing the Account Recovery of Popular Websites When the Second Factor is Lost

Eva Gerlitz
Fraunhofer FKIE

Maximilian Häring
University of Bonn

Charlotte Theresa Mädler
University of Bonn

Matthew Smith
University of Bonn, Fraunhofer FKIE

Christian Tiefenau
University of Bonn

Abstract

Literature on two-factor authentication (2FA) lists users' fear of losing the second factor as one major constraint on acceptability. Nonetheless, more and more services offer or even enforce 2FA. Yet, little is published about what services do to prevent users from losing access to their accounts and how well users are guided through the process of regaining access to their accounts in case they lose their second factor. To fill this gap, we set up 2FA on 78 popular online services and apps and analyzed their user interface during the 2FA setup and recovery. Although there is no straightforward solution for account recovery when using a second factor, we identified easily fixable usability flaws. For example, in the setup phase, 28 services do not mention the possibility of losing the second factor at all. Furthermore, while it is common for services to provide a clearly visible "forgotten password"-link beneath the login field, an equivalent for 2FA is often missing, and a user is left alone with the problem. Our study provides insights for website designers and security practitioners seeking to enhance the usability of 2FA. We also discuss further directions for research.

1 Introduction

Two-factor authentication (2FA) is one powerful solution to improve account security. In 2FA, a second factor (*secondary authenticator*) is needed to confirm the user's identity. Typically, this second factor is something the user *is* or *has* [21]. This is used in addition to the *primary authenticator*, typically something the user *knows*.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

Using such a second factor is one of the most frequently given advice experts give non-tech-savvy users to stay safe online [5, 24], and indeed, the use of 2FA rose steadily over the last years [7]. Some services even force users to secure their accounts with second factors [19] or are required by law to do so, e.g., banking websites in the EU [34].

To understand the consequences of this additional security mechanism from the users' perspective, several studies examined the usability of (possible) second factors (e.g., [1,8,30,38,39]), their initial setup (e.g., [2,10,39]) , or looked at the acceptability of 2FA (e.g., [9, 10, 39, 43]).

Within these studies, participants repeatedly expressed the fear of losing the second factor [10, 25, 35] and statistics indicate that around 40% of smartphone users have had at least one incident in which they lost their device or had it stolen [3, 23, 27]. Considering that the personal smartphone is a convenient choice for 2FA [41], these numbers indicate that many users might find themselves in a situation where they no longer have access to their second factor and therefore be locked out of their account. The consideration of being locked out of a personal account can lead to a low acceptance of 2FA [10]. However, little work has been conducted to understand how services deal with the threat of their users being locked out.

In this work, we want to understand how websites and apps, as one major use case for 2FA, guide a user through the *setup* of 2FA and the *recovery* after losing the second factor. Specifically, we were guided by the following research questions:

RQ1: (How) do popular services communicate the issue of losing the second factor to their users? I.e., do they communicate the issue? Do services encourage users to set up another factor as a backup? Do they provide backup codes? Is the user forced to do something, e.g., downloading backup codes?

RQ2: How well are users supported through the services' recovery protocol when they try to log in but the second factor is lost? I.e., do users receive help during login if their second factor is not accessible anymore? What are

their options?

RQ3: What information do users need to provide to regain access to accounts? I.e., is personal identification needed? Does the user need to have information about the account's activities?

To answer the research questions, we conducted 78 expert reviews that focused on the current practice of online services. We created accounts, enabled 2FA, and analyzed the services' way of informing the user about the possible risks of enabling 2FA and what a user can do to mitigate them. We then ran through the account recovery processes without the second factor and without backup codes. We captured how the service led through this process, what was needed to recover the account, and whether recovery was possible at all.

Overall, we were able to gain access to half of the accounts. This low number might be well explained by security reasons but indicates that users' naive assumptions when they lose their second factor should not be that they could regain access as easily as they would in the case of a forgotten password.

Our results show that the investigated services do not share a common practice, neither during 2FA setup nor during recovery. Looking at the setup, 20.5% of the services do not seem to provide any backup possibilities at all; on the other hand, 20.5% of the services force the user to implement a fallback for the second factor or download backup codes. Only 12.8% of the services clearly communicate that the user will lose access to the account without the second factor or access to fallback authentication.

The same heterogeneity applies to the process of *recovery*: 19.2% of the services offer the user to use backup codes or alternative ways to receive the needed code during login and additionally link to a direct contact possibility if backups do not work either. On the other side of the spectrum, 17.9% of the services do not help the user at all during login, and the only possibility a user has is to cancel their login attempt and try to find a solution on their own (e.g., by looking at the website's FAQs).

Several of the issues we identified can easily be fixed. We suggest establishing a more standardized approach to 2FA setup and recovery to ensure convenience for their users without impacting security.

2 Related Work

This section summarizes work relevant to our study. We first look at the motivation of our work and the frequency users lose a second factor, followed by studies that analyzed the protocols of different aspects of account recovery on websites.

2.1 Losing Access by Losing a Second Factor

The fear of losing a device that is needed to log in, e.g., as a second factor, and losing access to the account, in general, is mentioned as one major constraint on the acceptability of 2FA in several studies (e.g., [10, 13, 25, 35]). Sometimes, this is accompanied by the fear of impersonation attacks after the loss or theft of this device [35]. Despite this fear, the results of a study by Das et al. [10] indicate that websites might not communicate the issue of loss well during the setup process: Participants were requested to add a security key to their email accounts and were explicitly asked what they would do if they lost the key afterward. Almost a fourth of the participants did not know how to recover this newly set up Yubikey in case it got lost or stolen. Yet, we are unaware of any study investigating how websites communicate a potential loss during login and whether users are nudged or forced to set up another factor as a backup login possibility. We fill this gap with RQ1. Additionally, we want to understand how justified this repeatedly mentioned fear of consequences of losing the second factor is by testing how easy a user could regain access to their account (RQ2 & RQ3).

How Likely is it to Lose the Second Factor? In the following, we report on how often users are confronted with the problem of losing their second factor. This motivates our task design, as we assume that the loss of the second factor is not a theoretical scenario. For smartphones, which are the most commonly used second factor [41], studies indicate that around 40% of smartphone users have had at least one incident in which they lost their device or had it stolen (around 10-15%) [3, 23, 27]. One study estimated that an average person living in the UK loses two smartphones within their lifetime [6]. However, the authors did not report the frequency of users being able to recover their devices: Data from 2014 show that while 90% of phone theft victims tried to recover their phone, only 32% were successful [27]. Furthermore, one study indicates that around 60% of the users who lost their device misplaced it, most often at home or work (49.5%) [22], where chances of finding the device again are high.

Dutson et al. [12], and Abbott et al. [1] looked at implications for the users after their universities adopted 2FA. In the study by Dutson et al. [12], around a fourth of the participants reported they have had at least one incident within one year in which they could not access their account due to an inability to access their phone (because it was lost or stolen, they forgot it somewhere or it ran out of battery). Around 16% of the support chats that were analyzed by Abbott et al. [1] concerned how to access the account if the second factor was inaccessible. For both studies, it remains unclear in how many cases this status was only temporary (i.e., how many people actually lost their device or had it stolen).

So, while we do not have much evidence, we think it is fair to assume that the loss of the second factor, i.e., the smartphone, is something that indeed happens.

2.2 Analysis of Recovery Protocols

We are aware of only a few studies that analyzed the recovery protocols users had to follow if the primary or secondary authenticator was lost or compromised:

Li et al. [26] investigated the recovery protocols for the **primary authentication** for over 200 websites in 2018. They found that on 89.1% of the websites, it was sufficient to have access to the registered email to recover the account. On 4.6%, it was sufficient to know the answer to a security question.

Neil et al. [31] analyzed 57 American websites in 2020 according to their user-facing advice on restoring the user account to a pre-compromise state. For the phase of account recovery, i.e., regaining access to the account **independent of the authentication methods** in use, the authors found that 96% of the websites had some information on what to do (e.g., advising to send oneself a password reset email). Over 60% of the websites recommend contacting their support. Markert et al. [28] extended the previous study by investigating 158 websites; covering the 50 most popular websites in 30 countries. Even though less than in the US American sample, most websites offered some advice on how to recover accounts; mostly by recommending to reset the password or by contacting the support.

Another related study was conducted by Quermann et al. [37], who analyzed the state of user authentication in 2017 for 48 different services (websites, IoT, and mobile devices). They found that none of them offered an easy way to recover accounts that were secured with a **second factor**, and almost all services require the user to contact the services' support.

However, Quermann et al. [37] did not further systematically investigate whether websites do anything to prevent user lockout when users set up a second factor or how well users who cannot access their second factor are guided through the support (e.g., do users have a direct and easy way to contact the support or do they have to search for a contact themselves within various articles?) We update and expand upon this prior work by conducting expert reviews mimicking a user who lost their second factor and analyzing the steps that needed to be taken to regain access, as well as the usability of the support offered by each website/service (RQ2).

3 Methodology

We analyzed how popular services communicate and handle the issue of second-factor loss during the setup and recovery. We did this by conducting 78 expert reviews. The tasks were first to set up a user account with 2FA and, second, to recover it without the factor. In this section, we describe how we selected the evaluated services, the tasks we performed, and how we analyzed the gathered data.

3.1 Service Selection

We used Tranco [36] to identify high-traffic websites and used the top 500 for our analysis. The list was generated on 2 August 2022 [42]. The websites were accessed between September 2022 and January 2023 from Germany with a Linux machine using Chrome. All services that required an app-based setup were accessed from a smartphone (Honor 8x) with Android 8.1.0. During the reviews, we visited the websites as they were referenced on the list. However, in some cases, the websites forwarded us to the localized site according to our location.

We excluded sites if they were marked insecure by Google Safe Browsing or if account creation was only possible for a specific user group. The whole list of exclusion criteria is given in Appendix A.1. An overview of this elimination process and the corresponding numbers is shown in Figure 1.

Websites that belong to the same domain or use shared accounts were merged (e.g., Google.com and YouTube.com). Finally, we checked whether we could enable 2FA on each of those websites. Similar to the findings of Gavazzi et al. [15], less than half of the websites offer 2FA. Finally, we ended up with 78 services for the reviews.

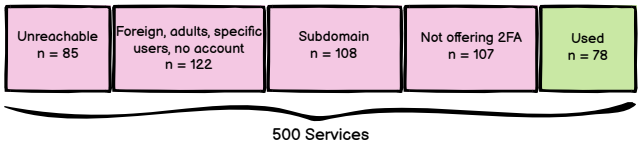

Figure 1: Overview of the service selection. We started with 500 high-traffic websites, according to Tranco [42]. Services were excluded based on criteria specified in Appendix A.1. Eighty-five were unreachable or marked insecure by Google Safe Browsing. This left us with 185 services, of which 78 offered to add a second factor.

3.2 Task

The expert reviews consisted of two tasks. The first task was to create an account and set up a second factor. In the second task, we tried to recover the account, pretending to have no access to the second factor. In the following paragraphs, we describe the tasks in more detail and explain how we conducted the reviews.

Task 1: Setup One researcher manually created accounts on all of the selected services. They always selected the free version of an account and used the same password. They enabled a second factor if possible. For this, they picked the first option allowed based on the following order 1) SMS

verification, 2) email verification,[1] and 3) an authenticator app. If an authenticator app was necessary, they used Google authenticator [44]. The researcher did not set up any additional second factor or possibility to be contacted during the setup phase, except when it was mandatory. The sessions were screen recorded.

After setting up all accounts, the browser was un- and reinstalled to remove artifacts from the setup phase. While this might make it harder to regain access, we opted for the lower-bound results. We believe that if recovery is possible in our scenario, it will also be possible when the browser was already used to log into the account, but not vice versa.

Task 2: Recovery One month after the second factor was added, the same researcher navigated to the login screen and tried to log in without the second factor, i.e., looking for an alternative or help. They did not have access to the backup codes if the service provided them. However, they could answer basic questions about themselves and the account. If 2FA was set up using a smartphone (SMS or authenticator app), the researcher could access the email associated with the account.

If the website gave instructions to regain access, they were followed. If the website did not provide assistance during the login process, the researcher searched through the help center, if any existed, and followed the steps, if any were given. If this also did not help to regain access to the account, the researcher consulted Google with the search term "2fa lost site:www.example.com." If they had to contact support, they used the following text (if applicable): "Hello, I lost my phone, which I use for two-factor authentication, and now I cannot log in. Would it be possible for you to deactivate this, or will I need a new account? Kind regards, [Name]." The recovery was declared successful if it was possible to log in without the second factor, and the second factor could be deactivated or changed. An account was marked as irretrievable if no information could be found on retrieving it, if instructions were given but failed, or if the instructions clearly stated that retrieval was impossible.

The sessions were again screen recorded, and related emails were saved.

3.3 Analysis

To find common themes during the setup and recovery phase, two researchers looked at a random subset of the services (14 services, 18% of all) to create an initial code book for each research question. In this step, each website was represented by all videos and emails associated with the setup and recovery procedure on this particular service (see Section 3.2).

[1] Even though receiving codes through email is not considered as a second factor by NIST [33], it was listed as such on these websites. We opted to go with the definition of the services, as we believe there are users who will do so as well.

The researchers then coded another eleven services (14% of all) using the code book, arriving at a weighted inter-coder reliability of 0.89 which was in the range of 0.56 to 1 for individual codes. For the full coding, each researcher coded half of the services.

4 Results

This section presents the results of the usability evaluation of the 2FA setup and recovery process of 78 services. We first give a general overview of what second factors were supported and recommended by the services. Following this, we show how services try to prevent issues that result from a user losing their second factor during the setup phase (RQ1), e.g., by recommending implementing alternative login methods as backups. In Section 4.3, we report how (well) services guided us through the process of regaining access (RQ2) and what information was needed (RQ3).

A complete overview of all services, the used second factors, and characteristics during setup and recovery are given in Table 2 in Appendix A.

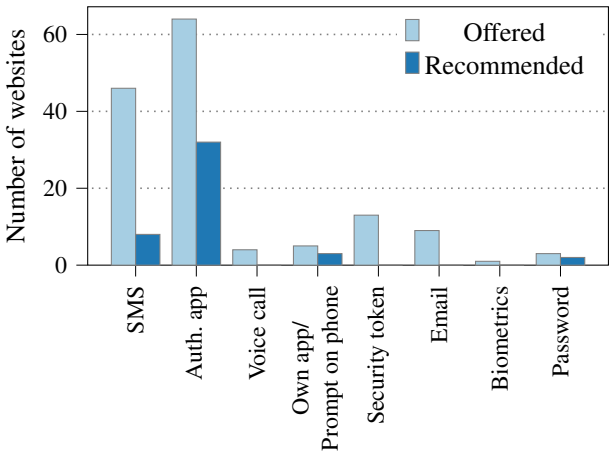

Figure 2: Overview of the allowed second factors on all sampled services. Most services allow users to use an authenticator app. Marked as "recommended" are those factors that were offered as the only possibility, were selected by default, or were marked as "recommended".

4.1 Allowed Second Factors

We were able to add a second factor to 78 services (see Figure 1). We registered a phone number to receive SMS codes on 46 services. If a service did not offer 2FA via SMS, we selected to receive codes via email ($n = 5$) or Google Authenticator ($n = 25$). There was no website where this was not sufficient. In the particular case of two apps where the phone number was already used as a primary authenticator, we added a password as a second factor.

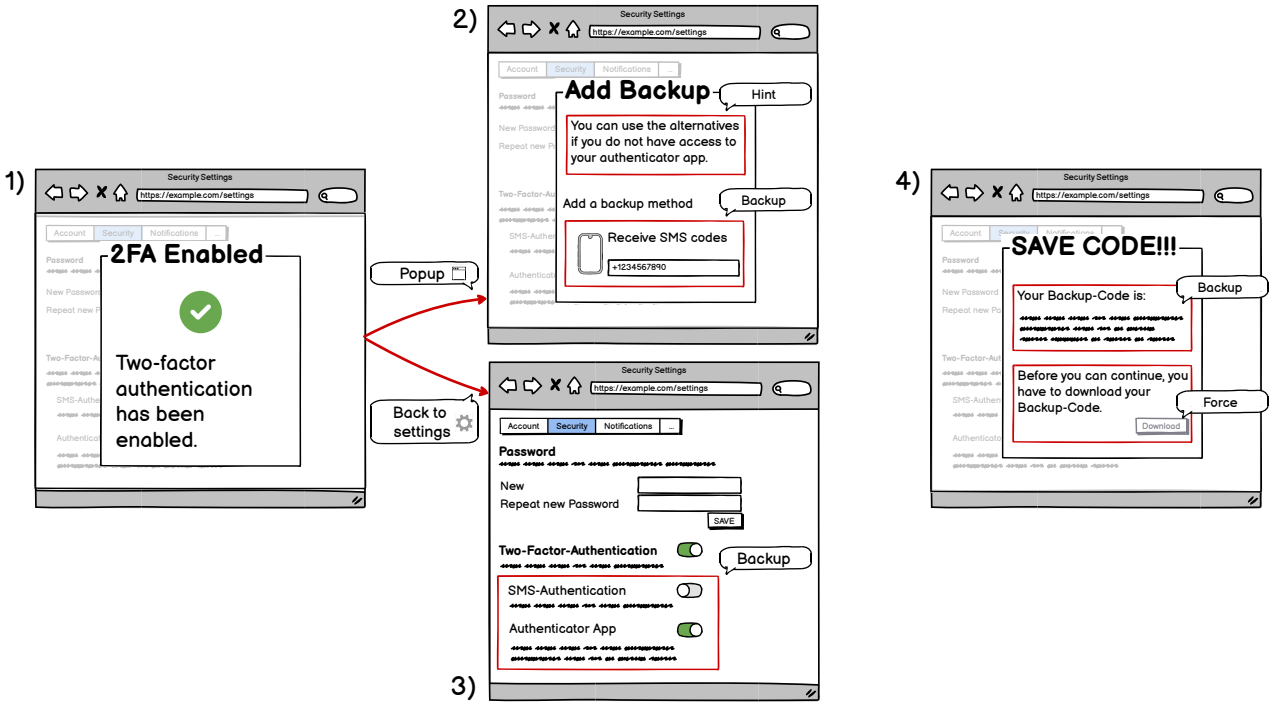

Figure 3: This figure shows four windows, with examples of information and cues we received during the reviews of the setup. A common workflow led us to one of two different states after enabling 2FA (1). In 52 cases (2), hints and backup possibilities were shown in the same popup that was used for setup. Some pages closed the window and led us back to the settings ($n = 10$) (3), where hints and backup possibilities were shown. 16 services required additional action from the users, e.g., requiring them to download backup codes or to add an additional phone number (4).

As shown in Figure 2, most of the investigated services offered the possibility to use authenticator apps to secure user accounts. Authenticator apps were also the most commonly recommended second factor (by 41.0% of the services). Some services mentioned specific authenticator apps, most prominently Google Authenticator ($n = 27$), followed by Authy ($n = 14$) and Microsoft authenticator ($n = 10$).

4.2 2FA Setup

In this section, we report whether and how the services communicated the issue of losing the second factor (RQ1).

For this, we analyzed how prominent they mentioned a potential second-factor loss. We tracked whether and how the services nudged or forced users to add another factor as a backup or store backup codes. The data for this section was gathered during and right after a second factor was added to an account, thus at a point in our scenario where the user still had access to the second factor.

During the analysis, we identified three cues (see Figure 3 for examples) of how services communicate with users related to the research question:

(a) **Hint**: The service mentions that the second factor could be inaccessible.

(b) **Backup**: The service presents possible backup possibilities - backup codes, a security question, or other available factors.

(c) **Force**: The service forces the user to add a backup or download backup codes.

The three cues were shown at one of two locations: Either in the settings ($n = 10$) after the setup of the second factor is completed or in a separate window during or following the setup ($n = 52$).

Backup On most services (79.5%), it was possible to add another alternative second factor ($n = 40$ services) and/or to download one or several backup codes ($n = 45$). Yet, the intended usage of the latter differed: While most services provided backup codes that can be used instead of a code sent by SMS or generated by an app, some services offered a backup code that will automatically deactivate 2FA once used. We found that the wording of these codes differed as well: Both terms “backup codes” and “recovery codes” were used interchangeably, sometimes meaning different things.

Hints Most services that offered backup possibilities (80.6% of the 62 services that offered a backup) hinted at

the possible inaccessibility of the second factor somehow. A typical text was similar to the following: “This code lets you log in if you don’t have access to your two-factor authentication methods.” In these cases, a user may understand additional factors as a possibility rather than a necessity. Only three websites communicated this a bit more clearly by using statements similar to “you will need these codes should you not have access to your phone.” In general, the consequences of loss (i.e., being locked out of the account if losing the second factor and having no access to any backups) were only communicated by a minority: Four services used phrasing similar to: “otherwise you may get permanently locked out.” Only ten services clearly stated that the provided backup codes or offered fallback authentication are the “only” way to log in if the second factor is not accessible. Interestingly, this turned out not to be the case for six of these services. We pick this topic up in Section 4.3.2.

Force The use of force was not that common. We only had to add a backup on 16 services. All except one page forcing the user to add a backup explained that this backup could be used to access the account.

Combinations The most common combination of the three cues was to have a hint and backup possibilities but no force to implement them ($n = 29$, 37.2%). The second most common combination was to show and mention nothing at all ($n = 16$, 20.5%): No hint as to what could happen and no way to resolve this. All combinations of the cues are shown in Figure 4. 64.1% of the websites gave a hint and offered a backup possibility.

4.2.1 Tales From the 2FA-Setup Land

We found an interesting case where one page advertised 2FA right after login and also included a small note that one should “remember to create backup verification methods.” However, after registering an authenticator app, this information was not shown anymore, though one of the presented verification methods was called “Recovery codes.” In another case, the website seemed to follow a more serious approach. After telling the users in the first step to “save this [backup] key,” they were told in the second step “Seriously, save this key.”

4.2.2 Summary of the Setup Task (RQ1)

To summarize, we were successful in activating 2FA on 78 services. Of these, 50 provided at least minimal information about what to do when the second factor is lost (Hint). Most services offer some form of backup method, and 45 provided backup codes. The degree of how straightforward consequences of loss were communicated differed. Only ten services clearly indicated that a user will lose access to the account without the second factor and without backups. Having all sorts of combinations of hints, backup possibilities, and obviousness, there does not seem to be a process or possibility for fallback authentication a user can assume by default or always rely on.

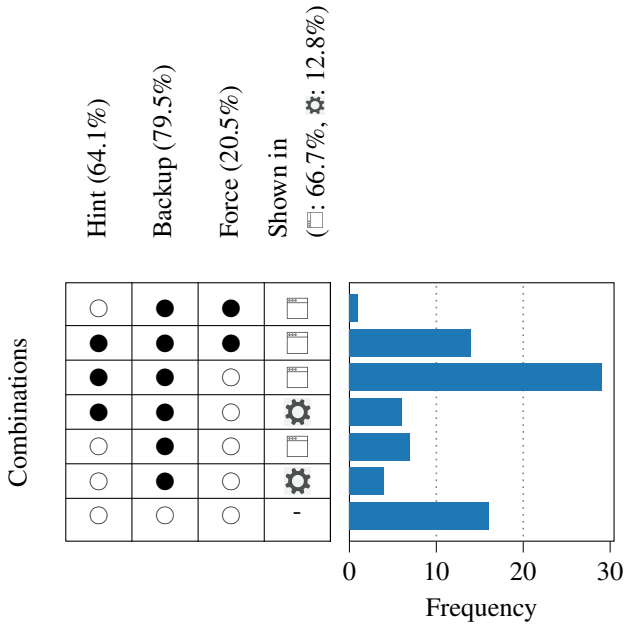

Figure 4: Number of websites that mention the possibility that the second factor is not accessible (Hint) in combination with showing alternative possibilities (Backup) or forcing the user to do something (Force) during 2FA setup. ○: The service does not include the characteristic. ●: The service fulfills the characteristic. “Shown in” depicts the location where this information is shown. ▭: The information is shown in a popup that also directed us through the process of adding the second factor. ⚙: The information was shown in the settings. Examples are given in Figure 3.

4.3 Recovery

In this section, we present the results for the second task, the account’s recovery after the second factor is lost (RQ2).

We looked at how and to what extent the services’ interface assisted the user during login, what needed to be done to regain access (e.g., what information had to be provided), and report on how many services we received full access to.

4.3.1 Assistance During Login

We found varying degrees of assistance from the services to guide the user during a login attempt. In the next paragraphs, we clustered common themes.

Missing Common Practice Today, it is common for websites to provide a “forgotten password”-link during login that

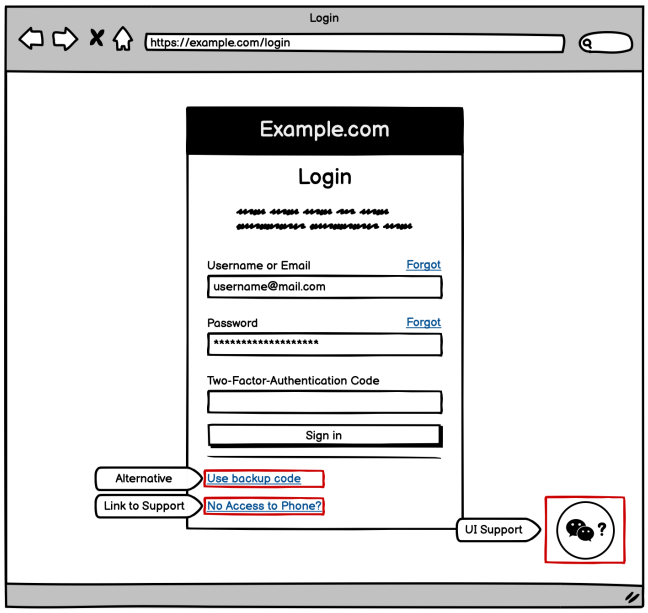

Figure 5: Example for the Login screen. If a link to the support existed, we noted whether it linked to a general FAQ, a specific FAQ (that at least partially mentioned what to do if losing the second factor), or whether a user is provided with an email address or can fill a form.

a user can use to reset their password. As expected, all websites in our set provided such a link. The equivalent for 2FA, i.e., a link a user can click while trying to log in but having no access to the second factor, is often missing. Even though 75.6% of the websites provided the user with some form of a button to offer help in such cases, the usefulness varied massively. Some services mentioned fallback authentication (e.g., suggesting to use backup codes), some linked to some sort of support, and yet others had an always visible support interface that was independent of the login screen. Examples of these possibilities are shown in Figure 5. Most often ($n = 15$), a website showed alternative authentication possibilities and directed the user to a direct contact form or email address where they could ask for help if fallback authentication did not work as well. Second most often ($n = 14$) was the exact opposite, where a service did not show any support at all during login; thus, the user's only possibility is to cancel the login attempt and look for help somewhere else. Table 1 provides an overview of the types and extent of support provided by various services during login.

Easiest Option is to use an Alternative Method If the user implemented a backup method (e.g., alternative email or phone number) or has access to backup codes, this is a simple and fast solution to regain access. During login, 50 services suggested using an alternative to the primary second factor. Interestingly, 16 further services generally offered backup methods during the setup but did not mention them during login.

Websites Could Have Directed us to a More Helpful Site Part of the task description was that the researcher had no access to the backup codes, so they looked for solutions outside of the login screen if the login screen was not helpful. Over half (52.6%) of the websites either did not link to any help at all or directed the user to a general help page. For these cases, we additionally tried to find a specific site that explained the procedure a user has to follow when losing access to the second factor. Interestingly, most websites that did not provide specific help when logging in offer a specific FAQ page related to the topic (90.2% of 41). This is especially striking for the 14 websites not supporting the user at all during login: All of them have a specific subpage explaining at least partially what to do.

Tales From the Login Land An existing support site was no guarantee for a goal-oriented process. There were five cases where the suggested or obvious procedure was not helpful at all. In three of those cases, we were stuck in an infinite loop, e.g., because the login screen directed to a help site with a button labeled "Account Recovery;" however, when clicking this, we were directed back to the initial login screen.

We also encountered that the linked support page was only available in the language of the sites' country we could not understand (without a translator). Please note that the rest of the site was available in other languages.

Apart from those five, one page did not provide us with a link to their support until having received a timeout for receiving the code via SMS. In case of a lost phone, this makes the search for help unnecessarily confusing.

4.3.2 Regaining Access

As shown in Figure 6, we were able to regain full access for 41 (52.6%) of the accounts. In nine additional cases, full access most likely would have been possible if we used the account properly and could provide the support with account information, such as banking details, that we did not add to the test account. In one case, the uploaded ID was not accepted, but we received no detailed feedback. We assume that more trials might have given full access.

"Backup Codes are the ONLY Possibility to Access the Account" As mentioned in Section 4.2, ten services explicitly said that users would lose access to their account if they had neither their device nor any backup code. Yet, on six of those, we gained full access after contacting the support. There were essentially two different cases. 1) Three requested details about the account owner or the account like a copy of an identity document, payment details, the address, or the

Total No. Services	No. where better FAQ exists	**Link to support**	Total No. Services	No. where better FAQ exists
15	-	Direct Form	5	-
6	-	Specific FAQ	1	-
6	4	General FAQ	1	1
3	2	Unusable	2	0
10	5	But UI support	5	5
10	6	Nothing	14	14

Use of backup suggested

Use of backup not suggested

Link to support given

No link to support given

Table 1: The table depicts the level of support a user gets during the login if they cannot access their second factor. The colors indicate whether a service a) suggests using a backup (e.g., sending the code via mail instead of SMS) and b) if a service provides the user with a link to any support. We also note how many services have a specific information site for 2FA recovery despite not linking to it on the login screen. The most common level of help was given by 15 services: Suggesting to use a backup and linking to a direct form to contact the services' support. On the other hand, 14 services do not support the user at all during login.

current IP address.[2] 2) For three other services, we gained access very easily. One support gave us access after answering a security question. As the researcher was not sure what the answer was, we got a hint after a close-to-correct attempt: ("your answer is close to being correct but is just missing something additional").

Obscure Procedures In the case of a meeting platform, we were asked for our personal meeting-ID. As we did not use the account, we did not store this anywhere and were thus not able to provide it. Interestingly, after disclaiming that we did not have access to this, the second factor was disabled anyway. Since we did not investigate the easiness of accessing the account specifically from an attacker's view, it is up to future work to understand how often information that is asked for is indeed not needed. On another website, we only had to send an email without providing further information, which resulted in us regaining access to the service. We assume, or hope, that this website has internal metrics that allowed them to judge our request. In any case, they did not communicate with us beforehand or even afterward.

4.3.3 Ways to Recover Accounts

We gained full access to our account on 41 services. We could simply receive the 2FA code via email in six of those cases. For the remaining services, we had to contact the services' support.

In the following, we give an overview of what information we had to provide to gain access. We identified five categories of information and evidence services that were asked for proof of ownership during the recovery:

- Personal information, such as name or address.
- Uploading an identity document .
- Basic account information, such as the username or payment details.
- Extended account information, such as information about the last purchase or the date the account was created.[3]
- The need to access the email address used to set up the account.

In general, we saw 17 different combinations of these categories for the 41 accounts we could access. Most commonly ($n = 7$), we were asked for basic account information and needed access to the email address linked to the account. On three services, accessing the account was very easy, as we only needed to provide the service with the email address used for the account, for which we wanted to deactivate 2FA. These services sent a confirmation via mail, but we did not need to react to it with, e.g., clicking a link.

Wait Time Seven services included a wait time for security purposes, meaning they would send a note to the email associated with the account. If they did not receive any negative feedback within a certain time, they would proceed to either delete the account or grant access to it. This waiting time ranged from 1 to 30 days.

No Access but Receiving Additional Help On 37 services, we were not able to regain access to the account. While most mentioned that they could not help us, four provided some

[2] We were in contact with the support via email and believe the IP was used to compare it with IP addresses that were previously used to access the account.

[3] While it was easy to provide the account creation date in our scenario, this question could be tough for users who have had their accounts for many years.

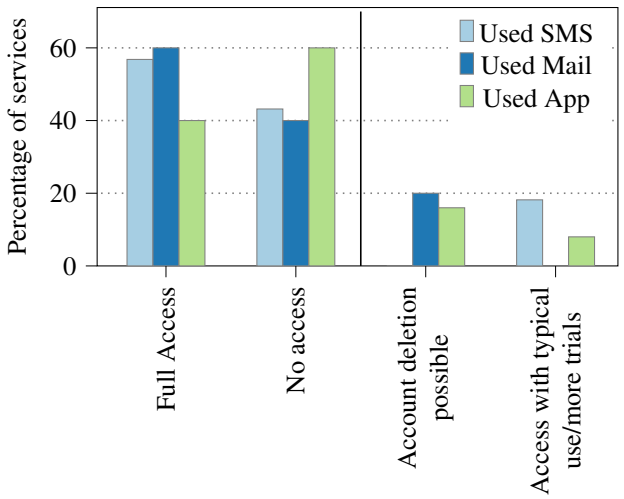

Figure 6: Overview of our results for the recovery process. It shows the percentages of services we either got full or no access to. Two accounts could be recovered using Authy. The right part shows the "no access" category in more detail. For some accounts, an account deletion was possible, on others, we assume we could have logged in with a more realistic setup. The percentages are grouped depending on the second factor we set up before. In the figure, we omitted the two apps where we used passwords as a second factor. In one of those cases, we could have deleted the account; in the other, we could have gained access after a security wait time but without restoring the data that was not backed up.

level of additional help, e.g., they recommended contacting our network provider to receive a new SIM card, which would fix the issue of not receiving SMS codes.

Email as a Second Factor We could recover three of the five services where we used our email as the second factor. To accomplish this, we always had to present the service with another email address. Apart from that, the services differed. In one case, it was sufficient to wait for a month. In the other two cases, we had to provide personal and account information or even upload our ID.

4.3.4 Summary of the Recovery Phase (RQ2+RQ3)

We found that almost the same number of services offered the user no support at all during login as services that gave the maximum possible support by presenting the user with the opportunity of using a fallback authentication as well as a direct contact possibility. Between these two extremes, we saw a lot of different approaches varying in helpfulness. Regarding account recovery, we were successful in regaining access to 41 accounts. However, there were cases where no additional info other than knowing the email address was necessary to disable 2FA.

5 Discussion

We conducted 78 expert reviews to study the setup of 2FA and account recovery on popular services that offer 2FA. In all 78 cases, we were able to successfully set up a second factor. However, our main interest was account recovery. We focused on the information a user was given during setup and the information and guidance these services offered in case the second factor was lost. We could recover access to 41 services without the second factor and backup codes. In general, we found the usability of the setup and recovery process to be lacking in many basic aspects. We discuss themes we saw and make suggestions to practitioners and the research community.

5.1 The User is Often Left Alone

Based on related literature that often mentioned fear of losing the second factor as a reason for not adopting 2FA [10, 25, 35], we phrased our research questions and were especially interested in how services communicate the mitigation and consequences of the loss of the second factor. Both during 2FA setup and recovery, we ran into situations where we only faced vague information or no help at all. During login, 16 services did not inform the user that backup codes can be used instead of codes generated by an authenticator app or sent via SMS, even though they existed. Services that communicated a potential loss of the second factor during setup and that offered backups often avoided statements about accessing the account without the second factor. Only ten services clearly stated that a certain backup would be the only way to gain access. Most other services framed consequences ambiguously, e.g., by stating users "might lose access."

When searching for help at the login screen in the event of a lost second factor, many websites linked to no specific help page, even though one would have existed. All of these problems go against the tenth principle of Nielsen's usability heuristics (help and documentation) [32], and we strongly advise website architects to resolve these easily-fixable issues by adding links to already existing documentation or communicating the possibility of using backup codes during login.

The issue of lacking information is also documented by related work concerning account remediation [28, 31].

5.2 There is no Common Workflow...

We could not identify a common workflow to add a second factor or to recover an account across the different services. This affected all parts of the process: the communication of possibilities for backups, the way a website communicates the consequences of loss, using unified terms, or what information a user needs to provide to recover the account. Currently, a user cannot infer from their experiences from one website to

another. With this, the fourth usability heuristic by Nielsen is violated (consistency and standards) [32].

In our view, this is a problematic situation, as 2FA in itself is a general technical measure to increase account security, and its' usage is likely to increase in the near future.

The origin of this heterogeneity is unclear. Maybe there has not yet been enough time elapsed for a best practice to evolve that everyone copies and can easily adopt. If this is the case, this is also an excellent opportunity to develop a best practice example and provide a fast, secure, and empirical evidence-based solution.

5.2.1 ... not Even Within Services

In addition to the above, many services are not even consistent within themselves. We found one example where 2FA was set up using SMS codes, but the code was sent via email during our login attempt. In another case, a button for "account recovery" existed in the FAQ but linked to the login screen. All of the websites that did not help the user at all during login had a subpage in their support section that explained what to do when the second factor is lost. Similarly, several of those websites that linked to a general FAQ could have linked to a more specific one, making the process much more user-friendly. On some websites, consequences of loss are communicated clearly within such help pages, and several also point to actions that can be done to prevent account lockout. Yet, this is barely mentioned during setup. We believe it is unreasonable to assume that users first look for this specific information on help pages before or after deciding to activate 2FA. Even if it is offered during set-up, users might click through the information, but it is more likely to be seen than if users have to actively look for it (and know-how, too). Fortunately, this is often an easy fix, and we are currently in the process of contacting the affected services to inform them.

5.3 Insufficient Support Structures

The services we used for our research are all popular services. Thus, they handle a lot of traffic and many users. Support on these services is often handled by a bot (chat or phone), and direct human-to-human support was often harder to find. This is fairly common and is likely driven by cost-cutting reasons.

However, depending on the service, it can be very detrimental and stressful to be locked out. We believe that the support structure of many of the services we analyzed does not fulfill the users' needs. We saw cases where support was only available for logged-in users or users who selected a paid product (with no real help available for those using a free version). One website did not offer any help article, but we found a community forum in which frustrated users explained what answers had to be given to the phone bot to end up with a human who could disable 2FA.

Depending on the kind of service, it might be reasonable from the website's perspective not to invest much into recovery procedures, especially in the case of unpaid accounts. Yet, we believe that any account can have a huge value, depending on who is using it for what, and that most users who turn on 2FA voluntarily do see value in their account.

From a usability perspective, we think there should be a dedicated channel for account-related cases. Or, if no dedicated channel is possible, services should at least provide upfront and transparent information on what can be done in such situations.

5.4 Summary: Recommendations for Websites

Summarizing Sections 5.1 to 5.3, we give the following recommendations to website providers:

1. Internal consistency and clear communication during login on what is possible and what is not. E.g., if backup codes exist, the website should mention them as an alternative. If an account cannot be recovered at all, this information should be clearly stated.

2. Services should provide some help during login, similar to the 'forgot password'-link.

3. This help should be as specific as possible. E.g., if the website offers a specific help page explaining how the account can be recovered, this should be directly linked. Preferably, every website had a specific form for this problem, so users could directly contact support.

5.5 Various (and Obscure) Options for Access

In our sample, it was rare to find cases where it was explicitly stated what information a user needs to regain access to their account in the absence of a backup. During recovery, we noticed situations in which access was accomplished very easily, and it was unclear if any technical measures were implemented that checked for the legitimacy of a request to disable 2FA (e.g., using the IP address). Results from Gavazzi et al. [15] indicate that only 22% of their investigated websites block suspicious login attempts, so if this also applies to the aforementioned sites, an attacker might easily get access to the account even if they only know the password.

This is a problem from both usability and security perspectives: The user has no possibility to assess whether the account is really as secure as hoped, i.e., how easy it is for an attacker to disable 2FA. We think when it is not communicated beforehand how access can be granted, users could get a false sense of security.

Similarly, in six cases, we were able to receive the code via email instead of SMS or the authenticator app. If, in these cases, the password can also be reset via email, an attacker

would not need any extra effort to get access as soon as they have control over the email address.

Future work should investigate whether and how users benefit from clear information about 2FA deactivation during or after setting up a second factor.

One solution for a service to make sure a request to disable 2FA is legitimate, also used by 1Password [14], is to combine several proofs of ownership, e.g., requesting access to the email address and also asking for extended account information (knowledge-based challenges). Doerfler et al. [11] studied several of such challenges individually, finding that only 13% of users in their data set were able to recall their account creation date and only 22% could answer their security question.

It remains to be investigated how usable and secure combinations of different challenges are and whether an optimal recovery procedure can be found.

5.6 Who Should be Responsible for Recovery?

We found many opportunities to make 2FA on services much more usable but found this directly connected to the question of who is or should be responsible for a successful recovery.

Most services provide the possibility to recover from lost passwords, so we believe many users might transfer this practice to 2FA.

Yet, we found that while some work has been conducted on how well different fallback authentication mechanisms work (e.g., [11, 29]), we currently do not know what the user's expectations are. Similarly, there is a lack of literature about how website owners and operators see this. It seems that the implicit mindset is that users are responsible for protecting access, including the backup. In any case, we think the easiest mitigation is currently on the side of the services. Transparency could resolve a lot of potential confusion without adding any obvious disadvantages. Golla et al. [20] found that telling people they are responsible for their accounts' security leads to higher adoption of 2FA. The same might apply to backups if the services clearly communicated the consequences.

Authenticator Apps Some authenticator apps provide backup possibilities, yet most rely on passwords, SMS, or emails [18]. Any backup possibilities offered by authenticator apps are currently not part of services' communication, and the Google authenticator is the app most commonly mentioned or recommended by the services ($n = 27$). Interestingly, at the time of the study, Google authenticator only provided one backup possibility, namely a manual QR code export [17, 18]. Since April 2023, Google Authenticator can be synchronized with the users' Google account [4].

Third Parties / Delegated Account Recovery Handling identities connected to user accounts can be challenging. We encountered one website that outsourced this. The website offered to start a recovery over PayPal if a PayPal account was connected to the account. Basically, this follows the idea of SSO. Only a handful of services are responsible for handling the identity. What worked for this website may not work for others, but it opens the question of whether one (or a few) single instances that provide 2FA should also handle the backup and recovery process. In our sample, some services referred to Authy for the recovery process. While, from a usability perspective, this worked well for us, Gilsenan et al. [18] note that Authy solely relies on SMS OTP during recovery. The authors also found several security and privacy issues [16].

5.7 Limitations

Our work has to be interpreted in light of the following limitations:

We focused our analysis on high-traffic websites, so we cannot generalize our results to less popular ones. Yet, we were able to identify issues on these top websites already and believe that administrators and web designers of less popular services can benefit from our results as well.

Not all services support identical second factors (see Section 4.1), but the recovery protocol of services might be influenced depending on the used second factor. We deal with this limitation by giving extra care when comparing the services and pointing to this difference in the results.

Access to some of the services is typically done through the smartphone app. Whenever possible, we used a browser. Thus, it might be possible that the app's interface, including links to the support, differs from the browser version.

Every recovery was made using the same IP that was also used for setup. However, we reinstalled the browser. We cannot estimate how many services checked such metadata before granting access to the account. Additionally, by reinstalling the browser, we chose a tougher scenario than many users would most likely face. We opted for this to capture the lower bound. Similarly, we noticed services that advised us to use a still-logged-in device to disable 2FA. It is up to future work to analyze this in more detail.

We used the accounts only for a short time and only for testing the recovery itself, which comes with further limitations:

- Some services rely on data that is stored within the account to be able to grant access after losing the second factor, e.g., by asking for personal data such as the address or banking details or for order numbers from previous transactions. As we did not add any information, we could not always mimic the whole recovery process. With the empty accounts, we also see the possibility that people working in the support might not have protected the account as much as they would have

with a regularly used account. This is especially critical for services where we were in contact with humans (see Section 4.3.2).

- Some websites periodically ask their users to review and confirm their recovery settings, but we could and did not investigate this feature.

- Some security features might be bound to the users' location or the time they have already used the account. Such details are not captured in our study.

5.8 Future Work

We encountered services that only asked for very basic information to grant us access to the accounts. Similar to as it has been done with security questions [40], it should be studied from an attacker's point of view how easy it would be to get access in such cases.

Two-factor authentication is not the only case where well-designed recovery processes are important. The rise of passwordless authentication is a quite recent example where these processes become crucial, a challenge that future work needs to address.

Due to the many serious issues that we discovered during our 78 expert reviews, we believe that currently, a study that evaluates the usability of account recovery for a lost second factor in a user study would not add much more insight. We are currently in the process of informing the services for which we identified issues.

6 Conclusion

In this study, we aimed to understand how popular services guide their users through the setup of 2FA and the recovery process when the second factor is lost.

We conducted expert reviews on 78 services, analyzing their approach to inform users of possible risks of 2FA, the availability of backup options, and how well users are supported if they cannot access the second factor during login.

Our results revealed that services do not seem to follow a standardized practice for 2FA setup or recovery, and the level of support provided varies greatly among them.

Our findings indicate that only a small percentage of services communicate the importance of a fallback. Additionally, some services do not provide any help during the recovery process, and users are left on their own to solve the issue. These findings suggest that there is room for improvement. Many services could benefit from establishing a more standardized approach to 2FA setup and recovery to ensure convenience for their users without sacrificing security.

Acknowledgments

We thank the Werner Siemens-Stiftung (WSS) for their generous support of this project and our anonymous reviewers for their help and feedback.

References

[1] Jacob Abbott and Sameer Patil. How Mandatory Second Factor Affects the Authentication User Experience. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13. Association for Computing Machinery, New York, NY, USA, April 2020.

[2] Claudia Ziegler Acemyan, Philip Kortum, Jeffrey Xiong, and Dan S. Wallach. 2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 62, pages 1141–1145, September 2018.

[3] Bitkom. Gestohlen oder verloren: Vier von zehn Personen ist schon mal das Handy abhandengekommen. https://www.bitkom.org/Presse/Presseinformation/Gestohlen-oder-verloren-Vier-von-zehn-Personen-ist-schon-mal-das-Handy-abhandengekommen. Accessed: June 08, 2022.

[4] Christiaan Brand. Google Online Security Blog: Google Authenticator now supports Google Account synchronization. https://security.googleblog.com/2023/04/google-authenticator-now-supports.html, 2023. Accessed: June 08, 2023.

[5] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Proceedings of Symposium on Usable Privacy and Security*. USENIX Association, 2019.

[6] Andy C. How To Avoid Losing Your Phone. https://www.mobiles.co.uk/blog/how-to-avoid-losing-your-phone/. Accessed: June 08, 2023.

[7] Dave Childers. State of the auth 2021. https://duo.com/assets/ebooks/state-of-the-auth-2021.pdf, 2021. Accessed: June 08, 2023.

[8] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human*

Factors in Computing Systems, pages 1–11, Montreal QC Canada, April 2018. ACM.

[9] Sanchari Das, Andrew Dingman, and L. Jean Camp. Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key. In *Financial Cryptography and Data Security*, volume 10957, pages 160–179. Springer Berlin Heidelberg, Berlin, Heidelberg, 2018.

[10] Sanchari Das, Gianpaolo Russo, Andrew C. Dingman, Jayati Dev, Olivia Kenny, and L. Jean 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*, STAST '17, pages 28–39, New York, NY, USA, December 2018. Association for Computing Machinery.

[11] Periwinkle Doerfler, Kurt Thomas, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, and Damon McCoy. Evaluating Login Challenges as a Defense Against Account Takeover. In *The World Wide Web Conference on - WWW '19*, pages 372–382, San Francisco, CA, USA, 2019. ACM Press.

[12] Jonathan Dutson, Danny Allen, Dennis Eggett, and Kent Seamons. Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 119–128, June 2019.

[13] Florian M Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In *Sixteenth Symposium on Usable Privacy and Security*, page 18, 2020.

[14] Pilar Garcia. 10 - Pilar Garcia - Who are you again? Verifying user access rights in an encryption based system. https://www.youtube.com/watch?v=JeV_rop5nmQ, 2019. Accessed: June 08, 2023.

[15] Anthony Gavazzi, Ryan Williams, and Engin Kirda. A Study of Multi-Factor and Risk-Based Authentication Availability. In *32st USENIX Security Symposium (USENIX Security 23)*, 2023.

[16] Conor Gilsenan and Noura Alomar. On Conducting Systematic Security and Privacy Analyses of TOTP 2FA Apps. In *Who Are You?! Adventures in Authentication Workshop*, WAY '20, pages 1–6, Virtual Conference, August 2020.

[17] Conor Gilsenan, Noura Alomar, Andrew Huang, and Serge Egelman. Decentralized backup and recovery of TOTP secrets. In *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, pages 1–2, Lawrence Kansas, September 2020. ACM.

[18] Conor Gilsenan, Fuzail Shakir, Noura Alomar, and Serge Egelman. Security and Privacy Failures in Popular 2FA Apps. In *32st USENIX Security Symposium (USENIX Security 23)*, 2023.

[19] GitHub. Top-500 npm package maintainers now require 2FA. https://github.blog/changelog/2022-05-31-top-500-npm-package-maintainers-now-require-2fa/. Accessed: June 08, 2023.

[20] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M Redmiles. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 109–126. USENIX Association, August 2021.

[21] Paul A Grassi, James L Fenton, Elaine M Newton, Ray A Perlner, Andrew R Regenscheid, William E Burr, Justin P Richer, Naomi B Lefkovitz, Jamie M Danker, Yee-Yin Choong, Kristen K Greene, and Mary F Theofanos. Digital identity guidelines: authentication and lifecycle management. Technical Report NIST SP 800-63b, National Institute of Standards and Technology, Gaithersburg, MD, June 2017.

[22] Beatriz Henríquez. Mobile Theft and Loss Report - 2020/2021 Edition | Prey Blog. https://preyproject.com/blog/mobile-theft-and-loss-report-2020-2021-edition. Accessed: June 08, 2023.

[23] Andy Homan. 44% of people lose their mobile. https://nuttag.com.au/blogs/news/44-of-people-loose-their-mobile. Accessed: June 08, 2023.

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

[25] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. In *Proceedings 2015 Workshop on Usable Security*, San Diego, CA, 2015. Internet Society.

[26] Yue Li, Haining Wang, and Kun Sun. Email as a Master Key: Analyzing Account Recovery in the Wild. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pages 1646–1654, Honolulu, HI, April 2018. IEEE.

[27] Lookout. PHONE THEFT IN AMERICA. https://transition.fcc.gov/cgb/events/Lookout-phone-theft-in-america.pdf. Accessed: June 08, 2023.

[28] Philipp Markert, Andrick Adhikari, and Sanchari Das. A Transcontinental Analysis of Account Remediation Protocols of Popular Websites. In *Proceedings 2023 Symposium on Usable Security*. Internet Society, 2023.

[29] Philipp Markert, Maximilian Golla, Elizabeth Stobert, and Markus Dürmuth. Work in Progress: A Comparative Long-Term Study of Fallback Authentication. In *Proceedings 2019 Workshop on Usable Security*, San Diego, CA, 2019. Internet Society.

[30] Karola Marky, Kirill Ragozin, George Chernyshov, Andrii Matviienko, Martin Schmitz, Max Mühlhäuser, Chloe Eghtebas, and Kai Kunze. "Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. *ACM Transactions on Computer-Human Interaction*, December 2021.

[31] Lorenzo Neil, Elijah Bouma-Sims, Evan Lafontaine, Yasemin Acar, and Bradley Reaves. Investigating Web Service Account Remediation Advice. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 359–376. USENIX Association, August 2021.

[32] Jakob Nielsen. 10 Usability Heuristics for User Interface Design. https://www.nngroup.com/articles/ten-usability-heuristics/, 2021. Accessed: June 08, 2023.

[33] NIST. NIST Special Publication 800-63: Digital Identity Guidelines - FAQ. https://pages.nist.gov/800-63-FAQ/#q-b11, 2022. Accessed: June 08, 2023.

[34] European Parliament and Council of the European Union. DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366. Accessed: June 08, 2023.

[35] Jeunese Payne, Graeme Jenkinson, Frank Stajano, M. Angela Sasse, and Max Spencer. Responsibility and Tangible Security: Towards a Theory of User Acceptance of Security Tokens. In *Proceedings 2016 Workshop on Usable Security*, San Diego, CA, 2016. Internet Society.

[36] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proceedings 2019 Network and Distributed System Security Symposium*, 2019.

[37] Nils Quermann, Marian Harbach, and Markus Dürmuth. The State of User Authentication in the Wild. In *Who Are You?! Adventures in Authentication Workshop (WAY) 2018*, Baltimore, MD, USA, August 2018.

[38] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A Usability Study of Five Two-Factor Authentication Methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 357–370, Santa Clara, CA, August 2019. USENIX Association.

[39] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 872–888, San Francisco, CA, May 2018. IEEE.

[40] Stuart Schechter, A.J. Brush, and Serge Egelman. It's no secret: Measuring the security and reliability of authentication via 'secret' questions. In *Proceedings of the 2009 IEEE symposium on security and privacy*. IEEE Computer Society, May 2009.

[41] Statista. Most convenient Multi-Factor Authentication (MFA) methods worldwide in 2021. https://www.statista.com/statistics/1303617/convenient-global-mfa-methods/, 2021. Accessed: June 08, 2023.

[42] Tranco. Information on the Tranco list with ID X5KYN. https://tranco-list.eu/list/X5KYN/1000000, 2022. Accessed: June 08, 2023.

[43] Jake Weidman and Jens Grossklags. I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference*, pages 212–224, Orlando FL USA, December 2017. ACM.

[44] Google Authenticator. https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2. Accessed: June 08, 2023.

A Website Analysis

A.1 Exclusion criteria for services

Services were excluded for the following reasons:

- **Security or Accessibility:** websites flagged as dangerous by Google Safe Browsing, URLs not belonging to a DNS server or are unreachable
- **Content**: adult entertainment websites or illicit content

- **Shared login:** sites belong to the same domain as a previously listed site and having shared accounts (e.g., Google and Youtube)
- **Language**: sites that don't provide an English or German interface
- **Payment**: requiring payment details for account setup. If a free short-term trial was available, we used this opportunity.
- **Specific user group:** requiring owning a product for account setup, accounts requiring the user to be in a specific region outside of Germany, sites restricted to specific users (e.g., university websites, accessible only by students and faculty members)
- **Additional steps:** requiring in-person interactions

Service	Second Factor	Setup				Recovery	
		Hint	Backup	Force	Shown in...	Link to Support	Suggests Using Backup
AOL.com	SMS	●	●	●	▭	○ But UI Support	●
Abusix.com	App	●	●	○	⚙	○ But UI Support	●
Adobe.com	SMS	●	●	●	▭	○ But UI Support	●
Amazon.com	SMS	○	●	○	⚙	● Direct Form	○
Apple.com	SMS	○	○	○	-	● Direct Form	○
Avast.com	App	●	●	○	⚙	● Unusable	●
Bit.ly	SMS	○	○	○	-	○	○
Booking.com	SMS	○	○	○	-	○ But UI Support	●
CloudDNS.net	App	●	●	○	⚙	○	●
Cloudflare.com	App	●	●	○	⚙	● Direct Form	●
Cloudone.trendmicro.com	App	●	●	●	▭	○ But UI Support	●
DNSmadeeasy.com	App	●	●	○	⚙	● Direct Form	●
Digicert.com	App	○	○	○	-	○ But UI Support	○
Discord.com	App	●	●	○	⚙	○	●
Dropbox.com	SMS	●	●	○	⚙	● Specific FAQ	●
Ebay.com	SMS	●	●	●	▭	○	●
Epicgames.com	SMS	○	●	○	⚙	○	●
Etsy.com	SMS	●	●	○	⚙	○	○
Facebook.com	SMS	●	●	○	⚙	● Direct Form	●
Fastly.net	App	●	●	○	⚙	● General FAQ	●
Fedex.com	SMS	○	○	○	-	● General FAQ	●
Fiverr.com	SMS	○	●	●	▭	● Direct Form	●
Gcore.com	App	○	●	○	▭	○ But UI Support	○
Gandi.net	App	●	●	●	▭	● General FAQ	●
Github.com	SMS	●	●	●	▭	● Direct Form	●
Godaddy.com	SMS	○	●	○	⚙	● Specific FAQ	○
Google.com	SMS	●	●	○	⚙	● Unusable	●
Grammarly.com	SMS	●	●	●	▭	● Direct Form	●
HP.com	App	○	○	○	-	○	●
Herokuapp.com	App	○	●	○	▭	○	○
IlovePDF.com	App	○	○	○	-	● Unusable	○
Indeed.com	SMS	○	○	○	-	○ But UI Support	○
Instagram.com	SMS	○	○	○	-	○ But UI Support	●
Intuit.com	SMS	○	●	○	▭	● Unusable	●
Kaspersky.com	SMS	○	●	○	▭	○ But UI Support	○
Kickstarter.com	SMS	○	○	○	-	○	○
Linkedin.com	SMS	○	○	○	-	● Direct Form	○
Linktr.ee	SMS	○	○	○	-	○	○
Mailchimp.com	SMS	○	○	○	-	○	○
Microsoft.com	Email	●	●	●	▭	● Direct Form	●
MyShopify.com	SMS	●	●	○	⚙	● General FAQ	●
Name.com	App	●	●	○	⚙	● General FAQ	○
No-IP.com	App	●	●	○	⚙	○ But UI Support	●
OK.ru	SMS	○	●	○	▭	● Unusable	○
Onlyfans.com	SMS	○	●	○	▭	○ But UI Support	○
Opera.com	App	●	●	●	▭	○	●
Patreon.com	SMS	●	●	○	⚙	○	●
Paypal.com	SMS	○	●	○	▭	● Direct Form	○
Pinterest.com	SMS	●	●	○	⚙	○	○
Reddit.com	App	●	●	○	⚙	○	●
Ring.com	SMS	○	○	○	-	○	○

Service	Second Factor	Setup				Recovery	
		Hint	Backup	Force	Shown in...	Link to Support	Suggests Using Backup
Roblox.com	Email	●	●	○	⚙	● Specific FAQ	●
Samsung.com	SMS	●	●	○	⚙	● Direct Form	●
Slack.com	SMS	●	●	○	⚙	● Specific FAQ	●
Snapchat.com	SMS	●	●	○	⚙	○	○
Sourceforge.net	App	●	●	○	⚙	○ But UI Support	●
Squarespace.com	App	●	●	○	⚙	● Specific FAQ	●
Steampowered.com	Email	○	○	○	-	● Direct Form	○
Stripe.com	SMS	●	●	○	⚙	● Direct Form	●
Teamviewer.com	App	●	●	●	▭	● General FAQ	●
Telegram.org	Password	●	●	○	⚙	● Direct Form	●
ThemeForest.net	App	●	●	○	⚙	○	○
Tiktok.com	SMS	●	●	●	▭	○	●
Tinyurl.com	App	●	●	○	⚙	○ But UI Support	●
Tradingview.com	SMS	●	●	○	⚙	● Direct Form	●
Trello.com	App	●	●	●	▭	● Direct Form	●
Tumblr.com	SMS	●	●	○	⚙	○	○
Twitch.tv	SMS	●	●	○	⚙	● Specific FAQ	●
Twitter.com	SMS	●	●	○	⚙	● Direct Form	●
Unity3d.com	SMS	●	●	○	⚙	○	●
VK.com	SMS	●	●	○	⚙	○	○
Vimeo.com	Email	○	○	○	-	○	○
Wetransfer.com	App	●	●	●	▭	● Direct Form	●
Whatsapp.com	Password	●	●	○	⚙	● Direct Form	●
Wixsite.com	Email	●	●	○	⚙	○	○
Yahoo.com	SMS	●	●	●	▭	○ But UI Support	●
Zendesk.com	SMS	○	●	○	⚙	● Specific FAQ	●
Zoom.us	SMS	●	●	●	▭	● General FAQ	●

Table 2: Overview of help a user gets during setup and recovery of a second factor. ○: The service does not include the characteristic. ●: The service fulfills the characteristic.
Except for one, all services that offered the user to use a backup during login but did not provide a backup possibility send the code to the email/phone number used to register. One service did not have clear backups but suggested using backup codes during login.