# The Never-Ending Story of Authentication

## Investigating Password Composition Policies and Second-Factor Recoverability

Dissertation

zur

Erlangung des Doktorgrades (Dr. rer. nat.)

der

Mathematisch-Naturwissenschaftlichen Fakultät

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von


**Eva Tiefenau**

aus

Bad Nauheim


Bonn, August 2024

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

Gutachter/Betreuer: Prof. Dr. Matthew Smith
Gutachter: Prof. Dr. Michael Meier

Tag der Promotion: 02.12.2024
Erscheinungsjahr: 2025

# Abstract

Authentication is an area where users regularly encounter IT security, and it has been studied in the field of usable IT security for at least 25 years. There are numerous proposals and ideas to improve the IT security of personal accounts through various mechanisms aimed at preventing unauthorized access.

This work aims to explore two of these mechanisms: password composition policies, which restrict password choices, and two-factor authentication (2FA), which requires two different factors for users to log into an account.

Regarding the first topic, this work presents the results of a survey conducted in German companies to understand the use of various elements in password composition policies and to investigate the challenges faced by decision-makers in creating such policies. By repeating the survey annually over four years, it was possible to observe the development of certain elements, such as enforcing regular, time-based password changes. This approach was recommended in the BSI guidelines in the first year of the survey but was changed shortly thereafter, advising against password expiry. This led to a decline in companies enforcing regular changes, though some continued to require them. The difficulties in implementing the new recommendations were often due to technical hurdles and lack of resources.

The second topic of this work is 2FA, specifically how account recovery is handled when 2FA is enabled. While access to accounts protected only by a password can often be restored via email, access to accounts with 2FA should be better secured to justify the increased IT security. At the same time, the requirements for legitimate users should be easy to implement. The first part examines the user interface and processes on 78 high-traffic websites during 2FA setup and account recovery. It was found that the protocols and support users receive vary greatly from website to website.

Building on these results, the following study investigates users' backup strategies and their expectations for account recovery on websites. The findings suggest that only a minority would be able to recover their 2FA-protected accounts if the websites do not accept personal information as proof of identity.

Combining these results with the insights from the processes and protocols on websites shows that there is significant potential for improvement in the area of account recovery.

# Zusammenfassung

Authentifizierung ist ein Bereich, in dem Nutzende regelmäßig mit IT-Sicherheit konfrontiert werden, und der seit mindestens 25 Jahren im Forschungsfeld der nutzbaren IT-Sicherheit untersucht wird. Es gibt zahlreiche Vorschläge und Ideen zur Verbesserung der IT-Sicherheit von persönlichen Konten durch verschiedene Mechanismen, die unbefugten Zugriff verhindern sollen.

Diese Arbeit zielt darauf ab, zwei dieser Mechanismen zu erforschen: Zum einen Passwortrichtlinien, die die Auswahlmöglichkeiten eines Passworts einschränken, und die Zwei-Faktor-Authentifizierung (2FA), bei der zwei verschiedene Merkmale benötigt werden, damit Nutzende sich bei einem Konto anmelden können.

Zum ersten Thema präsentiert diese Arbeit die Ergebnisse einer Umfrage, die in deutschen Unternehmen durchgeführt wurde, um die Verwendung verschiedener Elemente in Passwortrichtlinien zu verstehen und die Herausforderungen zu untersuchen, denen Entscheidungsträger und -trägerinnen bei der Erstellung solcher Richtlinien begegnen. Durch die jährliche Wiederholung der Umfrage über vier Jahre hinweg war es möglich, die Entwicklung bestimmter Elemente zu beobachten, wie beispielsweise das Erzwingen eines regelmäßigen, zeitbasierten Passwortwechsels. Dieser Ansatz wurde im ersten Jahr der Erhebung im BSI-Grundschutzkompendium empfohlen, aber kurz danach geändert, sodass seitdem von zeitbasierten Wechseln abgeraten wird. Dies führte zwar zu einem Rückgang der Unternehmen, die regelmäßige Passwortwechsel erzwingen, doch einige fordern ihre Nutzenden und Mitarbeitenden weiterhin dazu auf. Die Schwierigkeiten bei der Umsetzung der neuen Empfehlungen waren oft auf technische Hürden und fehlende Ressourcen zurückzuführen.

Der zweite Teil dieser Arbeit befasst sich mit Aspekten der 2FA, insbesondere die Frage, wie bei der Wiederherstellung von Konten mit aktivierter 2FA vorgegangen wird. Während der Zugang zu Konten, die nur durch ein Passwort geschützt sind, oft per E-Mail wiederhergestellt werden kann, sollte der Zugang zu Konten mit 2FA schwerer angreifbar sein, um der erhöhten IT-Sicherheit gerecht zu werden. Gleichzeitig sollten die Anforderungen für rechtmäßige Nutzer einfach umsetzbar sein. Im ersten Teil werden das Nutzerinterface sowie die Abläufe auf 78 stark frequentierten Websites während der Einrichtung von 2FA und der Prozesse zur Kontowiederherstellung untersucht. Es wurde festgestellt, dass die Protokolle und die Unterstützung, die Nutzer erhalten, von Website zu Website stark variieren.

Aufbauend auf diesen Ergebnissen werden in der folgenden Studie die Sicherungsstrategien der Nutzenden und ihre Erwartungen an Webseiten zur Kontowiederherstellung unter-

sucht. Die Ergebnisse legen nahe, dass nur eine Minderheit in der Lage wäre, ihre mit 2FA gesicherten Konten wiederherzustellen, sollten die Websites keine persönlichen Informationen als Identitätsnachweis akzeptieren.

Die Kombination dieser Ergebnisse mit den Erkenntnissen aus den Abläufen und Protokollen auf Websites zeigt, dass im Bereich der Kontenwiederherstellung im Falle des Verlustes des zweiten Faktors großes Verbesserungspotenzial besteht.

# Acknowledgements

There are people who, knowingly or unknowingly, actively or passively, academically or otherwise, helped make this thesis possible.

First and foremost, I would like to thank Matthew for giving me the opportunity to embark on this journey and for all his support, thoughts, and feedback over the past years.

I would also like to extend my gratitude to all my colleagues, co-authors, and students I met along the way. Thank you for the great discussions, the numerous lunch breaks, and the Zoom meetings that made home office a bit more bearable. To name a few: Thanks to Anna-Marie for keeping my blood sugar high, Kerrin for keeping me up to date on gossip and news about 'famous' people, Nina for the longest-lasting collaboration I've encountered, and Alena and Anastasia for welcoming me when I joined the group!

A special thanks to Maxi and Julia for the pub visits and sailing trips.

My deepest gratitude goes to Chris for being the amazing person you are (enumerating everything in detail would be a thesis in itself).

Huge thanks to Ve, Isabel, Lena, and Tamara for many hours of walks, several liters of coffee, hot chocolate, and tea, piles of pies, and big and small adventures.

Last but not least, thank you, Mom and Dad, for making me the person I am and supporting me in every decision.

*It's okay password,*
*I am insecure, too.*

# Contents

# Glossary

**BSI** : Bundesamt für Sicherheit in der Informationstechnik; Federal Office for Information Security, Germany. The "BSI as the Federal Cyber Security Authority shapes information security in digitization through prevention, detection and reaction for government, business and society." [59]

**NIST** : National Institute of Standards and Technology, America. Their goal is "[t]o promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." [128]

**2FA** : Two-factor authentication. A user needs to provide two different ways during login to prove their identity. The two different factors have to come from two distinct categories from the possible three: something the user *is* (e.g., fingerprint), something the user *has* (e.g., a device), something the user *knows* (e.g., a password) [82].

**MFA** : Multi-factor authentication. At least two factors are needed to log in to an account. More generic term for 2FA.

**RBA** : Risk-based authentication. During login, a risk factor is calculated based on a user's typical behavior, such as their IP address or location. If a certain risk factor is exceeded, a user could, e.g., be prompted to confirm their login attempt via mail or SMS, or the login could be blocked. [65, 115].

**PKQ** : Personal knowledge question(s). These questions concern personal information and need to be answered while a user has access to their accounts, e.g., during account registration. They were often used in the past in case an account holder was not able to provide their normal authenticators (e.g., their password) [150]. They have been proven to be insecure, as they often consist of easily obtainable information [150].

# Chapter 1

# Introduction

As of 2024, around two-thirds of the world's population uses the internet [96], which often necessitates creating user accounts. Typically, this process is straightforward, requiring only an email address or phone number and a primary authenticator, such as a password. Protecting accounts with a password, first introduced in the 1960s [38], is intended to prevent unauthorized access to user data and user privileges. However, it is well known that users sometimes choose weak passwords and reuse them across multiple websites [170, 91, 164, 139, 31, 174, 176, 79], making it easier for attackers to gain access to accounts and the data stored within them.

There are various approaches to counter the selection of insecure passwords and improve overall account security, and this thesis explores two of them.

The first, commonly used by service providers (websites and companies), involves **password composition policies (PCPs)**. These policies restrict the types of passwords users can choose by, for example, preventing commonly used passwords or requiring a minimum length. Especially in companies, these measures should secure not only employees' data but also company data and secrets.

PCPs have been in use for at least 20 years [17], leading to a substantial body of research. This research includes analyses of end-user-facing PCPs on websites ([15, 175, 155, 142]) and studies on how users cope with various characteristics of PCPs ([95, 156, 118, 83]).

Findings from these studies have often informed recommendations by organizations such as the American National Institute of Standards and Technology (NIST) [82], the German Federal Office for Information Security (BSI) [48] or the Open Web Application Security Project (OWASP) [133]. These organizations provide guidelines to help companies select secure authentication mechanisms for their customers and employees.

While end-user-facing PCPs have been studied extensively, there is a research gap regarding their prevalence and usage in a corporate context, e.g., the rationale behind specific policy elements from the perspective of those responsible for creating PCPs.

This gap is especially interesting given that the BSI changed its recommendation regarding regular, time-based password changes in early 2020, shifting from recommending them to

not recommending them. This scenario presents an opportunity to investigate not only the policies in use but also the speed of adaptation to new guidelines, a topic that has been understudied in the field of usable security and privacy.

To shed light on current practices and the speed of policy adaptation to recommendation changes, we conducted a survey of German companies four times: once before the recommendation change and three times afterward, each approximately one year apart. We inquired about the authentication systems in use, and we asked detailed questions about password policies. Participants were recruited via the BSI newsletter, targeting a sample likely interested in IT security.

In 2019, we found high heterogeneity in the PCPs and a high prevalence of PCP elements that the research community and NIST consider harmful, such as password expiry and character class requirements. Following the recommendation change, fewer companies require a regular password change over the years (72% in 2019 to 45% in 2023). Participants whose companies still use a regular expiry often argued that this improves security or that there are additional guidelines by other institutions they must follow. Alternative checks were often not implemented due to resource constraints or technical hurdles.

The second approach covered in this thesis to improve account security is **two-factor authentication (2FA)**. In 2FA, a second factor (*secondary authenticator*) is required to confirm the user's identity, typically something the user *is* or *has* [82]. This is used in addition to the *primary authenticator*, typically something the user *knows*. Experts frequently advise non-tech-savvy users to use 2FA to stay safe online [93, 18], and its use has steadily increased in recent years, both for individuals [25] and within companies [71] (see Chapter 5). Some services even mandate the use of second factors [77] or are required by law to do so, such as banking websites in the EU [137].

Within several studies, participants repeatedly expressed the fear of losing the second factor [35, 99, 138] and there are indications that around 40% of smartphone users have had at least one incident in which they lost their device or had it stolen [12, 87, 107]. Given that personal smartphones are a convenient choice for 2FA [161], these numbers suggest that many users might find themselves locked out of their accounts if they lose access to their second factor.

While passwords can often be reset by accessing the connected email address [106], recovering a second factor should theoretically be more complex to maintain the increased security of 2FA. For bank accounts and company employees, recovery can typically be done through in-person verification, as the institution possesses extensive knowledge about the account owner. However, for services operating solely online that do not require extensive account owner information, account recovery becomes more complex.

To assess this complexity and related issues, the second half of this thesis focuses on second-factor recoverability. Initially, we conducted 78 expert reviews, examining current practices of online services and their assistance to users in regaining account access. We found that the investigated services lacked a common practice during both 2FA setup and recovery. Yet we managed to recover half of the accounts.

In a second study, we conducted 16 interviews and surveyed 95 participants to ask them about their current backup plans and their expectations regarding account recovery. We

found that only approximately half of the interview participants had considered the issue of losing their second factor or had experienced access problems, and even fewer had a backup plan. Many participants expected services to offer support and believed they could reach out for help with login issues.

This thesis makes the following contributions. In the first half,

- I present 259 password composition policies used in German companies between 2019 and 2023 and compare them to recommendations from scientific work and national organizations.
- I present and discuss reasons why companies do not or cannot comply with recommendations regarding expiry and alternative checks for account compromises.

In the second half,

- I present the recovery protocols for the second factor of 78 top-traffic websites, including the website's communication and usability concerning this topic.
- I estimate backup prevalence and account recovery probability among 16 interview- and 95 survey participants, highlighting a strong reliance on personal data and website support.
- I outline users' expectations, understandings, and feelings of responsibility regarding account recovery.

This dissertation is structured as follows:

In Chapter 2, I present the theoretical background and related work on which this thesis is based. I provide an overview of scientific and institutional recommendations on authentication and recovery and summarize the current status of these two topics for both companies and end users.

Chapters 3, 4, and 5 present survey studies conducted in German companies focusing on the employee-facing authentication process and the reasons for selecting specific mechanisms. Chapter 3 summarizes the method used, and Chapter 4 presents the results from the first survey distribution in 2019 and its implications, and Chapter 5 compares the results from several years, discussing reasons for not adopting new recommendations.

Chapters 6 and 7 investigate the recoverability of a second factor. I start by showing the process that is followed by websites when users lose access to their second factor in Chapter 6 and then examine how users cope with such a situation and their expectations from service providers in Chapter 7. Both chapters discuss implications for service providers.

# Chapter 2

# Background and Related Work

***Disclaimer:***
*Several contents of this chapter were previously published or are currently under review as part of the following four papers:*

- *"Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies" presented at the 17th Symposium On Usable Privacy and Security (SOUPS) in 2021 [71]. I worked on this together with my co-authors Maximilian Häring and Matthew Smith. This chapter uses text from the paper's related work section, for which Maximilian and I conducted an extensive literature review. We wrote the section iteratively together and it was revised by Matthew.*
- *"Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security" presented at the 19th Symposium On Usable Privacy and Security (SOUPS) in 2023 [72] together with my co-authors Maximilian Häring, Matthew Smith and Christian Tiefenau. I conducted a literature review for literature not included in or published after the previous paper. This chapter uses text from the paper's related work section, for which the first version was written by me (except for the adoption speed of HTTPS, which was written by Christian). The section was iteratively revised by Maximilian, Christian, and me.*
- *"Adventures in Recovery Land: Testing the Account Recovery of Popular Websites When the Second Factor is Lost" presented at the 19th Symposium On Usable Privacy and Security (SOUPS) in 2023 [70] together with my co-authors Maximilian Häring, Charlotte Theresa Mädler, Matthew Smith, and Christian Tiefenau. This chapter uses text from the paper's related work section, for which Charlotte and I conducted an extensive literature review. I wrote the first version of the section and it was iteratively revised by Maximilian, Christian, and me.*
- *"They are responsible for ensuring that I can continue to use the service. Investigating Users' Expectations Towards 2FA Recovery in Germany." This work is currently under review. I worked on this together with my co-authors Julia Grohs,*

> *Maximilian Häring, Matthew Smith, and Christian Tiefenau. This chapter uses text from the paper's related work section, for which Julia and I conducted an extensive literature review. I wrote the first version of the section and it was iteratively revised by Julia, Maximilian, Christian, and me.*
>
> *As all the following work was conducted with my co-authors as a team, this chapter will use the academic "we" to mirror this fact.*

The general topic of authentication can be researched from two different angles: First, how companies and services handle authentication, what methods they provide and support, and whether any additional rules are set. Secondly, one can study how end users cope with a given method and what their expectations are.

As authentication and passwords, in particular, were an early starting point for usable security [5], there is a large body of literature on various authentication aspects. Thus, this section only focuses on the topics relevant to this thesis: password composition policies and account recovery, especially if 2FA is used. It is not meant to be complete but to offer important context for the following chapters. We look into these topics from both above-mentioned angles: Once from an organizational side (i.e., companies that want to authenticate their employees) and second from an end user perspective.

The following section first summarizes current recommendations concerning authentication, both from research and national institutions in Section 2.1. We also estimate how fast we expect recommendations to be adopted. After this, we present a look into whether the recommendations are followed. We start with the current status of authentication in Section 2.2 and then present the status of recovery in Section 2.3.

Our work results from a research gap highlighted in this chapter.

## 2.1 Recommendations from Organizations and Science

Several countries have an institution that aims to support and guide end users and companies [59, 128, 58, 22]. Often, these recommendations are based on scientific results [82].

This section gives an overview of recommendations concerning authentication and account recovery for companies and end users, both from scientific work and different organizations.

### 2.1.1 Recommendations for End Users

Ideally, users would be unable to compromise the security of IT systems or would have to make a very deliberate choice to follow an insecure path. Unfortunately, this is not yet the case in all areas, which is why experts, e.g., the Federal Office for Information Security, recommend that end users adopt practices that help them to navigate the internet securely [61]. Parts of this often also relate to the area of authentication, and end users are advised to use strong, unique passwords (e.g., with the help of password managers) and

make use of 2FA if possible [93, 18, 60, 62]. In their article about 2FA, the BSI brings up the issue of a possible second-factor loss and recommends adding more than one second factor [62].

### 2.1.2 Recommendations for Service Providers and Companies

Companies and service providers have the potential to impact many people with their decisions concerning authentication, as they set rules for their employees and customers who want to or need to use their service. For this reason, it should be of high priority to choose methods and rules that are easily usable and lead to secure behavior at the same time.

In the following, guidelines for those handling and issuing electronic credentials are summarized.

#### Institutional Recommendations Regarding Authentication and Recovery

In Germany, where we sampled participants for survey studies within companies (as explained in Chapter 3), the Federal Office for Information Security (BSI) "is the National Security Authority and the chief architect of secure digitalisation in Germany" [55]. Once a year, it publishes an updated version of its IT-Grundschutz Compendium [49], which "offers a systematic approach to information security that is compatible with ISO/IEC 27001" [49]. The BSI additionally hands out implementation hints for some subsections, e.g., for identity and access management, including authentication [45].

Companies do not have any legal obligation to apply the IT-Grundschutz. Yet, it is one way to implement ISO 27001 in order to get certified [49]. There are several reasons for companies to do this, e.g., reputation, risk calculation, and compliance. Certification is valid for three years, with yearly audits [63]. Therefore, changes to the compendium should be implemented in the industry at the latest after three years.

We sent out the first survey in 2019 and the last one in 2023 (see Chapter 3). As the BSI adapted their recommendations at the beginning of each year, five versions are of interest for this work [47, 48, 51, 53, 54].[1] Relevant for this work are recommendations towards password composition policies (PCPs), multi-factor authentication, and account recovery (i.e., password and/or multi-factor reset), as found in "ORP.4 Identity and Access Management". The recommendations for the first two changed only once in 2020, and for password and/or multi-factor reset, all versions are identical. An overview of all elements relevant to this work is depicted in Table 2.1 and explained in the following.

Regarding **PCPs**, the guidelines in the compendium (since 2020) are quite vague and state that "Passwords MUST be sufficiently complex so that they are difficult to guess. Passwords MUST NOT be so complex that users cannot utilise them regularly with a reasonable amount of effort [50]. It additionally states that "Passwords that are easy to guess or are

[1] English versions are only available for the versions from 2019 [46], 2021 [50], and 2022 [52].

kept in common password lists MUST NOT be used [50]."[2] The implementation hints are more specific and recommend not using words from the personal or work environment and comparing the passwords to lists of leaked passwords. It also suggests combining complexity and length requirements (e.g., 8-12 characters + 4 character classes or 20-25 characters + two character classes) [45].

In 2019, it stated that "[the organization] MUST specify that only passwords of sufficient length and complexity are to be used [46]".

While in 2019, the compendium included a passage stating "The passwords SHOULD be changed at appropriate intervals" [46], this has changed at the beginning of 2020. Since then, users should only be prompted "to change their passwords with a valid reason. Changes based on the passage of time alone SHOULD be avoided. [50]" Instead, mechanisms must be implemented to detect compromised passwords, e.g., detecting parallel logins from different systems or locations. Only in case these alternative mechanisms cannot be implemented should a regular change be considered [50, 45]. The guidelines lack specific implementation ideas for these alternative mechanisms. Looking at available products, it would for example be possible to check whether a password an employee wants to use is already leaked (e.g., [143, 89]) or get notified if new leaks occur that include specific email addresses or domains (e.g., [92, 89]) Additionally, there are ideas on how to automatically classify and extract threat intelligence information concerning identity breaches to, e.g., support security analysts [110].

While all versions of the BSI guideline include a passage about considering **multi-factor authentication** for accounts with increased protection needs, in 2020, the BSI also added a paragraph about multi-factor authentication concerning all user accounts: "[the organization] MUST consider whether passwords are to be used as the sole authentication method, or whether other authentication features or methods may be used in addition to or instead of passwords [50]". In 2021, a new passage about dual control for administrative activities was added [50].

Concerning **recovery**, the compendium only includes a passage considering resetting passwords, stating that "[a]n appropriate and secure procedure SHOULD be defined and implemented." It further specifies that "[i]n case of higher password protection needs, a strategy SHOULD be defined for cases in which a support staff member cannot accept responsibility for providing a password due to the lack of secure options available." [50] The implementation hints offer thoughts concerning several different ways of how a password reset should take place, e.g., by letter, via phone, or personal contact. They mention measures on how to make sure the requester is the correct person, e.g., that the voice of a person must be known by the IT staff if reset over the phone is possible, or that security questions can be included, but that they should not be easily obtainable from public knowledge [45].

Yet, neither the compendium nor the implementation hints offer guidance on how to deal with the loss of a second factor.

[2] At the time of writing, the English version of the 2024 version has not been published. The quotes are taken from the English translation of the compendium from 2021. The quoted passages of both German versions are identical.

Chapters 4 and 5 investigate how German companies handle employee authentication. We assume that many will act according to the recommendations given by the BSI.

The US American equivalent of the BSI, the National Institute of Standards and Technology (NIST), gives more specific advise and recommends that user-chosen **passwords** should at least be eight characters long and shall be compared "against a list that contains values known to be commonly used, expected, or compromised" [82], e.g., passwords from previous leaks, dictionary words, repetitive or sequential characters, and context-specific words. Since 2016, the recommendations have advised against requiring periodical changes [81], and only force a change if there is evidence for a compromise. Verifiers "SHALL implement controls to protect against online guessing attacks" [82]. NIST also mentions techniques such as risked-based authentication using IP addresses, geolocation, and browser metadata as a measure to reduce the risk of an attacker locking a legitimate user out of their account as a result of rate-limiting.

NIST differentiates between three Authenticator Assurance Levels (AALs). The higher the level, the better capabilities and resources an attacker needs to have to undermine the authentication process. According to NIST, single-factor authentication is appropriate for AAL1. AAL2 and AAL3 require **multi-factor authentication**.

For the topic of **recovery**, NIST mentions that "it is essential that it not be possible to leverage an authentication involving one factor to obtain an authenticator of a different factor." [82]

Chapter 6 analyzes the recovery protocol of top-traffic websites. Many of these have headquarters in the United States of America, and their protocols are likely to be oriented at the guidelines given by NIST.

#### What Science Says About Password Composition Policies

Over the last years, several researchers have experimented with different elements often seen in PCPs, trying to understand their implications on usability and security [166, 98, 95, 83, 157, 156], as summarized in the following.

**Length and Complexity** Komanduri et al. [98] studied password strength and user sentiment across four password composition policies in 2011. For this, they invited 5000 people to participate in an online study where participants had to create a password that they had to recall two days later. The policies requested a certain length (8 vs. 16 characters) either alone, with an additional complexity requirement, or the non-existence of dictionary words in the chosen password. They found that participants across all conditions used at least 2.2 digits, while symbols were mainly only used if a policy requested to do so. Also, requiring a high complexity led to passwords with a higher entropy than other policies. At the same time, high complexity and the ban of dictionary words made password creation more complicated, with only 17.7% of participants being able to create a password in one try compared to the 52 to 84 % with other policies. The authors noted a correlation between storing passwords and the use of higher-entropy passwords. Of the four tested password

| | **NIST** (2020)[82] | **BSI Old** (2019) [46] | **BSI New** (since 2020)[48] |
|---|---|---|---|
| **Policy Elements** | | | |
| Quality | - | - | Appropriate |
| Minimal length | 8 | Sufficient | - |
| Minimal maximal length | 64 | - | - |
| Complexity | Advised against | Sufficient | - |
| Maximal age | Advised against | Appropriate | - |
| Allowed characters | All ASCII & Unicode characters | - | - |
| Blocklist | At least: | - | Easy to guess |
| | - Leaked passwords | | Common passwords |
| | - Dictionary words | | Reused passwords |
| | - Repetitive or sequential characters | | |
| | - Context-specific words | | |

**Table 2.1** – Recommendations for password policies by different organizations, split by their elements. The BSI revised their recommendation in 2020.

composition policies, the one asking for at least 16 characters but not requiring anything else seemed to be the best trade-off between usability and security of the resulting passwords.

The same approach was followed by Kelley et al. [95] in 2012, Shay et al. in 2014 [156] and 2016 [157], and Tan et al. [166] in 2019. Kelley et al. [95] tested the effect of policies of different lengths and complexities as well as the presence of password blocklists, which varied in size and complexity. They found that larger and more complex blocklists lead to stronger passwords. Shay et al. [157] examined 15 password policies by inviting 20,000 participants. Their password composition policies included policies that required only a minimal length or a length in combination with complexity or a certain number of words. The authors found that requiring a longer password with less complexity made it easier for participants to create and recall them while being less likely to be guessed. While experimenting with password blocklists, they noted that substring blocklists made passwords more secure without making recalling them more difficult. Policies that only requested minimal lengths were found to be usable; however, many of the resulting passwords were very weak. Additionally, the authors found the frequently used PCP consisting of a minimum of 8 characters and one character of each character class to be less usable and secure than some other tested policies. Based on their findings, the authors also gave recommendations for service providers regarding password composition policies.

Tan et al. [166] tested 21 policies, including composition requirements, blocklist requirements (using different lists and four different matching algorithms) and minimum-strength requirements (i.e., the number of guesses needed). During creation, a password meter showed compliance with the requirements and gave additional hints on how to increase the security once compliance was met. The study was completed by 6477 participants. The

authors found that character-class requirements are annoying while simultaneously resulting in passwords that can be easily cracked using state-of-the-art password-cracking tools. They additionally saw usability differences when comparing different blocklists and found no benefit of requiring four character classes in addition to a large blocklist. They recommend using a minimum-strength requirement in combination with a length requirement and rate the benefit of minimum-strength higher than blocklists in protecting against offline attacks.

According to current knowledge, the best combination seems to be one of a minimum length requirement combined with a minimum strength requirement (policies that require the password to exceed a strength threshold) or, if the latter is not possible, a carefully configured blocklist [166].

**Password Expiry** For a long time, it was recommended that users change their passwords regularly for two reasons: first, if the passwords were ever leaked, chances were high that the list was already outdated when an attacker got access to it. Second, attackers would need more time or computing power to brute force passwords. For the latter, 90 days was often seen as a reasonable trade-off that would make it impossible for attackers to guess the passwords in time but still be usable enough for users [165].

The usability and security implications of password expiry have been studied several times.

Looking at usability, findings suggest that users have trouble recalling new passwords and find forced password updates annoying [158, 90, 84, 26].

Security-wise, studies show that password expiry does not seem to offer the security benefit it was thought to have. Many people simply modify the accounts' current password or reuse a password from another account [158, 179, 84, 24]. In 2010, Zhang et al. [179] examined whether password expiration meets its intended purpose. For this, they analyzed a data set consisting of 7700 accounts. They found that 41% of the new passwords can be broken with knowledge about previous passwords for the same account within seconds, and 17% of the accounts can be broken into with five online password guesses.
Habib et al. [84] found that 67% of the participants from an online survey self-reported creating their new password by modifying their previous one; most prominent was capitalizing a letter, which was done by 30%. Still, according to self-reports, regular password changes do not seem to lead to weaker passwords. 82% of the participants agreed that frequent password expiration secures accounts against unauthorized persons.

Additionally, credentials are often used within hours after compromise [6], which cannot be prevented by a regular password change.

**Influence of Bad PCPs on Mood and Productivity** Studies have shown that password composition policy (PCP)s do not only influence the memorability and security of the resulting passwords but can also go beyond: Inglesant et al. [90] let 32 staff members of two different companies keep a password diary for one week and interviewed them regarding the details of each password. They found that the policies existing in 2010 were too complex, which, in the worst case, harmed the (organizational) productivity. A study by NIST

looked at the behavior of over 4000 employees of the Department of Commerce in 2014 and estimated that they spent over 12 hours per year if passwords needed to be changed every 90 days and over 18 hours per year if passwords needed to be changed every 60 days [26].

In a study of passwords collected from over 25.000 members of their university, Mazurek et al. [118] found the passwords of people who were annoyed by the complex password composition policy to be weaker compared to those who were not annoyed.

### 2.1.3 Recommendation Adoption Speed

After a recommendation is released by, e.g., institutions like NIST, or research, adoption takes time [120, 42, 7, 144] as the people in charge of implementing it are unaware of the recommendation [120], have no time [105, 167], or do not have the necessary knowhow [120]. In many IT security-related topics, technology has changed over the years, and with it, the knowledge of what is secure or usable secure.

To understand how fast the knowledge about best practices takes to reach those in charge of using this information, we highlight this process for two examples: deprecated hashing algorithms and HTTPS.

#### Deprecated Hashing Algorithms

One security-related area that encounters constant changes in recommendations is hashing. Algorithms get deprecated because they were found to be broken [160] or key lengths have to be increased due to the rising computing power [124]. In 2008, it became clear that MD5 was broken [160] and should thus not be used for storing passwords. Despite this being public knowledge for more than ten years now, some developers seem to be unaware of this fact. In a 2019 study, Naiakshina et al. [120] asked freelance developers to implement the password storage functionality for a website. Over 20% of the participants used MD5 (18% even stored the passwords in plain text/Base64 encoded). Using the same task, Naiakshina et al. found that MD5 was also used within a sample of computer science students [121] and developers within companies [119]. Danilova et al. [33] asked participants to review the program code and included insecure password storage (such as MD5). Only 36% pointed out this problem, and one even mentioned MD5 as a hash algorithm to improve security. Ntantogian et al. [126] investigated the default password hashing scheme of 25 content management systems and web application frameworks in 2018. MD5 was the default hashing scheme for around 27% of the analyzed CMS.

This problem can also be seen when looking at the database of "Have I been pwned" [144]: around 30% of the datasets that included passwords and that were breached in 2021 or 2022 used MD5 for password hashing; for datasets leaked in 2023, only 15% included MD5.[3]

[3]Based on the information available in July 2024.

#### HTTPS

In 2015, the W3C Technical Architecture Group encouraged the use of HTTPS instead of HTTP [172]. At this point, only around 32% of all pages visited by Firefox browsers supported HTTPS. Around that time, Let's Encrypt was founded and, for the first time, enabled server owners to acquire TLS certificates for free [154]. The updated recommendations, in combination with the easier access to certificates, led to the fact that, in 2022, seven years later, the percentage of servers that supported HTTPS grew to nearly 80% [42], and most (79,8%) of the web servers specifically allow only HTTPS-connections [173].

Even though 80% is the majority, this, in turn, also means that one-fifth of the servers still do not support TLS-secured connections. This can be due to compatibility reasons or an administrator's incorrect mental model of the technology [7, 100].

## 2.2 The Status of Authentication

This section summarizes how authentication is currently handled, what methods are used, and what issues are faced. Especially Section 2.2.2 is meant to set important context for Chapters 3, 4, and 5, where we investigated authentication in German companies and how a recommendation change impacted them.

### 2.2.1 End Users

Generally, it is hard to estimate how many accounts an average user owns and, thus, for how many accounts users need to handle some kind of authentication mechanism. Still, some questionnaires were conducted to shed light on this. One study from 2024, for example, reports that users have, on average, 168 accounts [171], and it seems that the COVID-19 pandemic increased the number of accounts a person has [31]. Additionally, there seems to be a huge variety in account numbers per user, as in another study, around 30% of the respondents reported that they have no idea how many accounts they own, as there are too many, while another 30% reported to have less than 10 [108]. Looking at the number of websites that require a password entry on a day-to-day basis, a study found that participants visited around 26 different web domains that required authentication within 90 days in 2017 [139], and in another study, the median user visited 16.5 websites within 6 weeks in 2016 [176].

Regardless of specific numbers, it can be assumed that many people who use the internet regularly are in some form of regular contact with authentication.

One common approach is to use passwords, and the number of users using 2FA has increased regularly over the last years [25]. Some services even enforce 2FA for some of their users [112, 76] to decrease account compromises [97] or are required by law to do so [137]. For 2FA, the smartphone currently seems to be the most used approach, by either receiving a code via SMS or using authenticator apps [161].

Apart from pure numbers, several studies investigated how users cope with different authentication mechanisms.

To understand common password patterns and users' misconceptions about password strength, Ur et al. [170] asked 49 participants to create an account for fictitious banking, email, and news websites while thinking aloud. The authors found that while some weak passwords were created consciously, most were a result of misconceptions, e.g., that a "!" at the end makes a password more secure or that hard-to-spell words are more secure than easy ones. Additionally, many participants demonstrated misconceptions regarding possible attacks, believing that personal data as passwords is secure as long as it is not known publicly. When confronted with policies that required the participants to add numbers or symbols to their password, which they had not included before, many simply appended one to their password.
Stobert et al. [164] found participants often chose their passwords based on personal goals, beliefs, or information associated with the website.

Apart from the creation process, several studies have repeatedly shown that users tend to reuse their password (exactly or partially) [139, 31, 174, 176, 164] and that passwords are even commonly continued to be used and reused if they are leaked [174, 79]. Frequently entered passwords and complex ones seem to be reused more often [176].

For 2FA, a lot of literature was conducted to understand how users cope with 2FA methods, initial setup [147, 148, 30, 3], and what impacts acceptance [177, 35, 148, 34]. Generally, it was found that many 2FA systems offer good usability [147, 148] and that users sometimes reported that it was easier to use than expected [30].

Studies also found that users often lack the correct terminology when it comes to authentication and show misconceptions about authentication measures [102, 5, 9, 99, 37].

### 2.2.2 Authentication in Companies and on Websites

In this section, we look at literature concerning the current state of authentication in companies and on websites and how the decision process for PCPs looks.

In 2010, Florêncio et al. [57] examined the password policies of 75 websites, including top, high and medium traffic sites as well as banks, universities and government sites. They calculated the minimum strength of each password policy using the cardinality of the minimum character set required and the minimum length given in the policy. Afterward, they analyzed if different characteristics correlate with stronger password policies but found no correlation between the website's size, the number of users, or the frequency of attacks. Instead, they noted a strong inverse correlation between password policy strength and sites that accept advertising and sponsored links. The authors hypothesized the necessity of those websites to have high usability to keep users on their site.

Mayer et al. [117] replicated and extended this study in 2016 by analyzing the password policies of the same websites as visited by Florêncio et al. and additionally investigating a corresponding sample of German websites. They noted that the average strength of the password policies had grown significantly in the US, except for websites that display third-party advertisements. In all samples, an inverse correlation was found for users visiting

a website with a clear competitor regarding their service. While comparing the password policies of German websites and those from the US, the authors noted a much smaller median of policy strength on German websites, with especially weak policies on banking websites.[4]

At the beginning of 2019, Gautam et al. [67] extracted and analyzed the password composition policies of 270 websites with the highest ranks in ten different countries. They compared the policies to the recommendations of NIST and found that only around 40% followed the recommended minimum length of 8 or more characters, while more than 70% had an unnecessary maximum length requirement. Two-thirds did not enforce certain character classes and thus followed the recommendations.

Lee et al. [104] analyzed 120 of the most popular websites in 2021 and compared the password policies to current best practices from academia: blocking common passwords, requiring specific character classes, and using a password meter to provide feedback on the security of a password. They found that 60% of the websites do not prevent the usage of the most common passwords at all, and a further 15% seem to use a very limited blocklist, thus still allowing many easy-to-guess and leaked passwords. Contrary to recommendations, 45% of the websites required specific character classes. Only 19% used a password meter of any sort. Interestingly, the authors captured 73 distinct password policies among the 120 websites.

Going beyond passwords, it can be seen that additional and alternative methods are not already used everywhere: 2FA was found to be supported in less than half of 208 popular websites [68], and passkeys are even less prevalent [1].

Looking at employee authentication, in 2022, Hypr, a company aiming for passwordless authentication, conducted interviews with 500 IT decision-makers within financial services organizations in Europe and the United States of America. They found that 32% use 2FA for their employees, while 22% use only the username and password [88].

To understand more about authentication in companies, we surveyed German companies, as explained in Chapters 3, 4, 5.

Another paper closely related to our studies presented in Chapter 4 and Chapter 5, but conducted after our work, is that of Sahin et al. [149]. They interviewed eleven website administrators to understand what considerations impact the PCPs they employ and what challenges they face when doing so. The authors found that administrators often face design challenges, competing interests, and deployment challenges. We build upon their work by a) recruiting a larger sample and b) focusing on security professionals within a company. In a professional context, accounts not only hold personal information about a user but might also give access to sensitive company internals. We believe the behavior of decision makers might be influenced by the fact that not only the company's reputation is at stake but also company secrets.

[4] It should be noted, though, that the login for customers is protected by rate-limiting. Further actions need to be approved by a second factor [152].

## 2.3 The Status of Account Recovery

If an authenticator for an online account is not available, either for a certain period or permanently, a user might need to look for alternative ways to gain access to their accounts. For password resets, most often, an email can be sent to the email address connected to the account in question [106]. However, before the work conducted for this thesis, it was mostly unclear what the situation looked like in case of an unavailable second factor.

In this section, we summarize work that sets the context for Chapter 6, where we analyzed the recovery protocol of websites, and Chapter 7, where we investigated users' expectations and backup plans.

### 2.3.1 End Users' Experiences with Loss and Account Recovery

Motivating our research area, studies found that participants are sometimes concerned about losing a second factor or its temporary unavailability, and thus potentially losing access to their accounts [36, 35, 99, 138, 37, 43]. Sometimes, this was accompanied by the fear of impersonation attacks after the loss or theft of this device [138].

This section seeks to give insights into the following areas: a) How often do users really lose their second factor? b) Do users have recovery plans? c) What do users think of different backup possibilities? d) what expectations do users have towards service providers if they lose their primary or secondary authenticator?

**Losing Authenticators and Losing Account Access** In the following, we report on how often users are confronted with the problem of losing their second factor.

For smartphones, which are the most commonly used second factor [161], 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%) [12, 87, 107]. One study estimated that an average person living in the UK loses two smartphones within their lifetime [20]. However, the authors did not report the frequency of users being able to recover their devices. For thistopic, data from 2014 show that while 90% of phone theft victims tried to recover their phone, only 32% were successful [107]. Furthermore, one study indicates that around 60% of the users who lost their device misplaced it, most often at home or work (49.5%) [85], locations where the likelihood of recovering the device is high.

Dutson et al. [41], and Abbott et al. [3] looked at implications for the users after their universities adopted 2FA. In the study by Dutson et al. [41], 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. [3] 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).

Höltervennhoff et al. [86] conducted a survey with users of an end-to-end encrypted email service provider and found that 29 of the 281 participants tried to recover this account in the past. The authors also analyzed support requests for this email provider on Reddit and saw that in six of the nine cases in which a user claimed to have lost access to their second factor, the user had also lost their recovery code. In one case, a user had lost both their password and second factor. In 37 cases, users lost both their password and recovery code.

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.

**Do People Have Backups to Access Their Accounts?** To the best of our knowledge, only three papers give insights into the question of whether people have backups for their online accounts that are secured with a second factor. Still et al. [163] conducted a survey and found that only 40% of their 103 participants have more than one device enrolled per personal account. Colnago et al. [30] analyzed the authentication log data of their university after 2FA was activated. Similar to Still et al., they found that, on average, each user uses 1.3 of the possible methods (push notifications, app-generated passcodes, and hardware tokens). Yet, in both studies, it did not become clear if the mentioned methods included backups or if any specific backup possibilities existed. Backup codes might, e.g., not have counted as another factor in the previous studies.

Apart from a dedicated backup method, personal information may also help to recover an account. In the paper by Colnago et al. [30], where the data of employees and students of a university were used, the IT helpdesk should likely be able to compare stored personal information to data provided by someone who lost their second factor.

Höltervennhoff et al. [86] surveyed 281 users of an end-to-end encrypted email service provider and analyzed 196 Reddit support requests related to access and recovery issues for accounts on this provider. They found that around 50% of their survey participants mentioned they would use a recovery code to access their accounts if they lost their password or access to their second factor. For the second factor, almost 20% mentioned the backup of an authenticator app, their device, or security key. As the participants were users of a security and privacy-centered service, the authors argue that their results likely represent an upper bound.

To gain more insights into the existence of backup plans (e.g., an activated backup or assuming to regain access by providing personal information), we asked the research question: *What backup strategies - if any - do users have for their 2FA accounts?* that we present in Chapter 7.

**What Backup Possibilities Do People Favor?** Some papers studied the usability of different recovery possibilities and captured users' preferences. As the literature is sparse, we present studies focusing on 2FA recovery, password recovery, passwordless recovery, and the basic usability of methods that might be used to recover a second factor.

*Personal knowledge questions (PKQ)* were found to be neither secure nor usable, as participants were often not able to remember their own answers but still gave answers that were

easily predictable [14, 150, 146]. *Recovery via trustees* was rated more secure than with backup codes [162], but in another study, it took much more time to conduct a recovery with trustees than with a PKQ or by using SMS or email [114]. Additionally, users do not seem to be good at memorizing who they chose as their trustee for a long time [151]. Recovery via *SMS and email* were generally rated as easy and were also quick in their usage [114]. These solutions were also more successful than PKQ [14].

Höltervennhoff et al. [86] asked security-savvy participants about their opinions on recovery codes and found that almost 66% of the participants deemed privacy more important than account access, even though the consequences of account loss were rated as severe by most. Recovery codes were rated as secure but less usable compared to methods like email or SMS recovery, or PKQ.

However, not all studies looked at the same methods, and some of the studies are several years old, with several technical changes and new possibilities since then that might also lead to a change in perception.

To add to this knowledge, we dive into the question of *What 2FA backup mechanisms do participants favor over others, and why?* in Chapter 7.

**What Do People Expect from Service Providers in Terms of Account Recovery?** While the literature gives indications on what properties users expect from an authentication method that can be used as a second factor (e.g., [116, 138]) and how easily different authentication schemes can be used (e.g., [147, 180, 30]), there is only limited literature on what users expect to happen if they lose their second factor. Höltervennhoff et al. [86] found that for an end-to-end encrypted email service provider, some users believed that the support would be able to support them in regaining access to their emails or restoring the list of their contacts, even though this is not possible.

Yet, it is unclear whether users feel responsible for making sure not to lose access, whether they expect the service to help them, or something in between. Payne et al. [138] found that one reason participants did not want to use Pico (an authentication scheme based on authentication tokens) was the concern about being personally more responsible for authentication and recovery. We assume that this concern might also affect users' expectations towards service providers.

Knowing about the users' expectations is important because only then can we compare them to the current situation on websites, as summarized in the following section, and direct further actions. By doing this, we might be able to prevent unwanted side effects from users that might negatively impact IT security. We, therefore, asked: *What expectations do people have of websites regarding account recovery? Who should be responsible for account access?* in Chapter 7.

### 2.3.2 Account Recovery User Journeys on Websites

Despite participants' concerns about losing a second factor or its temporary unavailability [36, 35, 99, 138, 37], the results of a study by Das et al. [35] indicate that websites might

not communicate the issue of loss well during the 2FA 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 added Yubikey in case it became unavailable.

To understand 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 analyzed websites in 2022 (see Chapter 6).

Additionally, we wanted 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. The following summarizes work that analyzed the recovery protocols (automatic or user-facing) if the primary or secondary authenticator was unavailable.

Li et al. [106] investigated the recovery protocols for the **primary authenticatior** 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 account to recover the account. On 4.6%, it was sufficient to know the answer to a security question.

Neil et al. [122] 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. [113] 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.

Büttner et al. [19] conducted an analysis of whether and how top traffic websites that use RBA also use Risk-Based Account Recovery (RBAR) when a user attempts to recover their **primary authenticator**. For this, the authors analyzed 5 Websites with different risk factors (e.g., IP addresses). They found that two of them did not make use of RBAR. One website added CAPTCHAs if the request came from an unknown IP address. The other two websites did not show consistency, probably showing that additional risk factors next to IP address and browser are used to calculate the risk status. Even though the authors did not investigate the recovery of a second factor and only conducted their analysis on a few websites, we suspected that RBAR might have influenced our results in Chapter 6.

Another related study was conducted by Quermann et al. [145], 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. [145] 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 this prior work in Chapter 6.

Most relevant to our work on 2FA recovery are two papers from 2023 that were published around the same time as our own work ([70] as presented in Chapter 6) and that provide additional insights into 2FA setup and recovery user journeys [10, 109]. In the following, we briefly summarize their results and how our and their results impacted our assumptions for Chapter 7.

Identical to our work ([70], Chapter 6), Amft et al. [10] found that several websites did not warn users during setup that they might lose their second factor or stayed vague in their statements. We thus expect that users might not be aware of this issue.

Depending on the used methodology and selected sample, the literature reports different numbers on how many websites offer a user to set up a backup for their second factor, ranging from 40% to 80% [70, 10, 109]. A minority of them forced the user to implement backups, but several nudged the user and explained why a backup might be important [70, 109]. Based on this, we assume some users have backups for certain services, but not all, and others may have none at all.

Amft et al. [10] and we ([70], Chapter 6) could regain access to around 50% of the accounts, e.g., by providing knowledge about the account or the account holder, by having access to the connected email address or by uploading an identity document. We included this knowledge in our study to understand what users would be willing and able to share during account recovery.

We and Amft et al. also analyzed help offered by the websites (during login or on their FAQs) and found that a minority directly helped the user in the fastest possible way [70] and that no FAQ matched the user experience [10]. Having this in mind, we explore the expectations users have for websites and account recovery in Chapter 7.

# Chapter 3

# Studying the Status Quo and Evolution of Authentication in Companies

***Disclaimer:***
*Most contents of this chapter were previously published as part of the following two papers:*

- *"Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies" presented at the 17th Symposium On Usable Privacy and Security (SOUPS) in 2021 [71]. I worked on this together with my co-authors Maximilian Häring and Matthew Smith. This chapter uses text from the paper's methodology section. The study was designed by Maximilian, Matthew, and me. Maximilian and I conducted the pilot study, and Matthew contacted the BSI for recruitment via their newsletter. The section was written by Maximilian and me and revised by Matthew.*
- *"Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security" presented at the 19th Symposium On Usable Privacy and Security (SOUPS) in 2023 [72] together with my co-authors Maximilian Häring, Matthew Smith and Christian Tiefenau. This chapter uses text from the paper's methodology section. Maximilian and I adapted the survey each year based on the results from the previous year and changed circumstances. Matthew and Christian gave feedback on the new and adapted questions. I contacted the BSI to ask them for inclusion in the newsletter. I wrote the initial version of the methods section in the paper, and it was iteratively revised by Maximilian, Christian, and me.*

*As all the following work was conducted with my co-authors as a team, this chapter will use the academic "we" to mirror this fact.*

To investigate the current state of password composition policies in German companies and to understand how quickly password recommendations from the BSI are adapted, we sent out surveys at four different times through the BSI mailing list. The surveys were aimed at people who are responsible for PCPs in German companies. The questionnaire was offered in German and English since employees at this level can be from an international context.

The first survey was sent out between September and October 2019, the second in October and November 2020, the third in February and March 2022, and the last in January 2023. For easier readability, we will refer to the surveys and datasets as follows: `PCP19` for data from 2019, `PCP20` for data collected at the end of 2020, and `PCP22` and `PCP23` for data collected at the beginning of 2022 and 2023. Figure 3.1 gives a graphical depiction of this timeline.

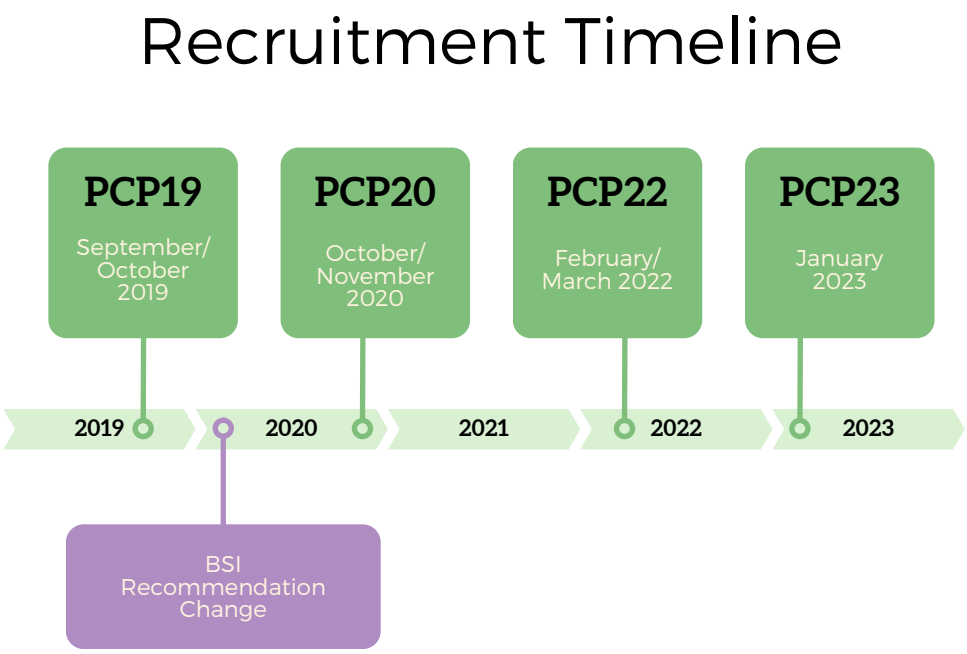


**Figure 3.1** – Time table of the recruitment process. "BSI recommendation change" concerns the major change in the recommendation concerning regular password updates.

This chapter describes the survey design, ethical considerations, and how we recruited the participants.

## 3.1 Survey Design

Since our target audience is usually very busy and extremely hard to recruit for research purposes, we paid special attention to keeping the survey as short as possible. Thus, our

survey was designed to take around ten minutes.

The survey consisted of five blocks, as presented in the following paragraphs. Each questionnaire differed slightly from the one sent out the previous year, adapting to new situations and gathering further insights. The survey is given in Appendix A.1, including annotations highlighting differences between the years.

**Account per Employee and Login** The participants were asked whether their company makes use of a centrally-managed account for each employee (Q1[1]), what services it can be used for (Q3a), what authentication methods can be used (Q3b, Q3c), and if two-factor authentication is possible (Q4). For those companies that did not have a centrally managed account, we opted to study the authentication methods for the company's email accounts, as we were fairly certain that most companies would use such a service. This way, we could include these companies and observe possible differences in these application areas.

**Passwords** The password section was shown to all participants, who indicated that the employee account was secured with passwords. If a company did not have such an account, all questions concerned email passwords. We asked the participants for their password policy (and encouraged them to provide a copy of it, Q6) and for elements allowed or forbidden in the password (Q16, Q17). The participants could indicate how the policies impact the security and usability of the overall authentication system and how often problems occur (Q26 - Q28).

Starting from `PCP20`, we also asked the participants whether there are additional specifications for particular user groups (Q18) and when and why the policy was changed last (Q22-Q25). Additionally, the changes in the BSI recommendations were brought up, and the participants were asked whether they looked into the changes and adapted their policy based on them (Q29, Q30). In 2023, we added further open-ended questions to understand if and why a company uses password expiry and how accounts are checked against a compromise (Q8 - Q14).

**Biometric Authentication and Hardware Token** All participants who indicated that the employee account could be unlocked using biometric authentication or a hardware token were asked for details (which biometric authentication is used (Q34) and whether the token supports FIDO2[2] (Q39)). Similar to the password part, they were asked for their perceived influence of the biometric authentication and token on the security and usability of the authentication system and the frequency of problems (Q35-Q37, Q40-Q42).

**Passwordless Authentication** We added one open-ended question in PCP23 asking for the general sentiments towards passwordless authentication (Q44).

[1] The notation Qx references to the corresponding question in our questionnaire.
[2] "Authentication standards based on public key cryptography for authentication" [8]

**Demographics** In the final part, the participants were asked for details about themselves and the company they work for. In PCP19, this included the total number of employees working for the company (Q52) and the number of employees working on IT security topics full-time (Q54). From PCP20 on, the participants were also asked for the sector (Q47), the country the headquarters of the company is located (Q51), whether it can be seen as Critical Infrastructure (Q48), as well as the position of the participant (Q55), and their years of experience (Q56). In all years, the participants indicated their satisfaction with the overall authentication system (Q59). From PCP20 on, they could also indicate that they participated in the survey the previous year (Q58), which only two people affirmed in PCP22.

## 3.2 Survey Testing

Since we set a strict time limit for the survey, it proved challenging to formulate short enough questions not to slow down the survey but also unambiguous enough to gather useful data. The initial survey underwent five internal iterations, and we conducted a pilot study with the VP of Security of a large multinational company and an administrator responsible for a small organization. We integrated the feedback from the pilot study into the final version of the survey.

Each year, we added new questions to adapt to changed circumstances. We discussed these new questions with colleagues who were not part of the survey creation process to make sure the changes in the survey could be understood correctly.

## 3.3 Recruitment

For the first survey in 2019, we tried different recruitment channels: a newsletter sent by the BSI, via contacts of two German digital associations (Bitkom [111] and Cyber Security Cluster Bonn [13]) and personal contacts. The most effective channel by far was the newsletter sent by the BSI ($n = 69$ valid data sets of 83 valid data sets in total), so we used only this recruitment channel in the following years.

Our survey targeted the person within the company responsible for the authentication system and the PCP. Since we had no way of contacting them directly, we clearly stated that only these people should fill out the survey and requested that the survey link be passed on to this person within the company. As we offered opt-out options, we believe that an accidental non-decision maker would have to have had malicious intent to affect the results negatively. Participation was voluntary and not compensated.

In the latest run in 2023, which also included the highest number of questions, participants took a median time of 16 minutes to finish the survey.

We collected between 72 (2020) and 122 (2023) answers per year.

## 3.4 Data Quality

Since we expected a heterogeneous set of PCPs and asked questions that are either sensitive or broad and thus may not apply to every participant, we included “Other”, “I do not wish to make a statement”, and “I do not know” options to questions (see also Section 3.5). This way, we wanted to prevent the participants from leaving after facing a question they could or did not want to answer.

We eliminated all incomplete answers from our analysis and one participant whose answers to open-ended questions indicated that they did not understand the questions correctly in PCP19. We further removed the response of one participant whose self-reported role does not clearly indicate being able to decide on the company’s authentication in the dataset of PCP20. Before analyzing the data, we checked for duplicate companies by using the company demographics and policies for each year. We saw nothing to suggest that one company participated more than once.

## 3.5 Ethics

Our university’s Research Ethics Board approved the study, and we adhered to the German data protection laws and the GDPR in the EU.

The companies were asked for details of their authentication methods and policies, which could give indications of vulnerabilities. To keep the risk of exposure low, we did not collect any information that could identify a company or individual.

Participants had to consent to their data being used for research before the study began, and we included the option "I don’t want to state" for all questions. Participants could drop out at any point in time.

The study included multiple open-ended questions. If a participant’s answer contained deanonymizing information (e.g., their company name), we deleted it before we continued the analysis.

## 3.6 Methodological Limitations

This work needs to be interpreted in light of the following limitations:

Even though we recruited the participants through the BSI newsletter and clearly stated who the survey is aimed at, we cannot be sure that only the responsible employee took part. From PCP20 on, participants were asked what position they held. Except for one, all participants who specified their role indicated working in a position with detailed domain knowledge about the company’s authentication system (see Table 5.3). Yet, especially for bigger companies, we cannot rule out that only one member of the IT security team took part in the survey. We checked for duplicates in the company characteristics in combination with the given PCP but could not identify any identical entries.

Using the newsletter sent by the BSI for recruitment may have caused the participants in the samples to be a) more interested in security topics and news than the average employee who is responsible for authentication and b) belong to an even more interested subgroup, as those are more likely to read the study invitation and follow it. As participation was voluntary and not remunerated, this effect was even heightened. We discuss the possible implications in Chapter 5.

Due to differences in company structures, there are likely questions that are not in the direct area of responsibility of the participants among the diverse set of questions asked. We tried to mitigate this with a clear statement at the start of the survey to ensure that at least password policies are present in this area. If the participant did not know the answer, there was the answer option “I do not know”.

All data are based on self-reports, and participants might have forgotten to include elements, especially for the password composition policy. We tried to counter this by asking them to copy and paste their policy.

It is possible that participants answered to be more socially desirable. To reduce this bias, we kept the surveys anonymous and asked for as little demographic data as possible.

As with any survey, participants may have selected the first answer that seemed appropriate without deeply thinking about their true beliefs and behavior. We tried to mitigate this by randomizing the answers wherever meaningful. We also designed the survey to be as short as possible. We aimed for ten minutes, which we almost achieved for PCP19: Here, participants needed, on average, eleven minutes to answer the survey. However, in the latest run in 2023, which also included the highest number of questions, participants took a median time of sixteen minutes.

Over the years, the survey was adapted, and questions were added. This could have caused participants to be in slightly different states of mind when answering questions. However, we included new questions only after similar questions had already been asked and included page breaks.

The survey for PCP22 contained minor improvements mentioned above, as well as an additional question about the reason for the existence of a password expiry that was not recommended by the BSI anymore at this point. After the newsletter inviting participants for PCP22 was sent and 36 participants had already completed it, we noticed that the questionnaire for PCP20 was handed out by mistake that did not include the changes and the additional question. We still decided to switch to the improved survey since we were confident that the additional insights from the new questions outweighed the minimal risk of receiving different answers due to the slightly modified questions.

# Chapter 4

# Password Composition Policies in German Companies in 2019

***Disclaimer:***
*The contents of this chapter were previously published as part of the paper "Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies" presented at the 17th Symposium On Usable Privacy and Security (SOUPS) in 2021 [71]. I worked on this together with my co-authors Maximilian Häring and Matthew Smith. This chapter uses text from the paper's introduction, results, and discussion section. The study was designed by Maximilian, Matthew, and me. The data was analyzed by Maximilian and me and the implications of the work were discussed jointly with all authors. The sections used in this chapter were iteratively written by Maximilian and me and revised by Matthew.*

*As this work was conducted with my co-authors as a team, this chapter will use the academic "we" to mirror this fact.*

## 4.1 Motivation

Passwords as a security measure are the daily reality of users working with computers, and even with technologies like FIDO2, they will likely stay for a while. It is well known that users sometimes choose weak passwords regarding their security effect. Websites and companies thus try to prevent this by using password composition policies (PCPs). These policies constrain the passwords users can choose, e.g., by preventing commonly chosen passwords. However, poorly chosen PCPs can be detrimental to usability and security [157]. A large body of work looks at PCPs in end user-facing websites, e.g., [15, 175, 155, 142], and how users cope with PCPs, e.g., [95, 156, 118, 83]. In this paper, we look at this topic from the view of those who manage PCPs. We conducted a survey with IT staff from 83 German companies. We focused on employee-facing PCPs since their passwords often protect accounts of great value for hackers (e.g., espionage or access to large amounts of user data).

To help companies with the creation of PCPs, organizations like the American NIST (National Institute of Standards and Technology) [82], OWASP (Open Web Application Security Project) [133] or the German BSI (Bundesamt für Sicherheit in der Informationstechnik, the German Federal Office for Information Security) [48] provide guidelines. To analyze if and how these guidelines affect the creation of PCPs, we surveyed what PCPs our participants used for company-wide user accounts or company email accounts and what information sources they used during creating the PCPs. We also surveyed what their experiences and perceptions of the PCPs are. We found a very heterogeneous set of PCPs with a surprising number of creative and unique PCP elements.

In this chapter, we:

- give an overview of the PCP landscape of 83 German companies.
- look at possible influences on and of PCPs.
- compare the identified PCP elements with recommendations.

## 4.2 Methodology: Data Analysis

We designed and conducted the study as explained in Chapter 3.

To analyze the PCPs that participants gave in an open-ended text entry, we used open coding as described by Corbin et al. [32].

Even though the policies mainly were enumerations of several elements and did not allow much room for interpretation (with few exceptions like "no *easy* passwords"), two researchers independently coded the policies to reduce errors. As suggested by Campbell et al. [21], we developed a codebook by coding a small set of policies (n = 10) separately and comparing the codes. This then served as a base for future codes. After coding all the remaining policies independently, the codes were compared, and the inter-coder agreement was calculated using Cohen's kappa coefficient ($\kappa$) [29]. Our agreement was 0,89. A value above 0.75 is considered a good level of coding agreement [56]. We were able to resolve all conflicts.

We found a large set of possible properties concerning a PCP, which we used to categorize each PCP based on its attributes (e.g., minimal length = 8 characters, minimal age = 1 day, maximal age = 90 days). We opted against calculating the strength of the PCPs as done by Florêncio et al. [57], and Mayer et al. [117], which only describes the theoretical size of the possibilities. It is also acknowledged by Florêncio et al. and Mayer et al. that this is not a good metric for calculating the resulting password strength. Instead, we discuss compliance with recommendations regarding PCPs from related work in Section 4.4.

This study contributes data with an exploratory approach guiding further research themes. Trends and interesting data were rarely tested on statistical significance to reduce the problems of multiple comparisons analysis.

When looking for statistical significance, we corrected the results with the Bonferroni–Holm method, also taking tests into account that we did but did not report. In the following sections, the stated $p$ is that after correction. Percentages are reported rounded.

After filtering, we were left with 83 complete, valid data sets, and 77 policies.

For analysis, we separated the 77 password policies by their usage for a centrally managed account ($n = 64$, in the following called PWA for "Password Account") and those applying for email accounts ($n = 13$).

## 4.3 Results

In the following section, we will present the results of the survey. First, we present the demographics and the authentication methods used by the participating companies. This is followed by an analysis of the present password composition policies and their different components with respect to Table 2.1.

We conclude this section with an overview of the potential impacts different authentication methods have.

### 4.3.1 Demographics

Table 4.1 shows the number of employees of the companies the participants worked for ($n = 83$). Table A.1 in the Appendix additionally depicts the number of desktop clients the participants had to handle, split by the company size.

We asked the participants what situations regarding their emails apply to their companies. 60 (72%) stated that employees can access their emails outside the company network. In 51 (61%) companies, emails can be accessed through a web login. In 28 (34%) cases, the employees do not need to know their password to access their emails, e.g., because of pre-configured mail clients.

On average, it took the participants eleven minutes to complete the survey.

| **Company Size** | **No. of Participants** | |
|---|---|---|
| | **Company-wide account** | **Email account** |
| 1-9 | 5 | 3 |
| 10-49 | 7 | 5 |
| 50-249 | 12 | 1 |
| 250-499 | 7 | 2 |
| 500-999 | 6 | 1 |
| >= 1000 | 30 | 3 |
| No answer | 1 | 0 |

**Table 4.1** – Number of participants by company size, split into those who answered the questions for the company-wide centrally managed accounts and those who answered for their email accounts.

### 4.3.2 General Authentication Setting

Of the 83 participants, 68 (81.93%) reported the use of company-wide accounts, of which all were secured at least with passwords. Ten (12%) companies additionally used biometric authentication (face recognition [n=2], fingerprint [n=7], and palm vein recognition [n=1]). One mentioned that face recognition is allowed on mobile devices. 29 (35%) participants stated that they use hardware tokens in addition to passwords. Eight (10%) participants reported they offer authentication with passwords, biometrics, and tokens. Apart from this, two (2%) participants mentioned (device) certificates.

15 (18%) of the surveyed participants do not use company-wide accounts. These participants answered questions regarding their companies' email passwords. We will look at these policies in Section 4.3.3.

### 4.3.3 Password Composition Policies

In the following, all presented results only refer to PCPs used for the companies' user accounts (for regular employees) unless stated otherwise ($n = 68$).

63 (93%) of the participants stated that users are allowed to set their own account password. Two (3%) mentioned that the password is given to the user and cannot be changed by themselves. We could not find any outstanding property for these two participants. In two (3%) cases, it is explicitly mentioned that an initial password is generated by the system and is changeable later; one company directly demands a change.

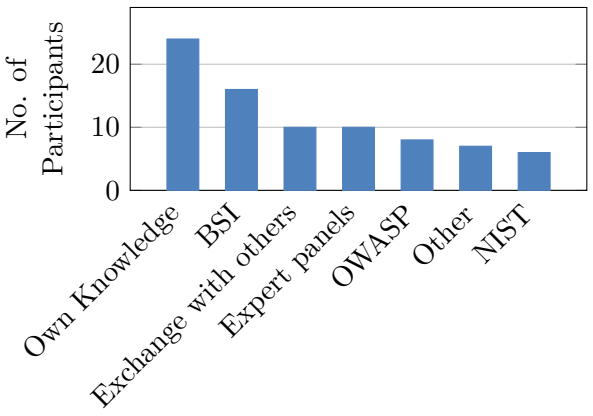


**Figure 4.1** – Sources of inspiration for the password composition policies reported from participants who took part in the creation (n=29, PWA). Multiple answers were possible.

From the 68 participants who use company-wide accounts, we could extract 64 password composition policies. The remaining participants did not define a policy but gave a general description of how a policy could look. 59 (92%) of the policies get enforced technically. In two of the four companies, where this is not the case, participants mentioned using awareness training for their employees to counter the problem of common passwords.

Twenty-nine (45%) participants were part of the password policy creation process, and 15 (23%) stated that the PCP was created by their predecessor.

As was expected based on the recruiting procedure, many (55%) participants who were part of the creation process of the password composition policy relied on the BSI as an influence

in the PCP creation process. Figure 4.1 shows which other inspirations were used by our participants who were part of the creation process. Some other sources mentioned were ANSSI (French National Agency for the Security of Information Systems), ISO 27001, and PCI DSS (Payment Card Industry Data Security Standard). The option "Expert Panels" did not concern any specific panel but was given as a non-explicit, "consulting with experts".

### PCP Components

In the following section, we present which elements were present in the PCPs that refer to companies' user accounts. For this, we follow the policy elements mentioned by official recommendations, as summarized in Table 2.1. An overview of the elements "minimal length", "password age" and "complexity" can be found in Table A.2 in the Appendix.

**Length** Sixty-one (95%) companies use length requirements to ensure a secure password. While a minimum length is widespread (54 companies, 84%), some participants also mentioned fixed lengths (11%). However, the data for maximal and fixed length was not always clear, for example, in the case of participants who stated: "Password length 8. [...]". In these cases, we count them as minimal and maximal length. In 33 (52%) companies, the participants mentioned eight characters as their minimal password length. Eleven (17%) companies require 10 characters, and 9 (14%) participants stated their minimal length to be 12 characters. Figure 4.2 gives an overview of how many participants mentioned which minimal length.

**Password Complexity** The complexity of a password depends on the number of character classes being used to create the password. For this, five different character classes can be used: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), special characters including the space character, as well as the remaining Unicode characters that are alphabetic but not uppercase or lowercase (e.g., Chinese symbols). The latter was only mentioned by one participant, who indicated the complexity as "Windows Password complexity," which includes all Unicode characters. In the following, we will concentrate on the first four character classes.

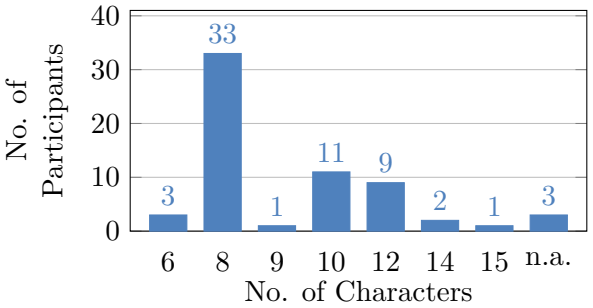


**Figure 4.2** – Minimal character length of passwords (PWA). "n.a." means no answer was given

Overall, 57 (89%) companies give constraints regarding the complexity. Seventeen (27%) companies require their users to build passwords using characters from all four classes. In one case, two characters of each class were demanded, one company requires a mixture of one or two characters per class, and in the other companies, one character of each class was sufficient.

Thirty-two (50%) participants mentioned that to fulfill their policy, characters from 3 of the four classes need to be present in a password. Fifteen (23%) specified which classes need to be covered, while 17 (27%) accepted a password as long as any three classes were present.

In five (8%) cases, participants stated that a complexity requirement is in place but did not specify how this requirement looks.

Seven (7%) of our participants did not mention any requirements regarding complexity. However, none of them explicitly mentioned not using one.

**Password Age and Password History** As suggested by the BSI during the time of our study, 45 (70%) of our participants stated to force their users to change their passwords regularly. The top three rotation cycles were 90 days (34%), 180 days (14%), and 365 days (11%). Two participants explicitly mentioned not using a password expiration. While the percentage for 90 days (34%) is similar to what Habib et al. [84] found (28%), our peak at 180 and 365 days cannot be found in their sample. All password rotation cycles can be seen in Figure 4.3.

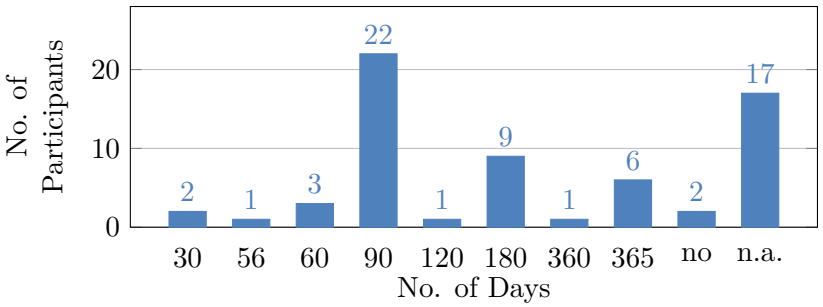


**Figure 4.3** – Password rotation cycle in days (PWA). "no" indicates participants who explicitly mentioned not using expiring passwords. "n.a." means no answer was given

Thirty (47%) participants reported a password history to prevent users from reusing previously used passwords. Twenty-seven (42%) of them check whether the passwords are identical, whereas three (3%) of the companies require significant changes, where it is, for example, not sufficient to increase a number within the old password to create a new one. Most mentioned was a history of 10 passwords (14 %) and 24 or 5 passwords (6% each). Figure 4.4 shows how many participants mentioned how many previous passwords are stored.

When presented with the need to change their password and not be allowed to reuse a certain amount of their last passwords, users might counter this by changing their password several times in a row until they are allowed to use their original password again [135]. Because of this, companies use a minimal password age, as mentioned by 15 (23%) participants, so that users cannot change their password within this time period [135]. The minimal ages range from 24 hours (eleven companies) to 14 days (one company).

**Allowed Characters** NIST [82] recommends allowing all printing ASCII characters, the space character, and Unicode characters for user-chosen passwords. As most participants

only mentioned which characters are not allowed or which classes should be covered, it is hard to draw reasonable conclusions about the allowed character sets. However, one participant mentioned that a password needs to cover the "Windows Password complexity", which includes Unicode characters, e.g., "from Asian languages" [136].

**Blocklists** Twenty-six (41%) participants affirmed the question of whether passwords were checked against common or leaked passwords. However, we did not ask for details, so we do not know how the comparison is made technically or which lists are used for this purpose.

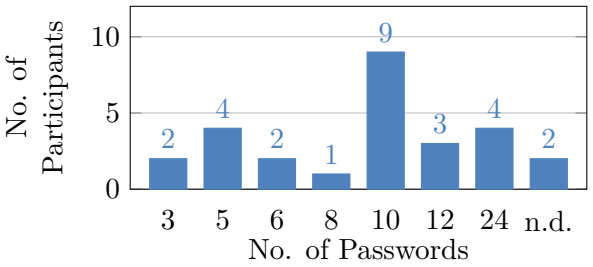


**Figure 4.4** – How many previously used passwords are not allowed to be reused (exact match). (PWA) "n.d." means no detail was given but a password history was mentioned.

**Rarely Encountered** We also found several constraints, which were only mentioned in at most three policies and were constraints to particular cases. We believe some of these are used since certain characters might break backend processing or serve as substitutes for blocklists (e.g., to prevent passwords consisting of personal information such as nicknames). These constraints included: (1) No colloquial language of any language, (2) No words of any language written backward, (3) Certain special characters like € or umlauts, (4) Not more than 2 characters or sequences in series, (5) The last 20 passwords need to differ significantly from the new password, (6) Not more than 2 characters which appear in the same series in your name, (7) Not your license plate number.[1]

### Additional Policies

In addition to PCPs that define the user's chosen passwords on company accounts, some participants also mentioned additional PCPs, such as those for administrator accounts.

All participants who do not use company-wide accounts answered the questions regarding their email accounts.

We will present both extra sets of PCPs in the following paragraphs. Both sets are excluded from the analysis above.

**General** Three participants mentioned two different password composition policies. Two of them applied stricter rules if an account belonged to an administrator. In both cases, the

[1] While this was only mentioned by two participants, it is mentioned in the implementation notes offered by the BSI [45].

minimal length was increased to 16 characters (while the regular accounts were required to use 12 and 10 characters).

One company requires its employees to use at least 20 character long passphrases for SSH and PGP/GPG keys.

**Email Passwords** Companies that do not use company-wide accounts for their employees were asked about their email passwords. We received 15 (18% of all responses) answers and were able to extract 13 password composition policies. Though we did not ask whether the PCPs are given by an email provider, six (46%) indicated they were part of the creation process. The primary influences were the BSI, own knowledge, and expert panels (each one mentioned three times).

The median minimal length mentioned by participants in this group was 10 characters (range from 8 to 30 characters). Three participants mentioned very large minimal lengths: One (8%) needed 20 characters, and one (8%) only accepts passwords if they are 30 or more characters long. Additionally, the modes of the complexity were 3 and 4 character classes, and the median of the rotation cycle was 180 days (range from 180 to 365 days).

Interestingly, three of the email participants mentioned that employees generate their passwords with a password generator, whereas only one participant from the account group said so.

We also found one company that differentiated between regular and administrator accounts. They increased the minimal length from 12 to 16 characters and decreased the maximum age from 90 days for regular employees to 45 days for administrator accounts.

### 4.3.4 Effects of Authentication Methods

We asked participants how they rated password, biometric, and token authentication concerning their security and usability impact and how often they encountered problems with the systems (e.g., forgotten passwords or lost hardware tokens). Additionally, we asked for their overall satisfaction with all the authentication methods they used combined. Following related work (Chapter 2), we assumed that unusable policies would lead to more problems and eventually to a lower satisfaction of the responsible person.

#### Influence on Security and Usability

Figure 4.5 shows what influences the use of the PCPs (n=64), biometrics (n=10), and hardware token (n=29) has on the sensed security and usability of the authentication system as well as how often problems arise for each method. It can be seen that, according to the participants, passwords lead to problems more often and form the lower bound of usability and security.

However, when comparing the scores, one has to keep in mind that biometrics and tokens were never used alone but always in combination with passwords. As we first asked for

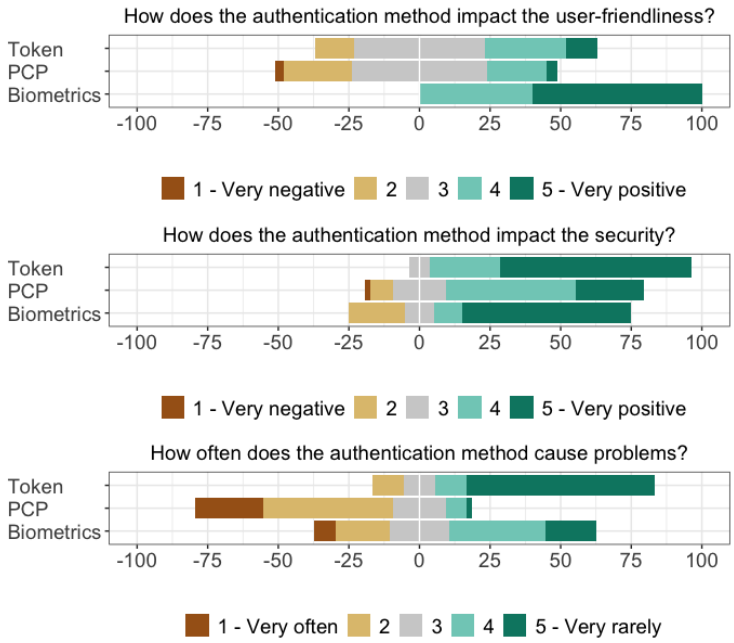


**Figure 4.5** – Impact of the different authentication methods: token ($n = 29$), the PCP ($n = 64$) and biometrics ($n = 10$) on the perceived user-friendliness, security and frequency of problems. Only PWA policies are used for the figures.

details about the password policies and only later for details of biometrics and tokens, the observed scores of biometrics and tokens may be compared to the security and usability of passwords. When looking at the number of problems arising from the authentication methods, tokens seem superior to biometrics and passwords. This is similar to the results of Abbott and Patil [3], who found tokens to have the second-highest UX rating when comparing different 2FA mechanisms.

We could identify a negative correlation between the reported impact on the security of the policy and the problems with passwords ($Spearman - \rho = -0.41294, p = 0.00938$), so the better the perceived security, the fewer perceived problems.

The connection between perceived user-friendliness and the problems is not statistically significant after correction ($Spearman - \rho = -0.3339, p = 0.05125$).

### Satisfaction of Authentication Methods

We asked participants how satisfied they are with the present overall authentication system. Figure 4.6 shows the observed scores depending on whether a company offers passwords alone or in combination with a token. Due to small numbers, we excluded those participants using passwords, biometrics, and tokens (n = 8) and participants using passwords and biometrics (n = 2). It seems that participants using passwords in combination with tokens are more satisfied than participants using only passwords.

When concentrating on passwords, participants who stated that they created the password

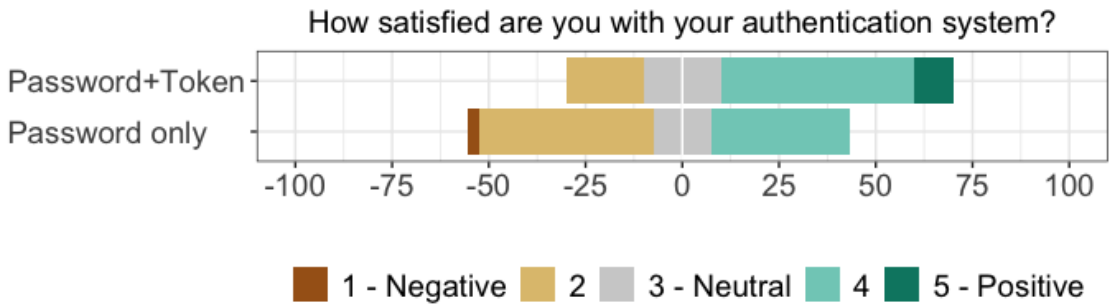


**Figure 4.6** – Satisfaction of participants with their overall authentication system, depending on methods in use: Passwords only (n = 33) and passwords in combination with token (n = 20). Numbers on the x-axis are percentages. Only PWA policies are used for this figure.

composition policy on their own had a median satisfaction of 4.00 (average: 3.41, sd: 0.95), while participants who were not part of the password policy creation had a median satisfaction of 3.00 (average: 2.94, sd: 0.92). This was not statistically significant (Mann–Whitney U test: $U = 624.5, p = 0.21824$).

However, a negative correlation can be reported between the number of problems with passwords and the satisfaction with the overall authentication system ($Spearman - \rho = -0.38639, p = 0.01409$); the fewer the problems, the more satisfied the participants.

### 4.3.5 Two-Factor Authentication (2FA)

If the participants stated that they use multiple mechanisms to authenticate accounts, we asked whether the methods are combined, for example, for 2-factor authentication. Of the 35 participants whose companies allow other methods than passwords, 18 stated that the methods are used as multiple factors, and five companies leave the decision which method to use for authentication up to the employees.

## 4.4 Discussion

In the following section, we discuss the results. For this, we first compare the PWA PCPs to recommendations given by organizations like the BSI or NIST. This is followed by comparing the PCPs to recommendations and lessons learned from related work. After this, we analyze factors that might have influenced the PCPs when being created.

### 4.4.1 Compliance with Recommendations and Usability

#### NIST and BSI

In the following section, we discuss and compare the password composition policies and their elements with recommendations by NIST and the BSI, as seen in Table 2.1. We can

only compare elements that are concretely covered by the corresponding guideline. The old BSI [46] guidelines do not make concrete recommendations regarding the length, complexity, or minimal password age and only require them to be "sufficient" or "appropriate". The same applies to the element "Quality", which was introduced with the new BSI recommendations [48] and is expected to be "appropriate". As the implementation notes [45] give concrete examples, we compare those to the policies.

We again want to point out that the old BSI recommendation included a password expiration period and a complexity requirement during the time of the study. At the same time, NIST did not have such requirements.

Anecdotally, one participant mentioned following guidelines given by the PCI DSS (Payment Card Industry Data Security Standard) but did not consider it reasonable.

**Length** NIST recommends at least 8 characters for user-chosen passwords. Thirty-three (52%) policies exactly fulfill this part, and 57 (89%) require 8 or more characters. Three (5%) companies go against this recommendation and require only six characters.

We cannot make any statement about the minimal maximum length of 64 characters mentioned by NIST. No participant mentioned fulfilling this, but again, this does not mean that the companies only allow shorter passwords.

**Complexity** NIST recommends not setting complexity requirements in the form of character classes, while the old BSI recommendation suggested using a "sufficient" complexity. Fifty-seven (89%) participants mentioned complexity requirements, most often with the necessity to include three character classes in the password, so the vast majority of the companies were more in line with the old BSI recommendations than with NIST. In the newer BSI [48] recommendation, the explicitly mentioned need to establish mandatory rules of the requirement of some complexity was removed,[2] and only included that a password needs to have some level of "quality". We thus believe that our dataset can serve as a baseline for future studies observing the development of policies in companies.

Independent of what a policy requires, Tan et al. [166] found that users tend to include more character classes in their passwords.

**Length and Complexity** As mentioned before, the implementation notes of the BSI [45] give examples of how to combine length and complexity requirements. There are two we can use: First, a length requirement of 8 to 12 and 3 character classes. Twenty-seven (42%) participants match this. Second, a length requirement of 20 to 25 and 2 character classes. None of the reported policies is equal to that example.

[2] Although the newer BSI [48] recommendations do not mention the complexity requirement as a mandatory rule, rules making use of complexity and length are used in the examples of the implementation notes [45].

**Password Age** When the study was conducted, the BSI recommended regular password changes. Forty-five (70%) companies follow this recommendation and force users to change their passwords regularly. In contrast, NIST updated their recommendations in 2016, in line with results from research [179], and since advised against regular password change. Instead, a change should be forced whenever there is evidence of a compromise [82]. The new BSI recommendations align with this but still recommend regular password changes if the passwords cannot be checked against compromises [45].

Two (3%) participants explicitly mentioned foregoing password rotation.

Regular password changes cause users to develop mechanisms to make these changes less painful. These mechanisms, in turn, can lead to new rules added to the policies. One example is password histories, meaning users cannot reuse a certain number of their passwords. While most companies mentioned that the passwords as a whole are not allowed to be reused, three (4.69%) participants mentioned that significant changes are necessary. We did not ask for details of the technical implementation. The naive solution for this would be to store all passwords in plain text. This is obviously not a good idea, and systems that can mitigate this issue have been proposed [23].

Another example of added rules due to a regular password change is minimal ages for passwords, where users are not allowed to change their passwords within a specific period to prevent them from cycling through and returning to their old password right away. However, this rule has the negative side-effect that users cannot change their passwords even if they assume it was compromised. Most likely, administrators could still make changes to the users' passwords instead of the users themselves, but it adds an additional step to the process. Minimal ages were mentioned by 15 (23%) participants.

Since regular password changes can cause several follow-up problems, it seems good that NIST and BSI no longer recommend this, and it will be interesting to see how and when companies adopt this change.

### Recommendations from Related Work

As summarized in Chapter 2, Shay et al. [157] tested 15 PCPs with over 20,000 participants. Tan et al. [166] tested 21 policies with over 6000 participants. Both research projects examined the strength of the policies by measuring password guessability and usability by looking at user sentiment, dropout rates, creation, and recall. Based on their findings, they gave recommendations for service providers, which we will have a detailed look at in the following. It has to be noted that their recommendations are based on only two studies, and thus, further research is needed to explore the discovered aspects further. Additionally, not all elements that we discovered in the policies were studied or mentioned in the recommendations.

**Avoid Using Length-Only Requirements** Some of the tested policies by Shay et al. [157] only included length requirements. These policies seemed usable, and while some of the resulting passwords were quite strong, many others were very weak. Therefore, the authors suggest introducing further requirements, even if the minimal length is high. When

looking at the three elements “minimal length”, “complexity” and “maximum age”, we only found two participants who only made statements about the length. One requested a minimal length of 6 characters but demanded the password not to include parts of the username or character/number sequences. The other company uses a minimal length of 12 characters and forbids easy-to-guess passwords. It has to be researched what effect these additional elements have on the resulting passwords.

**Do Not Concentrate on Character Classes** Tan et al. [166] included three policies containing only length and complexity requirements. They found that the resulting passwords could be cracked with equal success rates, independent of the number of character classes required in the password. The authors conclude that users, at least when seeing a password meter, tend to choose longer and more complex passwords than required. When using a large blocklist, additional character class requirements do not seem to have any positive effect. The authors also found that with a minimum-strength requirement, it is more usable to increase the length requirement or minimum-strength threshold compared to requiring more character classes to defend against offline attacks. In our sample, 61 of the 64 companies that also use a centrally managed user account and reported a policy mentioned using a character class requirement. Twenty-eight (46%) of them additionally mentioned the use of blocklists.

**If You Are Using Comp8, Replace It.** The PCP “comp8” included at least 8 characters, a complexity of 4, and no dictionary words. When testing this very common policy against others, Shay et al. [157] found three other PCPs to be more usable and more secure at the same time: “2class12” (minimal length of 12 characters, complexity 2), “3class12” (minimal length of 12 characters, complexity 3), and “2word16” (minimal length of 16 characters, at least 2 words). Looking at our sample, we find 10 (16%) participants who mentioned policies that match the “comp8” policy. Contrary, only four (6%) participants make use of “3class12” and no policy matches “2class12” or “2word16”. It is interesting to see that while research offers good alternatives, many companies do not seem to adopt them.

**Blocklists** Some policies tested by Shay et al. [157] prohibited passwords from containing substrings from a pre-specified list. They noted that this seemed to make creating a new password more difficult. However, this did not apply to the recall of passwords. Thus, they argue that including substring blocklists in the PCP is suitable if passwords do not expire too often. Tan et al. [166] found differences between different wordlists and matching algorithms (e.g. case-insensitive). They recommend not combining blocklist and character class requirements, especially when any password is rejected that exactly matches one included in a public leak.

Of the participating companies, 32 (50%) either confirmed whether they check the user-chosen passwords against commonly used passwords or mentioned prohibiting users from using certain sequences in their passwords as, for example, the company name, character/numerical sequences, or dictionary words. Twenty-five (78%) of them additionally re-

quire regular password changes, which Shay et al. consider as an unfavorable combination [157].

Twenty-eight (46%) companies used a blocklist in combination with complexity requirement, which is not recommended by Tan et al. [166]. We do not have further insight into (a) what lists were used nor (b) how the comparison takes place (are numbers and digits included in a full string comparison / is the comparison case-insensitive?). Since different implementations seem to affect the security of the resulting passwords, but also the time needed to create passwords, as found by Tan et al. [166], we believe future work should look at the actual implementation of blocklists within companies.

**Minimum-Strength Requirements** According to Tan et al. [166], minimum-strength requirements (i.e., number of guesses needed) are beneficial for password creation and, at the same time, result in strong and easy-to-remember passwords overall. When needing protection against offline attacks, the authors recommend the"1c12+NN10"-policy. In comparison to blocklist requirements, minimum-strength policies seem to combine better protection with improved usability.
None of our participants explicitly mentioned checking the passwords against a guessing attack. 5 participants required not to use "easy to guess" passwords. However, they did not specify if and how this is checked. It could thus be that the user is not supported in fulfilling this rule. It remains to be seen if and how this relatively new knowledge about minimum-strength requirements will be applied in PCPs within the following years.

Ur et al. [170] recommended supporting users in developing good approaches for creating passwords and teaching them to correctly judge their decisions regarding password strength instead of creating PCPs that focus on character-class structures. Two of the participants explicitly mentioned awareness training for their employees regarding passwords. We did not ask about this explicitly, so there are probably more participants who, in fact, use awareness training.
Inglesant et al. [90] studied the effect of the PCP of two different companies, from which one had a very complex policy. It required their employees to use passwords consisting of 7 to 8 characters, a complexity of 3, no dictionary words, not exchanging *o* with *0* or *i* with *1*, an expiration of 120 days, and significant changes to the 12 previous passwords.

Many participants from this company expressed frustration and negative feelings toward password creation and recall. The authors note that the unusability arises from the combination of complexity, regular password changes, and the necessity to make significant changes to a previous password. Even though they conducted the study 10 years ago, we still saw many policies that have the potential to create user frustration as they consist of many elements that all have to be kept in mind when creating the password (see Section 4.3.3). We hope that the revised BSI recommendations help in creating more user-friendly password composition policies.

### 4.4.2 Factors

Before conducting the survey, we had two themes that we assumed would influence the PCPs in companies:(1) **company size**: Tiefenau et al. [167] showed a significant difference between small and large organizations regarding formal update processes. We thus hypothesized that this difference could also be seen in other areas. (2) **the consulted recommendations (e.g., BSI or NIST)**, as they differ in details (see Section 2.1.2).

#### Size of Company

Table A.1 in the Appendix shows that the amount of clients managed by the participant grows with the company size based on the number of employees. The amount of participants reporting a company-wide account does not increase with the number of employees. Although the percentages at the two poles are different, the small number of companies per bin does not allow us to draw conclusions. However, using a company-wide account does not seem extraordinary, even for small companies.

When separating the small and medium-sized companies ($C_{small}$, n=23) from the big companies ($C_{big}$, n=40) according to the definition from the EU [129], we do not see a big difference in the PCPs. They do not vary much in terms of the mean length ($C_{small}$ = 9.8 vs. $C_{big}$ = 8.95) or the mean maximum age ($C_{small}$ = 156.8 vs $C_{big}$ = 141). We also found no difference in the modes of the complexity when simplified to only the number of required character classes (1,2,3,4): $C_{small}$ = 3 vs. $C_{big}$ = 3.

#### Consulted Recommendations

As already touched in Section 4.3.3 and can be seen in detail in Figure 4.1, the participants reported using different sources as a basis for their policies. In 19 out of 29 cases, the participants listed more than one source of information besides "Own Knowledge," statements from the "Other" text field included. Two participants reported only one institution besides "Own Knowledge".

Slightly more than half of the participants who were part of the creation process of the PCP (16, 55%) used the BSI as a basis for the policy. Fourteen of those were recruited via the BSI newsletter so we might see a recruitment bias here.

When looking at the minimal length, we could not identify a big difference between those who use the BSI as an inspiration and were part of the creation process ($C_{BSI}$, n = 16) and those who do not ($C_{noBSI}$, n = 13): We found a mean minimal length of 10.5 characters for $C_{BSI}$ and of 9.7 characters for $C_{noBSI}$. Nevertheless, we saw deviating means for the maximum age of passwords (225.00 days for $C_{BSI}$, 135 days for $C_{noBSI}$). The BSI guidelines suggested a regular password change. The high number could be based on the will to mitigate this measure but does not explain why the mean number of days for $C_{noBSI}$ is so low.

Potentially, this points to the need to further separate the participants into groups classified by aspects like industrial sector or based on a risk evaluation.

#### Self-Made Policies

During analysis of the data, we found that a higher amount of policies that require a minimal length of 8 characters were mentioned by participants who were not part of the creation process (31% in selfmade vs. 69% in not-selfmade). Overall, the mean minimal length of the not-self-made PCPs is also slightly lower (10.1 characters vs. 8.5 characters). A possible explanation might be the time a policy was created and official recommendations during those times.

Most (24 of 29) of the participants who helped create the policy reported having based the policy on 'Own Knowledge.' Future research should investigate this further as it is open to discuss whether this is a situation of "writing your own crypt library" or not. It should be noted that the software used often provides options for policies, so this probably heavily influences the policies (e.g., through default values).

PCPs of participants who were part of the creation process contained more elements when compared to the PCPs of participants who stated that they were not involved. This mainly included forbidden password elements as not using the username or license plate numbers. This may be an artifact of the methodology (e.g., recall bias).

While it is tempting to see a causal relationship here, be aware that the hypotheses around the self-made aspect are built from the data, so this phenomenon should be investigated in a separate study.

### 4.4.3 Heterogeneity

One of the main observations we made is that there is large heterogeneity in the landscape of PCPs, which we reported in Section 4.3.3. All PCPs used for company-wide accounts arrange in the area of 6-15 characters minimum (with a clear peak at a minimal character length of 8, Figure 4.2), an expiration range from 30 to 365 days (with two peaks at 90 and 180 days, Figure 4.3) and a password history of 3 to 24 passwords (with a peak at a history of 10, Figure 4.4). Yet we only found two PCPs that were identical concerning *all* mentioned elements, such as password history and forbidden words. As this could be an artifact of our methodology, as discussed in Section 4.5, we focused on the most common combinations of the three elements "complexity requirement", "minimal length" and "password rotation" as well as the number of PCPs that mentioned this combination (see Table 4.2). As mentioned in Section 4.3.3, some participants specified which character classes need to be covered in case they had the complexity requirement "3 out of 4". We merged all of them for Table 4.2 and only looked for the number of required character classes. Using the three elements, we found 41 out of 540 (9 different minimal lengths * 10 different maximum ages * 6 different numbers of required character classes [1 to 4, not stated, unspecific]) possible combinations in the PWA policies.

| Complexity At least one char | Min. Length | Max. Age | Policies |
|---|---|---|---|
| 3 classes | 8 | 90 days | 7 |
| 4 classes | 8 | 90 days | 5 |
| 3 classes | 10 | 90 days | 4 |
| 4 classes | 8 | n.a. | 3 |
| 3 classes | 8 | 180 | 3 |
| 4 classes | 12 | n.a. | 2 |
| 4 classes | 10 | 90 | 2 |
| 3 classes | 8 | 60 | 2 |
| 3 classes | 8 | 365 | 2 |
| 3 classes | 8 | n.a. | 2 |
| 3 classes | 12 | 365 | 2 |
| | | Sum: | 34 of 64 |

**Table 4.2** – Most common PCP element combinations of complexity (at least one character of each class), minimal length and maximal age. n.a. = no answer given
**Policies** gives the number of policies that showed this element combination. Other combinations only occurred once in the data set.

## 4.5 Limitations

Apart from the methodological limitations as given in Section 3.6, our analysis also faces a limitation. Due to the heterogeneity of the PCPs, making direct comparisons is challenging. Many of our comparisons are conducted in broad groups, considering only a few individual elements and overlooking their combinations.

## 4.6 Future Work

As mentioned in Section 2.1.2, the BSI changed its recommendation after this survey was conducted. In future work, we will monitor how this guideline change affects the PCPs of companies.

Most of our findings indicate trends that need further research with other methodologies to validate them. We encountered several PCP elements that can not easily be enforced technically. Future work should examine whether custom enforcement mechanisms were implemented or whether the hope is that users follow the instructions even though they are not enforced. It is also open to how users perceive the difference. While most policies were found to be similar in the big picture, they differed in their details. While this may be for good reasons, it also shows how diverse the landscape is, and further research is needed to see whether this is needed or if the benefit of one usable policy is higher.

The surveyed participants were all employees of German companies. Further research has to be conducted to validate the findings across cultures and study the influence of different local recommendations.

We could show a difference in the PCPs reported by their creators compared to PCPs created by somebody other than the participant. Still to be researched is the process of

creating this policy, how big the personal factor is (and should be), and what role official recommendations play.

# Chapter 5

# Measuring the Adoption of Password Expiry Recommendations by the German Federal Office for Information Security within German Companies from 2020 to 2023

***Disclaimer:***
*The contents of this chapter were previously published as part of the paper "Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security" presented at the 19th Symposium On Usable Privacy and Security (SOUPS) in 2023 [72]. I worked on this with my co-authors Maximilian Häring, Matthew Smith, and Christian Tiefenau. This chapter uses text from the paper's introduction, results, and discussion section. The data was analyzed qualitatively by Maximilian and me, and Christian and I performed a quantitative analysis. Maximilian, Christan, Matthew, and I wrote the introduction iteratively. Christian and I wrote the first version of the result- and discussion section, and it was iteratively refined by Christian, Maximilian, Matthew and me.*

*As this work was conducted with my co-authors as a team, this chapter will use the academic "we" to mirror this fact.*

## 5.1 Motivation

Password composition policies (PCPs) aim to increase account security. Yet, research has shown that individuals often devise strategies to deal with PCPs to make them less unpleasant, resulting in insecure passwords [170, 84]. One specific element of PCPs that leads

to user frustration while not improving the strength of passwords much is password expiry, which forces users to choose a new password on a regular basis [158, 179, 84]. The removal of this requirement has been discussed by academic research for at least 13 years now [90], but has not been fully implemented by the industry [71, 149].

National institutions, such as the NIST in the United States of America or the BSI in Germany, are possible facilitators in transferring academic findings into industry practice. These institutions offer recommendations concerning authentication and password policies in particular. Regarding password expiry, NIST removed its suggestion to enforce a regular password change in 2016, and the German BSI followed in 2020.

To understand at what speed such a changed recommendation is implemented in the industry, and especially what problems hinder adoption, we conducted three surveys (2020, 2022, 2023) with German companies after the BSI changed its recommendations. This survey was based on prior work [71] (Chapter 4), where we surveyed German companies in 2019, just before the change mentioned above.

We surveyed the used authentication system, including detailed questions about the password policy, especially password expiry. We recruited our participants via the BSI newsletter, thus focusing on companies likely interested in IT security topics.

We found that the number of participants whose companies use a regular password expiry decreased statistically significantly from 2019 to 2023. But with 45%, the number of participants whose companies use it is still high. Several of those participants whose companies still use password expiry stated that it is used to increase security, because they do not have the capability to implement the suggested alternative mechanisms as recommended by the BSI, or because someone still requested the change. We discuss these reasons and their implications and offer recommendations for future work and national institutions.

Summarized, our key contributions are:

- We document the progression of authentication processes (PCPs and alternative mechanisms) in German companies over the course of 3.5 years.
- We present reasons why companies do not or cannot comply with the recommendations regarding password expiry and alternative checks for account compromise.
- We offer suggestions and recommendations for researchers and national institutions.

## 5.2 Research Questions

The following research questions and hypotheses guide our analysis:

- **RQ1**: How did the authentication system within companies change over the years?
- **RQ2**: How did the usage of a maximum age develop over time after the BSI changed its recommendations in 2020? For this, we had the following hypotheses:

- ***H1***. *The total number of companies using password expiry decreased from 2019 to 2023.*
  This hypothesis is built on the fact that the BSI dropped their recommendation for using a regular password expiry. Only in case alternative mechanisms, such as checking for parallel logins from different systems or locations, cannot be implemented should a regular forced change be considered. We performed one Fisher's exact test, including all participants who made a statement about their password expiry.
- ***H2***. *For companies that use password expiry: The time range after which a password must be changed increased between 2019 and 2023.*
  We assumed that not all companies could implement alternative checks to remove password expiry entirely. We hypothesized that even if a company cannot remove the password expiry requirement, it would adapt to the BSI recommendation to increase the time intervals between enforced changes. We performed one Wilcoxon rank-sum test and included all participants who used a password expiry and also mentioned a specific time range.
- ***H3-6***: *Company characteristics or the use of certain policy elements influence whether the companies use a password expiry in 2023.* Factors like time, money, or flexibility could influence adopting the changed recommendations in a company. We, therefore, performed four Fisher's exact tests based on different company characteristics like their size (H3) or whether it belongs to critical infrastructure[1] (H4). We also tested if the usage of checks for password compromises (H5) or if the last change of password policies was before or after 2020 (H6) influenced password expiry usage.

- **RQ3**: What reasons do participants have to still use password expiry?
- **RQ4**: How do companies check for compromised accounts, or what hinders them from implementing such checks?

## 5.3 Methodology

We designed and conducted the study as explained in Chapter 3. This section explains how we analyzed the collected data and gives an overview of the participants and the companies in which they work.

### 5.3.1 Data Analysis

Over the years, the questions in the survey slightly changed. However, all questions for which we compared the results between the years were identical.

[1] "Critical infrastructures are organizations or facilities with important significance for the state community, the failure or impairment of which would result in lasting supply bottlenecks, significant disruptions to public safety or other dramatic consequences." Translated from the Federal Office of Civil Protection and Disaster Assistance [127].

**Coding** One of the open-ended questions was identical in all years and asked for the password composition policy in use (Q6). Answers for these questions from PCP20 and PCP22 were coded by two authors using the codebook created for PCP19 (see Chapter 4). For this step, we included all the complete answers that we received and merged answers from both years, such that during the coding process, the year in which the answer was given was not known to the coders.

First, both authors coded 31 answers to check for a similar understanding of the code book and then coded an additional 31 responses to calculate the inter-coder agreement. After that, each coder then coded half of the answers.

To date, most research on password composition policies has focused on minimum length, password expiry, the number of required character classes (complexity), as well as blocklists (see Section 2.1.2). To gain a complete overview of these components in the PCPs described above, we decided to code the participants' answers that did not mention their minimum length, password expiry, complexity, or a blocklist as 'not mentioned.'

We had 29 codes and used Recal2 [64] to calculate the inter-coder reliability (IRC). For all codes, the reliability lies in the range of (0.47, 1) with a weighted mean of 0.98. Table A.5 in Appendix A.3 shows the codes, their occurrences, and the code-specific ICR.

Since we noticed that the answers given for Q6 were very straightforward and did not leave much room for interpretation, the other open-ended responses that we analyzed (Q6 of PCP23, Q8/Q12: Reason for using password expiry, and Q14: How do compromise checks happen or why are they not used of PCP23) were coded by one of the researchers. Two authors discussed all codebooks and answers that were ambiguous.

We proceeded the same way for answers given for the "other"-option in multiple-choice questions. All citations from these answers in this chapter are translated from German.

### 5.3.2 Participants

In PCP19, we not only recruited over the newsletter but also used additional channels to distribute the survey.

When comparing the different years, we included only those answers by participants recruited through the newsletter for internal validity. To keep the samples as similar as possible, we included only those companies using employee accounts in our analysis. After this filtering, the datasets consisted of 54 (PCP19), 52 (PCP20), 63 (PCP22), and 80 (PCP23) answers.

All numbers for this filtering process are given in Table 5.1.

Table 5.2 and Table 5.3 show the participants' demographics and their company characteristics. Because of the different filtering, we additionally present the number of participants from PCP19 again.

| | **PCP19** | **PCP20** | **PCP22** | **PCP23** |
|---|---|---|---|---|
| All Data | 172 | 72 | 96 | 122 |
| Only BSI | 91 | 72 | 96 | 122 |
| Only complete | 71 | 57 | 66 | 83 |
| Individual filter | 69 | 56 | 66 | 83 |
| Only accounts | **54** | **52** | **63** | **80** |

**Table 5.1** – Elimination process of data sets. **Only BSI** = Only answers that were gathered over the BSI newsletter. Only in PCP19 were participants recruited over other channels as well. **Complete** = The participant filled out the whole survey. **Individual filter** = Participants were filtered manually if the answers indicated they did not understand the questions and if the role indicated not being able to decide on the company's authentication protocols. **Only accounts** = Participants indicated whether the company makes use of a centrally managed account. We only kept those who did.

| | | PCP19 | PCP20 | PCP22 | PCP23 |
|---|---|---|---|---|---|
| | | $n = 54$ | $n = 52$ | $n = 63$ | $n = 80$ |
| **Size of Company (Q52)** | 1-9 | 7.4 | 7.7 | 7.9 | 5.0 |
| | 10-49 | 13.0 | 3.8 | 11.1 | 13.8 |
| | 50-249 | 16.7 | 23.1 | 15.9 | 20.0 |
| | 250-499 | 7.4 | 7.7 | 9.5 | 12.5 |
| | 500-999 | 9.3 | 9.6 | 11.1 | 16.2 |
| | $\geq 1000$ | 46.3 | 48.1 | 44.4 | 28.7 |
| | Unclear | 0.0 | 0.0 | 0.0 | 3.8 |
| **Employees working full-time on IT security topics (Q53)** | 0 | 14.8 | 5.8 | 17.5 | 17.5 |
| | 1 | 22.2 | 36.5 | 27.0 | 23.8 |
| | 2-5 | 25.9 | 34.6 | 31.7 | 31.2 |
| | 6-10 | 5.6 | 11.5 | 7.9 | 8.8 |
| | 11-20 | 11.1 | 5.8 | 0 | 7.5 |
| | $\geq 21$ | 13.0 | 5.8 | 11.1 | 7.5 |
| | Unclear | 7.4 | 0.0 | 4.8 | 3.8 |

**Table 5.2** – Demographics of companies that were asked in all four years. All numbers are percentages of that year. "Unclear": Participants did not disclose the information, or we could not infer it from their answers.

## 5.4 Results

In this section, we present the findings of our survey. The changes between the years of the used authentication systems within companies are presented in Section 5.4.1 (RQ1). The usages of password expiry (RQ2) are summarized in Section 5.4.2. In Section 5.4.3 (RQ3), we present the reasons participants gave for using a password expiry, and Section 5.4.4 (RQ4) summarizes how companies currently check whether accounts are compromised and what issues hinder them in implementing checks.

| | | PCP20 $n = 52$ | PCP22 $n = 63$ | PCP23 $n = 80$ |
|---|---|---|---|---|
| **Sector (Q47)** | Services | 40.4 | 39.7 | 41.2 |
| | Industry | 17.3 | 15.9 | 15.0 |
| | Medical | 7.7 | 7.9 | 5.0 |
| | Infrastructure | 9.6 | 4.8 | 7.5 |
| | Public service | 9.6 | 9.5 | 6.2 |
| | Education and research | 5.8 | 9.5 | 6.2 |
| | Sales | 3.8 | 1.6 | 3.8 |
| | Other | 0.0 | 7.9 | 5.1 |
| | n.d. | 5.8 | 3.2 | 10.0 |
| **Critical Infrastructure (Q48)** | Yes | 19.2 | 15.9 | 13.8 |
| | No | 80.8 | 74.6 | 81.2 |
| | n.d. | 0 | 9.5 | 5.0 |
| **Incidents at company within last 5 years (Q57, MC)** | Easy PW used for attack | 11.5 | 9.5 | 11.2 |
| | Several PWs were stolen from database | 1.9 | 1.6 | 0.0 |
| | None of the above | 63.5 | 84.1 | 65.0 |
| | Other | 11.5 | 0.0 | 8.8 |
| | n.d./Don't know | 15.4 | 4.8 | 15.0 |
| **Own role (Q55)** | IT | | | |
| | C-level & management | 50.0 | 39.7 | 50.0 |
| | ISO | 17.3 | 28.6 | 20.0 |
| | Admin/DevOps | 13.5 | 12.7 | 11.2 |
| | Support | 0 | 1.6 | 0 |
| | Management | 1.9 | 9.5 | 7.5 |
| | DPO | 1.9 | 0.0 | 2.5 |
| | Consultant | 0.0 | 0.0 | 1.2 |
| | n.d. | 17.3 | 7.9 | 7.5 |
| **Own experience (Q56)** | $<$ 1 year | 1.9 | 1.6 | 2.5 |
| | 1-3 years | 17.3 | 17.5 | 12.5 |
| | 4-9 years | 30.8 | 30.2 | 28.7 |
| | $\geq$10 years | 44.2 | 50.8 | 52.5 |
| | n.d. | 5.8 | 0 | 3.8 |

**Table 5.3** – Demographics of companies and participants from PCP20, PCP22, and PCP23. All numbers are percentages of that year. "n.d": Participants did not disclose their answers. The participants indicated their current job position. Since some of them indicated holding different roles in the company (e.g., CEO and admin), the numbers exceed 100%.

### 5.4.1 RQ1 - Evolution of Authentication Systems

This section considers the evolution of authentication methods and password composition policies between 2019 and 2023.

#### Possible Authentication Methods

Figure 5.1 shows the percentage of participants per year who stated that their company offers their employees to authenticate using passwords, biometric authentication, and hard-

ware tokens, independent of their usage as the primary or secondary factor. Using authentication methods apart from passwords has risen steadily over the last few years. In 2023, for the first time, two companies indicated that their company does not use passwords. All numbers can be found in Table A.4 in the Appendix.

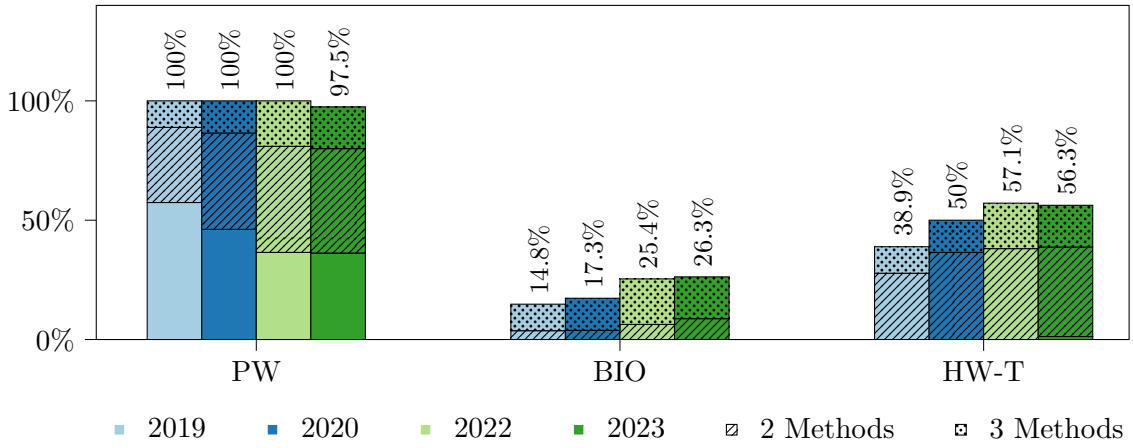


**Figure 5.1** – Percentage of participants who indicated that their company enables authentication using passwords (PW), biometric authentication (BIO), or hardware token (HW-T). Using authentication methods other than passwords rose steadily over the years. The bars also indicate the number of companies using one, two, or three authentication methods. Biometrics are seldom used as secondary factor alone.

If participants indicated that more than one authentication method can be used, they were asked whether these methods needed to be combined (two-factor authentication). Starting in PCP20, participants who mentioned only one method were additionally asked whether there is any possibility for two-factor authentication. The number of those requesting 2FA also increased, at least between 2019 and 2022: 22.2% of the companies that participated in 2019 required two-factor authentication – 32.7% did so in 2020, 55.6% in 2022, and 51.2% in 2023.

### Usage of Password Components

Participants were asked to indicate their current password policy (Q6). This question text included the example, "e.g., at least x characters, new password needs to be selected after x days," and participants were encouraged to provide a copy of their policy. In PCP23, we explicitly asked for password expiry in a separate question shown after a page break after Q6.

Figure 5.2 shows the development of the complexity, password expiry, and minimum length from PCP19 to PCP23. There is a slight increase in the number of participants who mentioned that their company requires all four character classes to be used in the passwords. While NIST advises against such complexity requirements, the BSI currently includes them in their implementation hints (see Section 2.1).

The figures also show a trend towards longer passwords and larger time ranges before the passwords expire, e.g., the number of companies that require a password change every 90

days decreased from 33.3% in 2019 to 6.2% in 2023, while those who explicitly mentioned not using password expiry rose from 1.9% in 2019 to 22.5% in 2023. In 2023, 10.0% of the participants did not include any information about password expiry in the open-ended response but disclosed they use a password expiry in the question explicitly asking for it (Q11). We further explore the details of password expiry in Section 5.4.2. The concrete numbers of companies using a certain minimal length, complexity, and password expiry are shown in Table A.5 in Appendix A.3.

We also looked at the most common combination of password expiry, a required minimum length, and complexity for each year and show the results in Table 5.4. The most common combination in PCP19 and PCP20 (minimum length of 8 characters, enforcing three character classes, and using a password expiry of 90 days) was not mentioned by any participant in PCP23.

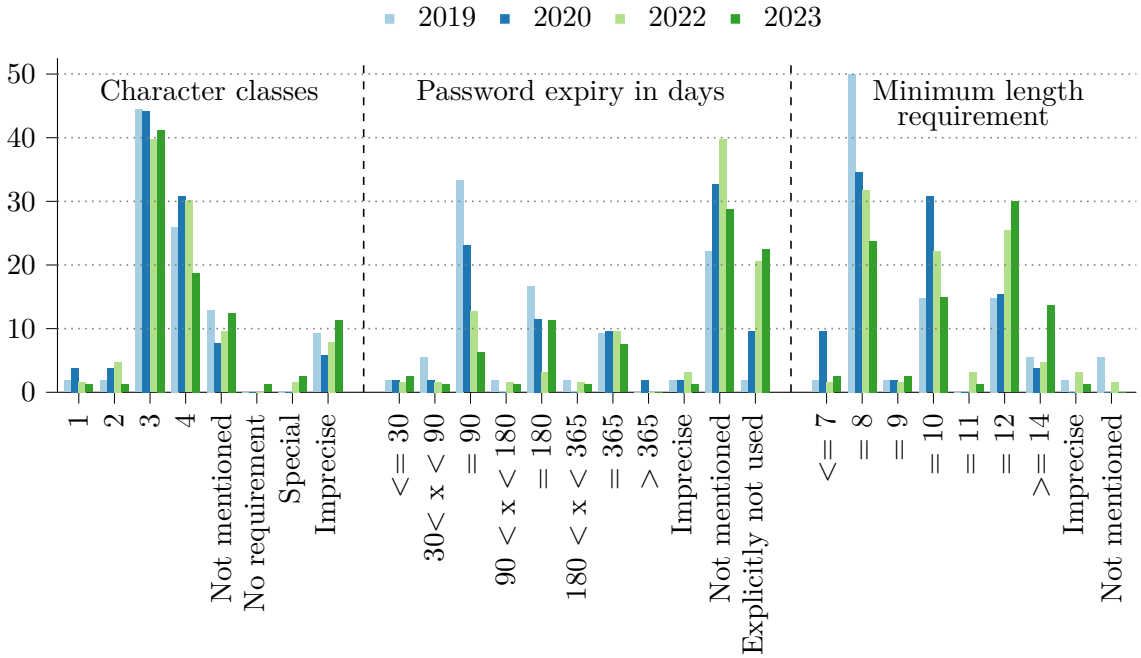


**Figure 5.2** – Overview of the required number of character classes that need to be covered in the user's passwords, number of days after which a user is requested to change their password (password expiry), and required minimum length in 2019, 2020, 2022, and 2023. Y-axis shows percentages. Answers from Q6. Findings: **1) Character classes:** Participants whose companies require at least three character classes either mentioned certain classes or allowed a password as long as any three classes were used. There are no big differences between the years. In their implementation hints, the BSI gives examples that include enforcing several character classes (see Section 2.1). **2) Password expiry:** The number of companies using password expiry of 90 or 180 days decreased from 2019 to 2023, and more participants explicitly mentioned not to use password expiry in 2022, following the BSI recommendations. **3) Minimum length:** Requiring passwords with at least 10, 12 or 14 characters is more common in 2023 than it was in 2019, where most PCPs asked for at least eight characters.

**Summary for RQ1** From 2019 to 2023, the companies our participants worked for offered more authentication methods next to passwords, and the number of participants whose companies require 2FA rose by almost 20 percentage points. Looking at PCPs, it is now more common than in 2019 to require longer passwords (12 or even 14 characters) and to refrain from using password expiry.

### 5.4.2 RQ2 - Password Expiry

As detailed in Section 2.1, the BSI advises against a mandated time-based change of passwords. Instead, companies should run analyses to determine whether a user account is compromised. This could, for example, be done by checking for parallel logins from several systems or locations. A regular change should only be considered if such checks are impossible.

While the development of the days after which a password change is required is given in the previous section, this section investigates H1 and H2, and we take a closer look at company characteristics that may indicate the use of password expiry (H3-6).

Since we wanted to dive deeper into the analysis of password expiration, we added an additional closed question about password expiry in PCP23 to double-check the open-ended general PCP question.[2] When comparing the numbers from the closed question to the open-ended answers, we noticed that ten percentage points fewer participants mentioned password expiry in the open-ended question than in the closed question (35% vs. 45%). It is interesting to note that 10% did not mention password expiry when describing their policy.

While we cannot say this for sure, we think it is likely that there has been a similar amount of underreporting in the previous years. However, to be on the safe side when comparing PCP23 to previous years, we use only the open-ended data, so the comparisons are made based on the same measurement instrument, i.e., we only use the 35% that were captured the same way as in PCP19.

However, we believe 45% to be more accurate and use it wherever applicable.

#### RQ2 - H1

We hypothesized that the *total number of companies using password expiry decreased from 2019 to 2023.* To investigate this question, we performed two Fisher's exact tests based on answers to Q6. The tests are based on slightly different assumptions. For the first one, we only included those participants who explicitly said something about their password expiry, either mentioning a time span or indicating they do not use one. In PCP23, 26.9% of those participants who did not mention a password expiry in the open-ended question (Q6) later stated one in the closed question specifically asking for it. The results show a statistically significant difference between the results from 2019 ($n_{exp19} = 39$, $n_{noexp19} = 1$) to 2023 ($n_{exp23} = 28$, $n_{noexp23} = 18$): $p_{(19,23)} = 0.00$, OR = 25.07.

[2] We added a page break to ensure participants were not influenced.

For the second test, we included all participants and assumed that not mentioning expiry is the same as not using one. In PCP23, this was true for 73.1% of those who did not mention password expiry in Q6. This test also shows a statistically significant difference between the results from 2019 ($n_{exp19} = 39$, $n_{noexp19} = 13$) to 2023 ($n_{exp23} = 28$, $n_{noexp23} = 44$): $p_{(19,23)} = 0.00$, OR = 4.71.

This suggests that within three years after the change, there has been a shift towards the new recommendations.

### RQ2 - H2

We further hypothesized that *for companies that use password expiry: The time range after which a password is required to be changed increased between 2019 and 2023.* For this analysis, we included only participants who used password expiry. We excluded all participants who gave no clear answer about the length of their password expiry (e.g., only stating that there is a password expiry but giving no numbers.) We performed a Wilcoxon rank-sum test for which we included 38 answers from 2019 and 27 from 2023. Figure 5.2 showed a trend towards fewer companies that enforce a password change after 90 or 180 days, and this theme was also picked up in the open-ended responses: "Jumping to unlimited passwords takes time because technical change and culture change take time. We went from 90 days to 1 year." Yet, the tests did not show a statistically significant result ($p_{(19,23)} = 0.131$, $Z_{(19,23)} = -1.511$).

### RQ2 - H3-6

Finally, we were interested in whether *company characteristics or the use of certain policy elements influence whether the companies use a password expiry in 2023.* We conducted four Fisher's exact tests to analyze the impact of the following variables on the existence of a password expiry: company size (<500, >=500), critical infrastructure (no, yes), last policy change (before BSI changes, after BSI changes), and technical measures that check for account compromise (no, yes). We used data from the open-ended response (Q6) and the explicit question asking for password expiry (Q11) for these tests. Taken together, 45% of the participants mentioned that their company uses a password expiry in 2023.

After correcting the results using a Bonferroni-Holm correction, none of the tested factors remained to have a statistically significant impact on the existence of password expiry. The contingency table for all tests is given in Table A.3 in the Appendix.

> **Summary for RQ2** Over 40% of the participants stated that their company still uses password expiry in 2023, although this is statistically significantly less than in 2019. None of the company characteristics for which we tested differences in the use of password expiry showed a statistically significant result.

| Expiry (days) | Min. Len | Complexity | 2019 | 2020 | 2022 | 2023 |
|---|---|---|---|---|---|---|
| 90 | 8 | 3 | 5 | 4 | 3 | 0 |
| 90 | 8 | 4 | 4 | 3 | 1 | 0 |
| 90 | 10 | 3 | 3 | 1 | 1 | 0 |
| 180 | 8 | 3 | 3 | 0 | 0 | 2 |
| 180 | 8 | 4 | 1 | 3 | 0 | 1 |
| Not mentioned | 8 | 3 | 2 | 1 | 4 | 2 |
| Not mentioned | 8 | 4 | 3 | 3 | 3 | 2 |
| Not mentioned | 12 | 3 | 0 | 3 | 1 | 5 |
| Not mentioned | 12 | 4 | 2 | 2 | 6 | 2 |
| Explicitly not | 12 | 3 | 0 | 0 | 1 | 4 |

**Table 5.4** – Number of times a certain policy was mentioned in 2019, 2020, 2022, and 2023. The more participants mentioned their company uses a policy, the darker the cell is shaded. A PCP is included in this table if it appeared at least 3 times in at least one year. While the most common policies in 2019 included a password expiry, this trend has shifted in 2023, where the most commonly mentioned policies do either not mention regular password rotation or explicitly state not to use one.

### 5.4.3 RQ3: Why Do Companies Require a Regular Password Change?

Thirty-six participants in PCP23 and nine in PCP22 answered why their company uses password expiry.

Apart from this explicit question, some participants included a reason for using password expiry in their open response to Q6.

In the following, we present the most commonly mentioned themes. The coding table is given in Table A.6 in the Appendix.

**Increase Security** In 2023, 17 participants said their company uses a password expiry for security reasons. Half of them stayed vague and stated "[password expiry] gives *some* security" or "improvement of password security." The remaining eight mentioned more specific reasons, e.g., "Because after a year, the risk of misuse of the PW through reuse with other, potentially corrupted services, is too great."

In 2022, two participants stated their company uses a password expiry to get rid of lost ($n = 1$) or leaked passwords where employees did not follow the recommended change after being notified about the leak ($n = 1$).

**Still Demanded** Another commonly mentioned reason was that someone or some regulation demands a password expiry. Four participants stated their CEO or internal policies require this regular change, "[...] contrary to the recommendation of the IT sec [department]" or because of "inertia in our security standards." Three participants mentioned that customers or the customers' compliance requires regular changes, and five participants mentioned official requirements, e.g., "Official (in my eyes outdated) requirements in handling officially classified data." The latter two reasons were also mentioned in previous years.

**No Alternatives** A small number of participants (Four in 2023, one in 2022) use password expiry because they have "No other method implemented yet" or because "there is currently no other technical solution." We look deeper into these alternatives in Section 5.4.4.

**Best Practice** Some participants (Two in 2023 and two in 2022) stated that password expiry is best practice or recommended by the BSI. One participant stated: "[We] consider it wrong not to change [the password] regularly." This was already a theme in 2022, so we asked in 2023 whether participants perceived a regular change as best practice before asking why password expiry was used. This question was affirmed by 23.1% of the PCP23 participants.

**Currently Changing** We also saw participants (One in 2023 and one in 2022) who stated they were currently in the process of eliminating password expiry. One mentioned: "The auditor still has to be convinced."

### 5.4.4 RQ4: How Do Companies Check for Compromised Accounts and What Hinders Them?

The BSI specifies that mechanisms must be implemented to detect compromised passwords (see Section 2.1). So, we were interested in the mechanisms companies use or whether they have problems implementing them. We included this question in the PCP23 survey, and 66 participants answered it. The coding table is shown in Table A.7 in Appendix A.3.

Of those 66 answers, 36 participants said their companies use technical solutions to check for password or account compromises, whereas 25 do not. In three cases, the participants gave no clear answer, and in two cases, checks were not used consistently for all systems (e.g., used for SSO but not for AD).

Those who use checks most often do so by checking against databases of leaked passwords ($n = 8$) or by using tools that check for anomalies within the system or during logins ($n = 16$).

The absence of technical checks was most often explained by missing resources (time, financial, or human resources) ($n = 7$), by structural and organizational issues ($n = 5$), or because the technical solution was not straightforward ($n = 9$). One participant mentioned a "conflict with the works council." Specific problems mentioned were that third-party tools are needed or behavior-based detection tests led to several false positives in the past.

Three participants questioned the possibility of checking for compromises in general: "It is not clear to us how to check if a [password] is 100% not compromised."

Additional ($n = 2$) or alternatively ($n = 4$) to technical checks, some participants stated their companies encourage their employees to check for a compromise themselves.

> **Summary for RQ3 and RQ4** Companies still use password expiry in 2023, mainly to increase IT security or because another entity requires it. Technical measures that check for account compromise were often not implemented because of missing resources.

## 5.5 Discussion

We conducted three surveys over three years to understand how password composition policies evolve. We found that companies now require passwords to have more characters than in 2019 and found significantly fewer participants whose companies rely on password expiry. When specifically asking for the reason for still using expiry in PCP23, we found IT security to be one of the leading explanations.

This section discusses the reasons why companies still use password expiry, draws connections to related work, and gives recommendations for future work and policymakers.

### 5.5.1 Password Expiry and IT Security

The BSI started advising against password expiry at the beginning of 2020. With this, they finally followed scientific work a full decade after it showed the usability of password expiry to be a problem [158, 90, 26]. In our study, four participants explicitly mentioned that employees wrote passwords down when they had to change them regularly, and the company thus got rid of this requirement.

Nonetheless, in the latest survey run in 2023, still, 45% of the participants stated that their company forces regular password changes from their employees. Several of them (17) argued for an improvement in IT security, confirming the findings of Sahin et al. [149]. In the following, we discuss these reasons and evaluate whether this situation is problematic.

**Compensation of Technical Issues** We found cases where password expiry was used to compensate for other technical issues. One participant mentioned using expiry to get rid of old hashing algorithms, one referred to a maximum password length of eight that was set by the system, and a third explained that MFA was not yet implemented for all accounts. It can make sense to keep password expiry to bridge the time until new technologies are implemented (as mentioned in the latter example). However, accepting all the drawbacks that regular password changes bring because of a legacy system that itself can be a security risk seems like a missed opportunity: Instead of adapting to the constraints of a system, system administrators could argue that they need a new and more secure system that can fulfill the updated recommendations. However, we must acknowledge that business constraints can make this difficult.

**Initiate Password Development** The most commonly used arguments for password expiry concerned initiating the development of passwords, i.e., making sure that a password is not in use anymore when an attacker gets access to it and reducing the problems that come with password reuse by, e.g., decoupling the employee account from private accounts for which the employee used the same password.

Both of those arguments sound reasonable in theory, especially as credential stuffing attacks (where an attacker tries to log into accounts by using passwords associated with that user in

leaks) made up almost a third of all attacks across the Arkose Labs network [101] and more than 12 billion leaked login combinations are public by the time of writing in 2023 [144].

However, estimating the real security benefit of such changes is hard. Studies indicated that many individuals simply modify a previous password when being forced to change it [84, 179]. This makes it easy for an attacker to guess the new password if they have access to a previous one, especially when considering advanced attacks where not only the password that is included in leaks is used but also variations of it (e.g., following the approach by Pal et al. [134]). Yet, simple attacks that use exactly the same password as found in leaks might be prevented.

Further, many attacks, e.g., data theft, do not require much time, and according to a study by Agari, 50% of the credentials were used within twelve hours after they were compromised [6]; thus, requiring password changes every month will likely not prevent many attacks.

If persistence is the goal, attackers will attempt to create further footholds so that losing access to the first account does not lock them out.

And while the results from a survey study by Habib et al. [84] indicate that users do not seem to choose weaker passwords when updating them compared to creating new ones, Adams and Sasse [5] argue that a regular password change could lead users to create very simple passwords. On a larger scale, it is unclear whether users' strategies for initially creating the password differ, depending on whether they know they will have to change it soon or can keep it for longer.

What is clear is that physical password handling differs depending on whether passwords need to be changed frequently or not: Habib et al. [84] saw a statistically significant increase in storing the main workplace password in the web browser when password expiry was in use. Depending on the details (usage of a browser password manager, behavior concerning device locking when leaving the desks, etc.), this might have a positive or negative impact on security. Similarly, if users are more likely to write down their passwords on sticky notes, physical access to a workspace would be a problem. Yet, unobserved access to a workspace might come with several other risks anyway, such as being able to insert a physical key logger (even though this involves more planning than simply using the password from a sticky note).

**Adding "Some" Security** The uncertainty of how much security is actually added was also present in the answers, where participants associated password expiry with "*some* security". While it can be reasonable to use every opportunity, even the small ones, to increase IT security, people nowadays already have to deal with many security mechanisms in their work environment (e.g., authentication, secure messaging, physical access control). Removing those requirements that are very time-consuming [26], and can even be replaced by technical checks thus seems like a good idea.

### 5.5.2 Further Reasons for Delayed PCP Updates

In this section, we discuss arguments for using password expiry apart from increasing IT security.

**Alternative Mechanisms Cannot be Implemented** One participant in 2022 mentioned that their company cannot remove the requirement for a regular change because of "inadequate control mechanisms to detect compromise." In 2023, participants mentioned technical reasons, e.g., that third-party tools are needed, current tools lead to too many false positives, or that, in general, the implementation of such checks is "too complex."

This problem can also be seen in other security-related areas, such as deploying updates, where systems are not updated because of legacy software that is known to be incompatible with up-to-date environments [167, 105].

The area of these alternative mechanisms remains to be studied in more detail. Further reasons for some companies being unable to use checks that indicate a password compromise need to be identified. One paper that has already studied these alternative mechanisms was published by Markert et al. [115]. The authors studied administrators' understanding of risk-based authentication. They found that the participants struggled with the meaning of the given risk levels and the configuration interface in general.

Depending on further findings, it might be helpful if the BSI, or any institution with a similar influence, could publish additional information about the available alternatives and how they can be implemented. At the point of writing, the suggestions concerning alternative mechanisms in the current implementation hints are very vague: "For example, logging and the corresponding evaluation of log files can be used to determine whether there have been unusual accesses or hacking attempts. Special security products are also available for databases, operating systems, web servers, and other applications."[3]

Looking at the area of HTTPS, the increase in its usage was not only sparked by a changed recommendation but also because there was a new and very easy way to follow it (see 2.1.3).

**Inertia** Participants pointed to the necessity of following requirements that still demand regular change, e.g., federal offices or the PCI (Payment Card Industry Data Security Standard). In some cases, internal security standards require the use. As pointed out in Section 2.1.3 and also mentioned by the participants, changes take time to reach every stakeholder, and one participant mentioned the word *inertia*.

The problem of contradictory guidelines can appear whenever multiple institutions publish different recommendations for the same topic. In these cases, administrators must decide which guidelines to follow or how to combine them.

**No Knowledge About Change and Misconceptions** Many technical news portals, e.g., [153, 140] and newspapers, e.g., [94, 44] reported the removal of password expiry in

[3]Translated from the German implementation hints [45]

the new BSI recommendations. However, we still encountered one participant who stated that this is recommended by the BSI. In 2020, 25% of the participants mentioned being unaware of the BSI changes published eight months earlier while being subscribers to the newsletter. This phenomenon can also be seen in other areas (see section 2.1.3).

We noticed misconceptions about how checks for account compromise happen and potentially problematic views toward security in general. One participant e.g. stated that passwords must be shared with third-party tools for compromise checks. Although this might be true for some checks, some solutions circumvent this problem [143].

Another participant mentioned that it is never 100% sure whether a password is compromised. While this is true for almost any other security-related topic, it should not lead to not using compromise checks at all.

Here, efforts such as the Let's Hash website of Geierhaas et al. [69] can help by providing participants with a programming aid that supports developers in securely implementing password storage. It seems beneficial to go further along this route and offer code-fulfilling recommendations from the BSI, NIST, or OWASP. While such a website is a good starting point, the people implementing the recommendations still need to be made aware of such platforms and that their knowledge is not up to date.

**Processes Need to Be Observed** Depending on the size and structure of a company, changing the PCP can require potentially complex processes and involve multiple parties. In our sample, we found cases where the CEO was involved in creating the PCP. While we do not know the whole picture, we sometimes assume a clash of very different goals. A CEO of a small company stated: "From our point of view, the management is responsible for the guidelines and not the IT admins." In another case, the CEO of a company required password expiry, even though the security department advised against this. In cases like this, non-technical explanations of why something should or should not be used from the IT perspective might help to convince decision-makers without deep technical background and help to mediate between different stakeholders.

Apart from this decision process, a new policy has to be included in the systems. Several participants indicated they use Microsoft's Active Directory for authentication. It would be interesting to ascertain whether and how the usage of central software positively affects processes in general. This way, and in combination with secure defaults, the processes might be improved in simplicity, speed, and security, as has already been seen in other areas [168, 159].

**Arguments for Change and Prioritization** One of the most commonly mentioned reasons why checks for password compromise are not implemented is missing resources, i.e., time, money, or human resources.

If decisions need to be made for prioritizing tasks, low-priority tasks are often postponed, and other stakeholders must be convinced that allocating time for this is a good idea. For this reason, the arguments for a change that impacts usability more than security need to be good. Official recommendations could explain their rationale behind decisions, perhaps

even beyond the security topic. That way, decision-makers have a better overview, and it might be easier to understand and communicate possible implications.

### 5.5.3 Sample and Recruitment Bias

We recruited over the newsletter sent by the BSI, thus focusing on companies interested in security-related topics, either out of an employee's personal interest or because their company has to follow specific guidelines. The latter might be the case for the 13.8% in our sample (PCP23) that indicated their company can be seen as critical infrastructure and for those 27.5% who indicated their company is certified with a certification relevant for IT security (6.2% indicated both). Yet, the effect of such a security focus is unclear and could lead to two very distinct outcomes: either following recommendations very closely or using every opportunity to increase security, even if the measures taken are questionable in terms of improving security.

# Chapter 6

# Testing the Account Recovery of Popular Websites When the Second Factor is Lost

***Disclaimer:***
*The contents of this chapter were previously published as part of the paper "Adventures in Recovery Land: Testing the Account Recovery of Popular Websites When the Second Factor is Lost," presented at the 19th Symposium On Usable Privacy and Security (SOUPS) in 2023 [70]. I worked on this together with my co-authors Maximilian Häring, Charlotte Theresa Mädler, Matthew Smith, and Christian Tiefenau. This chapter uses text from the papers' introduction, methodology, result, and discussion sections. The study was originally designed by Maximilian and me, and based on a small sample of websites, the study was modified by Charlotte and me, with Christian, Maximilian, and Matthew giving feedback on the study design. Charlotte collected data from the websites, and I supervised this collection. Charlotte and I conducted a qualitative data analysis, and Christian and I applied descriptive statistics. The introduction was written by Christian and me and iteratively revised by Maximilian, Christian, Matthew, and me. The methodology section was written by me and iteratively revised by Maximilian and Christian, and me. Maximilian, Christian, and I discussed the implications of this work. Both results and discussion were iteratively written by Maximilian, Christian, and me.*

*As this work was conducted with my co-authors as a team, this chapter will use the academic "we" to mirror this fact.*

## 6.1 Motivation

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* [82]. This is used in addition to the *primary authenticator*, typically something the user *knows*.

Using such a second factor is one of the most frequently given advice experts give non-tech-savvy users to stay safe online [93, 18], and indeed, the use of 2FA rose steadily over the last years [25]. Some services even force users to secure their accounts with second factors [77] or are required by law to do so, e.g., banking websites in the EU [137].

To understand the consequences of this additional security mechanism from the users' perspective, several studies examined the usability of (possible) second factors (e.g., [116, 30, 3, 147, 148]), their initial setup (e.g., [35, 4, 148]) , or looked at the acceptability of 2FA (e.g., [177, 35, 148, 34]).

Within these studies, participants repeatedly expressed the fear of losing the second factor [35, 99, 138] 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 [12, 87, 107]. Considering that the personal smartphone is a convenient choice for 2FA [161], 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 [35]. 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 users 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.

## 6.2 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 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.

### 6.2.1 Service Selection

We used Tranco [141] to identify high-traffic websites and used the top 500 for our analysis. The list was generated on 2 August 2022 [169]. 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 B.1.1. An overview of this elimination process and the corresponding numbers is shown in Figure 6.1.

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 website. Similar to the findings of Gavazzi et al. [68], less than half of the websites offer 2FA. Finally, we ended up with 78 services for the reviews.

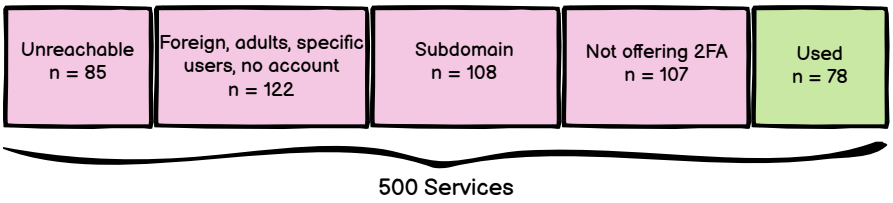


**Figure 6.1** – Overview of the service selection. We started with 500 high-traffic websites, according to Tranco [169]. Services were excluded based on criteria specified in Appendix B.1.1. Eighty-five were unreachable or marked insecure by Google Safe Browsing. This left us with 185 services, of which 78 offered to add a second factor.

### 6.2.2 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 [80]. 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 if 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

[1] Even though receiving codes through email is not considered as a second factor by NIST [125], it was listed as such on these websites. We opted to go with the definition of the services, as we believe some users will do so as well.

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.

### 6.2.3 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 6.2.2). 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.

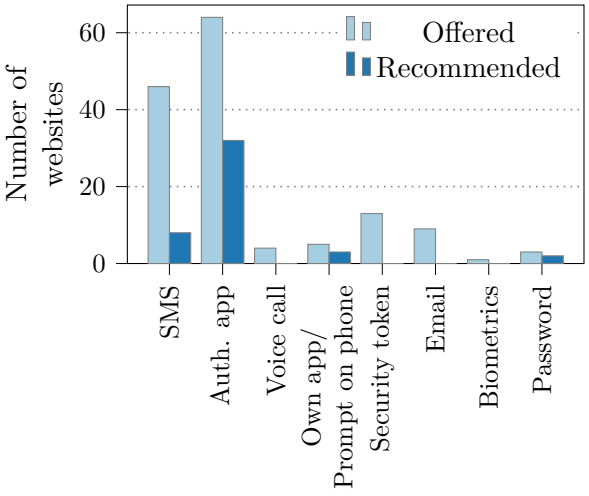


**Figure 6.2** – Overview of the allowed second factors on all sampled services. Most services allow users to use an authenticator app. Marked as "recommended" are those factors that were offered as the only possibility, were selected by default, or were marked as "recommended".

## 6.3 Results

This section presents the results of the usability evaluation of the 2FA setup and recovery process of 78 services. First, we give a general overview of the second factors that 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 6.3.3, 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 B.1 in the Appendix.

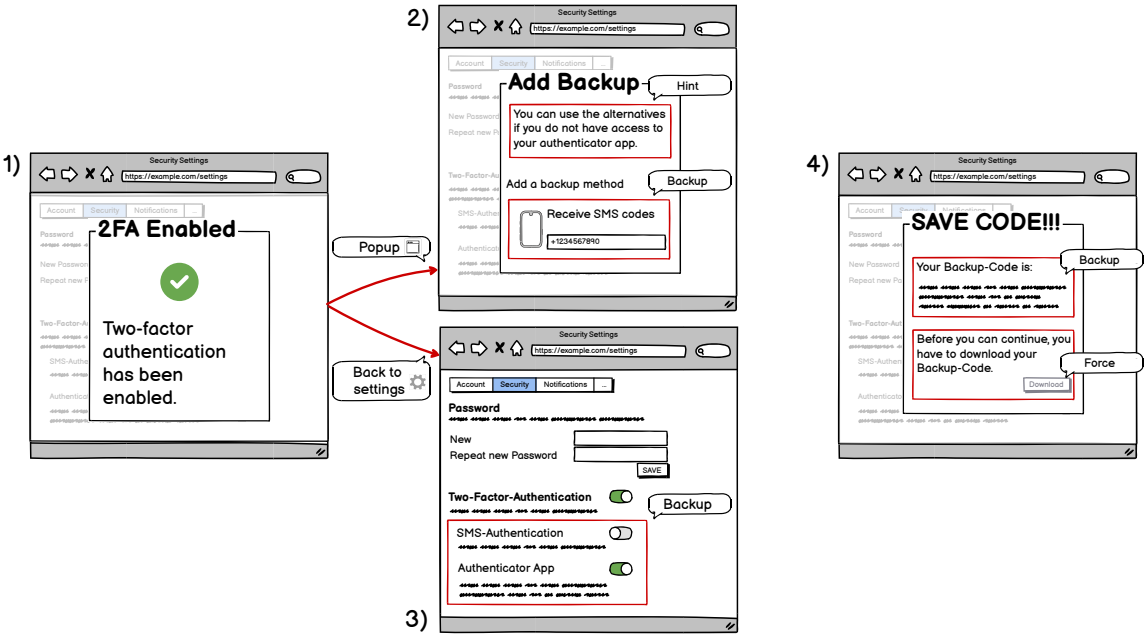


**Figure 6.3** – This figure shows four windows, with examples of information and cues we received during the setup reviews. A common workflow led us to one of two different states after enabling 2FA (1). In 52 cases (2), hints and backup possibilities were shown in the same popup that was used for setup. 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).

### 6.3.1 Allowed Second Factors

We were able to add a second factor to 78 services (see Figure 6.1). 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.

As shown in Figure 6.2, 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 ($n = 10$).

### 6.3.2 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 6.3 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 mandates users 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 6.3.3.

**Force** Mandating users to create a backup 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 6.4. 64.1% of the websites gave a hint and offered a backup possibility.

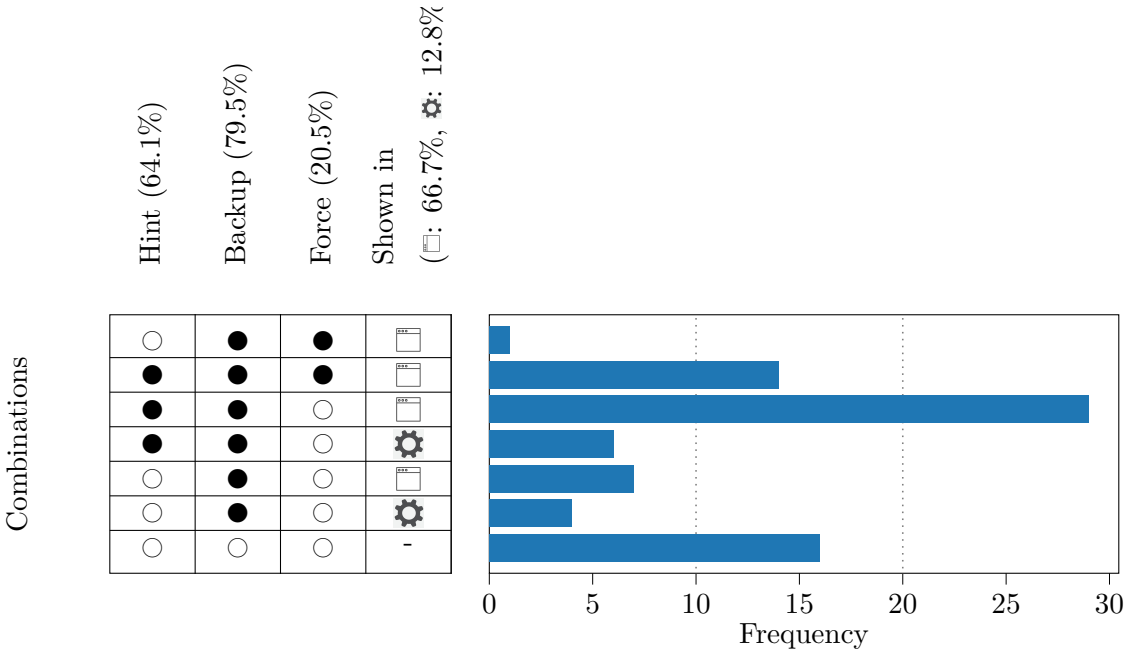


**Figure 6.4** – Number of websites that mention the possibility that the second factor is not accessible (Hint) in combination with showing alternative possibilities (Backup) or forcing the user to do something (Force) during 2FA setup. ○: The service does not include the characteristic. ●: The service 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 6.3.

### 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."

**Summary of the Setup Task (RQ1)**
To summarize, we successfully activated 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 a backup method, and 45 provided backup codes. The degree to which straightforward consequences of loss were communicated differed. Only ten services clearly indicated that a user would 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.

### 6.3.3 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.

#### 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 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 6.5. 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 6.1 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.

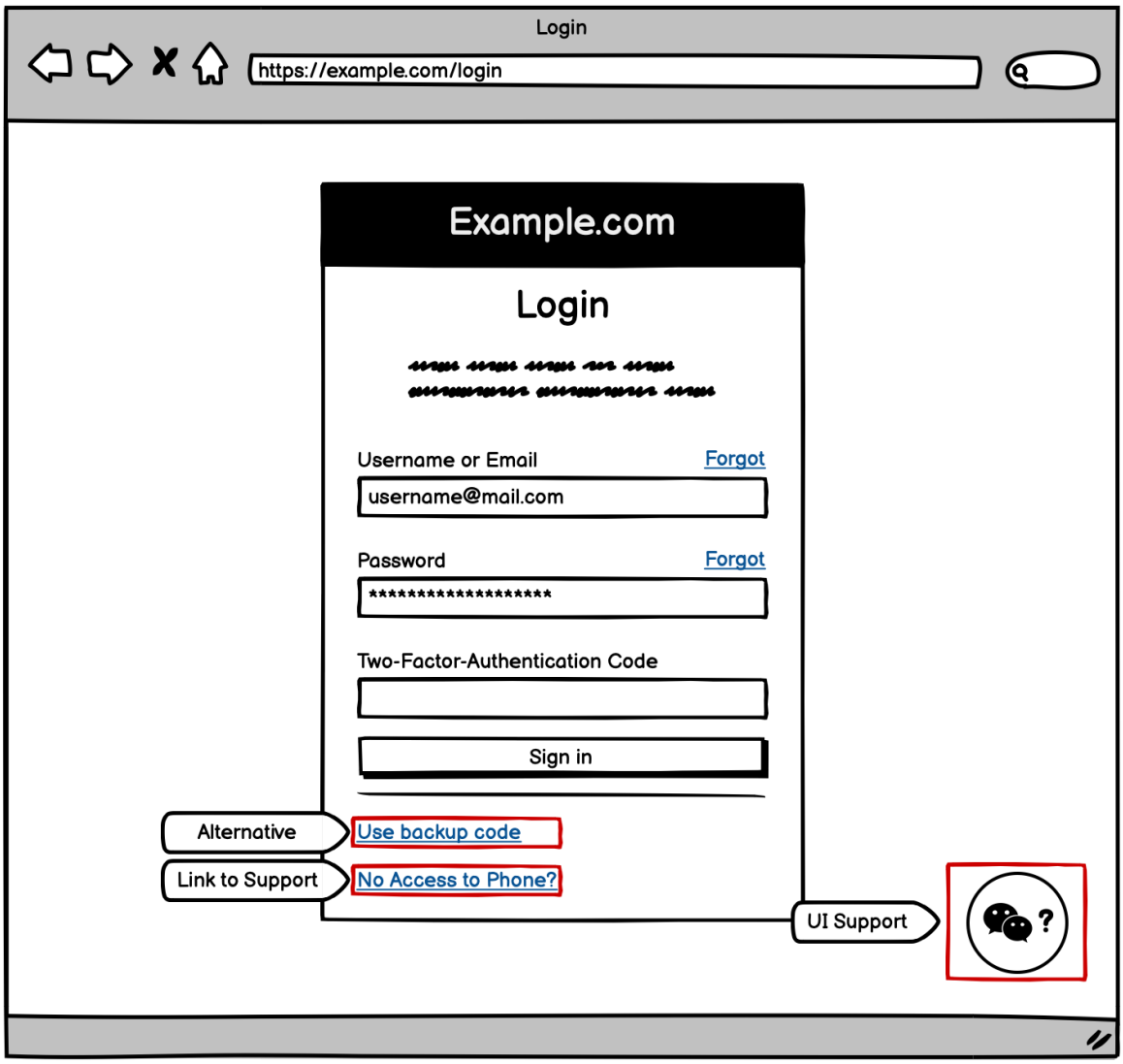


**Figure 6.5** – Example for the Login screen. If a link to the support existed, we noted whether it linked to a general FAQ, a specific FAQ (that at least partially mentioned what to do if losing the second factor), or whether a user is provided with an email address or can fill a form.

**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 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.

| 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 6.1** – 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.

**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, which we could not understand (without a translator). The rest of the site was available in other languages.

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

### Regaining Access

As shown in Figure 6.6, we were able to regain full access for 41 (52.6%) of the accounts. In nine additional cases, full access would have likely 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 6.3.2, 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 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 unsure 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").

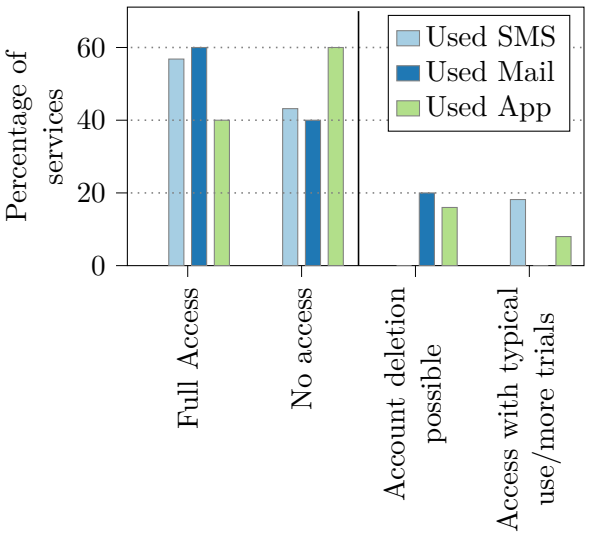


**Figure 6.6** – Overview of our results for the recovery process. It shows the percentages of services we either got full or no access to. Two accounts could be recovered using Authy. The right part shows the "no access" category in more detail. For some accounts, an account deletion was possible, on 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.

**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.

### 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

[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.

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 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 (e.g., by 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 could not regain access to the account. While most mentioned that they could not help us, four provided some 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.

**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 to use fallback authentication and a direct contact possibility. Between these two extremes, we saw a lot of different approaches varying in helpfulness. Regarding account recovery, we successfully regained access to 41 accounts. However, there were cases where no additional info other than knowing the email address was necessary to disable 2FA.

[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.

## 6.4 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 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 lacking in many basic aspects. We discuss themes we saw and make suggestions to practitioners and the research community.

### 6.4.1 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 [35, 99, 138], 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 case 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) [123], 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 lack of information is also documented by related work concerning account remediation [122, 113].

### 6.4.2 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, how a website communicates the consequences of loss, using unified terms, or what information a user needs to provide to recover the account. Currently, users cannot infer from their experiences from one website to another. With this, the fourth usability heuristic by Nielsen is violated (consistency and standards) [123].

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.

#### ... 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 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.

### 6.4.3 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 for these services is often handled by a bot (chat or phone), and direct human-to-human support is 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.

### 6.4.4 Summary: Recommendations for Websites

Summarizing Sections 6.4.1 to 6.4.3, we give the following recommendations to website providers:

1. Internal consistency and clear communication during login on what is possible and what is not. For example, 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. For example, 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.

### 6.4.5 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 without 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. [68] 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 cannot assess whether the account is 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 received 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 [66], 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. [40] 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.

### 6.4.6 Who Should be Responsible for Recovery?

We found many opportunities to make 2FA on services much more usable but noticed that this is 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., [114, 40]), 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. [78] 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 [75]. 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 [75, 74]. Since April 2023, Google Authenticator can be synchronized with the users' Google account [16].

**Third Parties / Delegated Account Recovery** Handling identities connected to user accounts can be challenging. We encountered three websites that outsourced this. One 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. Two other services directed us to Authy for the recovery process. In both cases, we used SMS as a second factor. While, from a usability perspective, this worked well for us, Gilsenan et al. [75] note that Authy solely relies on SMS OTP during recovery. The authors also found several security- and privacy issues [73].

### 6.4.7 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 identified 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 6.3.1), 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 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, banking details, or 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 6.3.3).
- Some websites periodically ask 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.

### 6.4.8 Future Work

We encountered services that only requested basic information to grant us access to the accounts. Similar to as it has been done with security questions [150], 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 quite a recent example of how these processes have become crucial, a challenge that future work needs to address.

# Chapter 7

# Investigating Users' Expectations Towards 2FA Recovery in Germany

***Disclaimer:***
*The contents of this chapter are currently under review. I worked on this together with my co-authors Maximilian Häring, Julia Angelika Grohs, Matthew Smith, and Christian Tiefenau. This chapter uses text from the paper's introduction, methodology, results, and discussion sections. The study was designed by Julia and me with feedback on the study design by Matthew and Christian. As it was part of her Master's thesis, Julia conducted the interviews, which were supervised by me. The data was analyzed by Julia and me and we discussed implications with Christian and Maximilian. The introduction was written by Christian and me and iteratively revised by the two of us, Maximilian, Julia, and Matthew. The first version of the methodology was written by Julia, and the section was revised by me. I wrote the first versions of the results and the discussion, and both were iteratively revised by Christian, Maximilian, Matthew, Julia, and me.*

*As this work was conducted with my co-authors as a team, this chapter will use the academic "we" to mirror this fact.*

## 7.1 Motivation

Creating an online account is usually simple, often requiring no more than an email address and a password. If a password is forgotten, account recovery is usually also simple, as a password reset email can be used. However, the security relies on the user choosing a secure password and protecting the email account as well. To improve security, users can add a second factor (2FA), like an app on a smartphone or a token. However, if the second factor becomes inaccessible, the recovery process is usually much more difficult or potentially impossible.

Two papers from 2023 investigated how services cope with the incident of a user who lost their second factor ([70] [Chapter 6] and [10]), finding that, while all investigated services offered a "forgot password"-button [70], help for an inaccessible second factor was less

prevalent. This means that users are responsible for having a backup plan if they want to avoid contacting the service and hope for a mitigation plan on their side. However, it remains mostly unclear how users deal with this situation and whether and how they actively try to prevent account lockout when using 2FA. If users do not actively implement a backup strategy for their second factors, there is the potential for a total loss of an account unless the service offers an alternative recovery mechanism. We thus formulated our first research question: **RQ1: What backup strategies - if any - do users have for their 2FA accounts?**

Previous studies have looked at the usability and users' preferences for backup methods but mostly studied the different methods in isolation, i.e., only looking at one method (per participant) in detail (e.g., [114, 150, 151]), comparing two methods (e.g., [162]), or evaluated the effectiveness of different challenges for real accounts [40]. These different approaches make it hard to compare the studies and backup methods to understand preferences in the current landscape. However, this knowledge would be useful in informing researchers and platforms which backup mechanisms are preferred and should be offered, leading to higher account accessibility. We were thus interested in thoughts toward existing and possible backup solutions: **RQ2: What 2FA backup mechanisms do participants favor over others, and why?**

Due to the diverse landscape of 2FA recovery suggestions and implementations of websites [70, 10], users may not be aware of necessary steps or even be overwhelmed in a recovery situation. As users currently cannot rely on something being implemented by all services, we were interested in their fundamental assumptions. **RQ3.1: What are people's expectations of websites regarding account recovery?** Prior work in the context of security tokens has shown a reluctance to accept tokens, as they shifted participants' perceptions of responsibility for authentication towards themselves [138]. We were interested in participants' current understanding of responsibility concerning 2FA (backups) and account access in general: **RQ3.2: Who should be responsible for account access (according to users)?**

To answer the research questions, we first conducted 16 interviews with German 2FA users. We found that only approximately half of the interview participants thought about the issue of losing their second factor or had experienced access problems. Only four had a backup plan they were aware of (e.g., knew where they stored backup codes), which most certainly works if their second factor was lost or broken. Based on the results of the interviews, we created a survey to gather more data. The survey was conducted with 95 German participants recruited via Clickworker [27]. Similarly to the interview, over half of the participants had not thought about what to do when their second factor is lost, and only 6.3% stated that they have a backup plan for all the accounts they protect with a second factor.

We found no clear answer on which backup method participants favor. Several participants focused on personal data, expecting that knowing certain things would be accepted as proof of identity. This often consisted of data that could also be gathered by attackers, making it an insecure wish. This was only recognized by a few participants. Connected to this assumption was the expectation that services offer support and users can reach out to them. We found a mix of feelings concerning responsibility: Even though several participants felt

it was more secure if they were responsible for their second factor and account recovery, many, at the same time, expected the website to help them as a last resort.

With this work, we contribute:

- An estimation of backup prevalence and account recovery probability among 16 interview- and 95 survey participants, which indicates a strong reliance on personal data and the websites' support.
- A set of expectations that users have towards services regarding account recovery.
- An overview of participants' understanding and feelings toward responsibility concerning account recovery.

## 7.2 Interview Study

To answer our research questions, both qualitatively and quantitatively, we followed a mixed-method approach consisting of interviews and a subsequent survey.

In this section, we present the interview study.

### 7.2.1 Methodology

We conducted 16 semi-structured interviews, as detailed in the following.

#### Recruitment

We recruited a convenience sample using three channels in May 2023: (1) by contacting all student councils of our university by email, asking them to forward it to their students, (2) by distributing flyers in supermarkets in our city, and (3) by placing an advertisement on Kleinanzeigen.[1] Through these channels, we recruited two, four, and nine participants, respectively, for the final sample. One additional participant heard about the study from a friend. In our invitation, we stated that the interview would concern 2FA but that no prior knowledge is needed. We stated it this way since the vast majority of Germans use 2FA, as it is required for online banking by EU law [137]. However, not everybody might realize that this is 2FA, and we did not want to lose these participants or anybody who is currently not using 2FA. Participants received a compensation of 10€. We reached saturation after 15 interviews.

#### Interview Structure

The interview was semi-structured and consisted of five different parts, briefly explained in the following. The guideline can be found in Appendix C.1. We expected the interview to take approximately 30 minutes.

[1] A German advertising website where users can sell items or look for jobs with some similarity to Craigslist in the US.

**Demographics and Explanation of 2FA** The study began with basic demographic questions and the participants' tech-savviness (hardware, software, and cyber security).

Next, we explained the basic idea of 2FA and how it works, typically in the context of online banking, to ensure basic knowledge.[2] We intentionally omitted the recovery process. Participants were then given the opportunity to ask general questions regarding 2FA to ensure their understanding.

**Experience with 2FA and Expectations** We then asked about participants' personal experiences with 2FA: if and where they use 2FA and what their second factors are. For inspiration, we mentioned PayPal or social media. We then asked how they would regain access to their accounts if they ever lost their second factor. If participants expressed that they had been in such a situation in the past, we asked if they regained access to the affected account, including required actions and time frames. For those without prior experience, we asked how they imagined a recovery process would look like, what they would try to do, including what they think is possible, and what they would be willing to do. For this last step, we gradually escalated the scenario to a worst case where an account stores no personal information and support is unreachable.[3] If participants mentioned receiving an email instead of, e.g., an SMS, we pointed to an attacker who had access to their email account and asked for their consideration on security. For actual circumstances (experiences and current backups), we kept asking until we felt participants shared everything they could recall or wanted to share.

**Videos** Following participants' theoretical considerations, we wanted to capture reactions to real recovery attempts and understand what users expect or wish for. For this, we showed two screen recordings of a recovery attempt that lacked user support. The first offered no help during login, while the second offered an "account recovery" button that, once clicked, resulted in an infinite loop by asking the user to log in first. We deliberately chose scenarios that did not give an easy solution (e.g., by receiving a code via email) to understand how users would cope with this and what they would try to do to solve their login issue. To mitigate ordering effects, we presented the videos in varying order.

After showing these videos, we asked the participants what they would do next.

**Backups** Next, we explored different existing and potential backup solutions (backup email address and phone number [from oneself or a trustee], backup codes, and an app that handles recovery with an identity document). We asked participants to choose their favorite method and discuss why they preferred it compared to the others.

**Responsibility** As a last part of the interview, we mentioned that it might be possible for a user to lose permanent access to their account if they lose the second factor. We asked

[2] One participant mentioned the use of 2FA in the work context prior to this explanation, so we used this as an example rather than mentioning online banking.

[3] We discuss the reasoning for this hypothetical question in Section 7.4.4.

the participants for their opinions on this and whether they felt responsible for their second factor and for setting up a backup.

### Analysis

One author used iterative open coding [32] to create a codebook based on the research questions, and another author coded all interviews based on this codebook. All data presented in this paper were discussed and agreed upon. All interviews were conducted in German. The authors translated all quotes used in this work.

### Participants

We conducted 18 interviews in person or via Zoom, each lasting 18 to 37 minutes. We excluded two participants: One because of technical problems and the other because they did not want to be recorded (both were compensated regardless). All remaining 16 interviews were recorded and transcribed.

With 75% of the participants being younger than 36 years and 56% describing themselves as being at least partially interested in technology, we have a rather young and tech-savvy sample. All participants owned and used a smartphone, and the majority also used a laptop. Table 7.1 depicts the participants' demographics in more detail. In the following, we give an overview of participants' usage of 2FA and their experiences with losing access to accounts.

**Usage of 2FA** All participants stated they use 2FA for online banking and at least one additional account, e.g., payment services, retail, email, or device accounts (see Table 7.1). Three participants mentioned they use 2FA almost anywhere they can or anywhere they get it suggested, any service they use often, or if a service handles finances and stores a lot of personal data.

In some cases, the behavior of websites as described by the participant does not necessarily indicate that the participant enabled 2FA, but could be explained by a verification of the home address or risk-based authentication (RBA) as well: "With PayPal [...], sometimes it comes, and then you have to confirm it again". While 2FA and RBA are based on slightly different technical ideas, they can be indistinguishable from a user perspective: In both cases, the password alone is not (always) enough to log in, but an additional confirmation via another way/factor is needed.[4] When talking about recovery, we explicitly mentioned that a user would normally need to receive a code via SMS, so when participants started to think about losing their phone, this happened under the assumption that they would need the phone to log in.

**Stories of Losing Passwords, a Second Factor, or Accounts** We asked participants how they would proceed if they could no longer use their second factor (e.g., by losing or breaking it.) Some participants then mentioned that they could tell from experience.

[4]Detail on this topic are given in Section 7.2.2.

Two of them did not experience 2FA loss directly but forgot the password for one of their accounts. Additionally, one had changed their phone number, and the other had lost their phone. Both could thus not validate a request sent to their device or via SMS. To regain access, one had to wait several weeks (Apple), and the other lost access permanently and had to create a new account (Snapchat).

Looking at the second factor, two participants broke their phone, and one changed their phone number, all resulting in access problems. All of them could access at least one account with another possibility (e.g., backup codes) or by contacting the support.

One of them was not able to recover all accounts, but lost access to two video gaming accounts, including several game licenses, characters, and items: "I can't find a way, so far, of getting there, somehow I keep going round in circles." (P5)

One participant did not experience loss but had a technical issue with their Yubikey. Only after they managed to remove the key from their account, [5] they noted that their computer did not use the correct time, which was needed by the Yubikey (and backup Yubikey).

Another participant never lost their second factor but expressed that they had thought about losing their phone often and were concerned about this: "I've often asked myself that. [...] I could no longer get into any of these [accounts], which I may not even remember. [...] So my phone is always in sight. [...] I mustn't lose it." (P13)

#### Ethics

Our study was reviewed and approved by our institution's Research Ethics Board and adhered to the German data protection laws and the GDPR in the EU. Participation was voluntary, and participants could drop out at any point during the study. Participants received a debriefing, emphasizing that a backup is potentially necessary if the account is very important and they do not want to risk losing access. Finally, we mentioned that the second factor and backup should be kept separated, e.g., not on the same device.

### 7.2.2 Results of Interviews

The following section presents the results according to the research questions.

#### RQ1: What Backup Strategies - If Any - Do Users Have for Their 2FA Accounts?

In the following, we present the participants' backup methods next to their primary second factor. For this, we summarize two things under the phrase "backup": A dedicated backup, such as backup codes, and methods that could count as an additional second factor (e.g., if one can choose between using the authenticator app or receiving SMS codes).

[5] The participant could not in detail state how they did this.

| ID | Age | Current Occupation | Highest Education | Tech-Savvy? | Devices (LAPTOP, SMRTPHONE, TABLET, PC) | Self-reported Services with 2FA | Second factor | Unav. Auth. |
|---|---|---|---|---|---|---|---|---|
| P1 | 26 | Student | BA | Yes (excl. security) | - (at least L,S,T) | Payment, Entertainment, ◇ | SMS, Mail | ○ |
| P2 | 34 | Student | VT | Yes (incl. security) | - | ◇ | Yubikey, SMS, Mail | ◑ 2* |
| P3 | 36 | Employed | Master | No | - (at least L,S) | Payment, Retail | SMS, PKQ | ○ |
| P4 | 28 | Student | BA | Yes (excl. security) | L,S,P | Entertainment, Email | Device, SMS | ◑ 2 |
| P5 | 50 | Employed | VT | Yes (incl. security) | L,S,T | Retail, email, gaming, work | Authenticator app | ● 2 |
| P6 | 20 | Apprentice | Abitur | No | L,S,T | Bureaucratic | - | ○ |
| P7 | 32 | Employed | MA | No | L,S | Payment | SMS | ○ |
| P8 | 25 | Employed | MA | Yes | L,S,T,P | Payment, reward system | SMS, App of service | ○ |
| P9 | 18 | Student | Abitur | Medium | L,S,P | Payment, email, social, communication | Authenticator app | ○ |
| P10 | 20 | Voluntary social year | Abitur | No | L,S,T | Work | SMS | ● 1 |
| P11 | 36 | Parental leave | VT | Medium | L,S | Payment | SMS | ○ |
| P12 | 32 | Student | Abitur | Yes (excl. security) | L,S,T | Payment, retail | SMS | ? |
| P13 | 46 | Employed | Graduate Degree | No | L,S | Payment, social, ◇ | SMS | ○ |
| P14 | 20 | Student | Abitur | Medium | L,S,T | Payment, retail, email | Device, App of service | ◑ 2 |
| P15 | 21 | Student | Abitur | No | L,S,T,P | Payment | App of aervice | ○ |
| P16 | 27 | Student | Abitur | No | L,S | Communication, Email | PIN, Device | ◑ 1 |

**Table 7.1** – Demographics of the 16 interview participants, including in what service category websites fall on which they use 2FA (following the categories used in the 2FA directory [2], if applicable.) All participants used online banking, which is not depicted in the table. For this, they all used the banks' apps.
**Education:** Abitur is the German secondary-school examination, VT = Vocational Training
**Services:** If ◇ is in the list of services: Participants expressed (sometimes additionally to specific services) that they use 2FA wherever possible/suggested by the website.
**Second factor:** If no second factor is given, the participant stayed too vague or could not remember.
**Unavailable Authenticator:** Has the participant ever (temporarily or permanently) lost access to their first ([1]) or second ([2]) authenticator? ○ = No, ◑ = Yes, and regained access to all accounts, ● = Yes, and lost access to at least one accounts. If marked with *: technical problem. P12 did not clearly indicate whether they have experience with losing one element of their authentication requirements

Only four participants mentioned explicit backup methods, which should also work if their primary second factor is temporarily or permanently not accessible. Participants mentioned the following approaches: a) Receiving an email instead of using their WhatsApp passcode [178], b) having backup codes stored in their password manager and using the cloud synchronization of authenticator apps, c) using redundant Yubikeys and an additional email address and phone number. One participant has to confirm logins in the service's app and uses this app on their phone and tablet.

One participant used an authenticator app and backup codes, but when asked if they could access them, they said:

> P9: "I'm just thinking about that. [...] Probably not. Yeah. I don't know. So it could be that I have them somewhere. I probably have them saved somewhere. I'll just have to go and find them first."

This participant later added that at least one of their accounts also stores their phone number as an additional backup.

All other participants (n=11) did not mention explicit backup strategies. Yet, nine of them seem to use 2FA solely for accounts that store personal information, such as their name, address, payment information, and prior transactions. Six of them assumed that they could regain access by providing such information or experienced this in the past (further information on this is given in Section 7.2.2). We believe this assumption is somewhat reasonable based on results from prior work [70, 10].

Eight participants used 2FA for at least one account by receiving a code via SMS. Even though only mentioned by two of them, these participants could regain access by ordering a new SIM card.

Overall, it seems likely that most or even all participants could regain access to their accounts, either by using their own backup, by ordering a new SIM card, or by providing personal information. The last option is only successful because websites currently *may* grant access when a user provides them with personal data.

#### RQ2: What 2FA Backup Mechanisms Do Participants Favor over Others, and Why?

We presented the participants with different backup methods. This included methods that are currently used in practice, such as backup codes, a backup phone number, or a backup email address. For the latter two, we mentioned they could also belong to a family member or friend to receive thoughts on account recovery with trustees. Additionally, we presented the idea of a delegated account recovery app combined with an identity document. While describing the last option, some participants were reminded of an app published by the German government that reads the identity document and can be used for several digital government services [131]. While this method is, as far as we know, not used in practice for account recovery, it should bring up the possibility of a third party handling account recovery and the idea of using personal information. We did not request statements on all

methods but asked participants to share their thoughts and select the method(s) that they would prefer. They could also mention additional methods.

Three methods were favored equally by five participants each: Backup codes, personal information (identity document), or a pre-registered delegated account recovery app. Even though we presented the latter two in combination, many participants rated them independently. Hardware keys and an alternative email address were preferred twice and trustees once.

In the following, we summarize positive and negative statements about the recovery methods:

*Backup codes* were perceived as more secure than SMS or emails, and it was positively emphasized that backup codes do not require the service to store additional information about the user. On the contrary, participants mentioned that backup codes do not scale well if used for several accounts and that they are often stored on the device, which is also used as a second factor (e.g., as a screenshot). Two participants each found backup codes to be either easy or cumbersome to use. One participant said:

> P13: "Well, I see [backup codes] sometimes. But I think to myself, where else should I save this? [...] I have no relationship at all to this [code]. And when I saved it, I no longer know what it was for."

Recovery via an *identity document* was rated as "good", as everybody owns one anyway.[6] One participant mentioned that this approach might be insecure, as it would be easy to find accounts that belong to a person if that person ever lost their identity document. [7]

Regarding a *delegated account recovery app*, participants mentioned they liked the idea if the implementation was easy to use and secure. Another participant feared the approach would not be accessible to users without much technical knowledge. One said they would not want to download another app just for that purpose.

Except for one participant who would like to use the email address of their partner for account recovery, participants only commented negatively on *trustees*. They mentioned they were not sure what their trustees would do with this power of potentially being able to access the account and that their trustees might not react quickly enough if ever needed. Yet, we only presented a very simple implementation of trustees, where a trustee would be the owner of the backup email address or phone number.[8]

### RQ3: What Expectations Do People Have of Websites Regarding Account Recovery?

To investigate participants' expectations, we used two approaches. First, we asked the participants straightaway what they would do if they lost their second factor. Most often

[6] From the age of 16, German citizens are required to own either an identity card or a passport [130].

[7] It is hard to estimate how easy such an attack would be, e.g., depending on whether recovery requires access to an email account additional to the identification document or whether it is possible to pretend not to have access to anything else.

[8] Some services use a more complex approach of trustees for emergency access, e.g., LastPass [103].

(12 times), they mentioned contacting the support to, e.g., provide additional information and wait for further instructions from them. The five participants who mentioned they do have a backup for at least one account stated they would use the backup for login; three of them additionally mentioned customer support. While our scenario described receiving a code via SMS and several participants also used this approach for their accounts, only two said they would order a new SIM card with the same number. One participant joked their current solution is to not end up in such a situation in the first place.

To get more insights into the users' expectations, we also presented each participant with two recordings of websites not supporting the user in the recovery process and asked for approaches in these scenarios. Participants mentioned they would look for a way to contact the service, and some also mentioned specific approaches, e.g., checking the "about us" section, using Google, or searching within the website FAQs. Four also mentioned they would first click on given links to see whether this helps, e.g., "login via SSO", or "forgot password". Four participants mentioned at some point that they would be lost in such a situation and would not know what to do. Some of these participants also stated they would be frustrated and annoyed.

Several of these steps are connected to assumptions concerning services and their recovery process. We detail these assumptions in the following.

**Support Availability** Twelve participants mentioned they would try to contact the support after being asked what they would do in general. One did not explicitly mention they would contact the support, but their statements included some form of interaction with the service:

> P14: "I could just imagine that you have to send [...] your access data or something to [the service]"

After seeing the videos, eight participants stated they would look for possibilities to contact the service.

Both forms of statements seem to be based on the assumption or hope that there is a) a possibility to reach out to the service and b) that this support is interactive.

Yet, not all participants expected the support to exist or be helpful. Especially those who had already been in a situation where they had to contact the support due to access problems noted that this is often not as helpful as they wished for:

> P15: "I also have a bit of experience with the fact that if you then go to these support websites, you won't get anywhere either"

Five participants stated they would carefully read through the support pages or the FAQs, and one noted they would highly value a method that supports them in helping themselves.

**Personal Data and Information Will Do the Job** Most participants assumed that there was another way in which they could prove their identity. Several of these alternatives included personal information, such as their name, address, payment information, answers to security questions, or providing the service with their identity document. One person mentioned they would be able to prove they lost their phone by using Apple's "Find my"-service [11]. One had no idea how identification for account recovery should take place if not by comparing personal information.

This assumption was sometimes based on experiences from the past: Five people had already used personal information after they lost access to their accounts (password or second factor) or remembered answering security questions in the past (yet, often not for the accounts they secured with a second factor).

While talking about these alternatives, six participants mentioned that providing the service with their information could or should only work if the website already has this information:

> P6: "So probably also something like an ID document. There's always a number on the ID card. They could perhaps ask for it. Although, of course, they have to have it beforehand."

Two participants noticed during the interview that giving access to the account based on personal data could potentially be insecure:

> P4: "[...] I think [...] I had to [...] confirm that I know which email [address] is linked to my account [or] somehow give personal details [...]. But when I say it like that, I think to myself, it's kind of error-prone. [...] It's not that difficult to find out my address, [...] nor my email address. [...] I'm a bit worried now that I got back into my accounts so easily (laughs)"

**Responsibility for Account Access** We asked participants who they think is responsible for their second factor and whether they would be okay if a website does not let them back into their accounts if they lost access to their second factor and their backups.

Most often (7 times), participants described a **mix of feelings**, e.g., by stating that they feel responsible for making sure not to lose their phone but that they still expect the service to help them regain access if necessary:

> P4: "So I think, yes, I am primarily responsible for making sure that I look after my passwords, my accounts and that they are available. But I also think that the company whose service I use is responsible for ensuring that I can continue to use the service."

Five participants agreed they are fine to be **responsible alone**, or at least to a much greater extent than the website. One compared this to physical access to their belongings:

> P10: "When I lock my bike, I don't want the bike shop to have a second key for it once I've bought it."

One participant would be **fine with both situations** but emphasized that the communication from the website needs to be very clear if the user bears the responsibility.

Another participant wished websites would take care of possible login problems.

Two participants made contradictory statements in the course of the interview.

### Additional Findings

**Every Additional Step Considered 2FA** Even though we briefly explained what 2FA is at the beginning, several participants confused this with other mechanisms. Some described a behavior that could also be triggered by risk-based authentication:

> P12: "And with [Service], I often get a text message when my wife or my sister logs in to see if I haven't been hacked, but if it's someone I know."

Others mentioned validation emails or letters one receives when registering for a new service or bureaucratic services and thought this might be 2FA. Two participants asked whether CAPTCHAs can also be considered 2FA:

> P6: "Would it be something like these pictures where you have to click on: There and there are traffic lights on it. Would that also be something like that?"

It seems that in several cases, participants were not sure why they had to perform the actions they had to perform, and that kept them from logging in.

We discuss the implications of this in Section 7.4.3.

**Access by Strangers** When being asked what participants think would happen if they lost their second factor and could thus not receive the SMS with the code anymore, six participants answered concerning others accessing their account and only then (or sometimes after being hinted to it) noted that this would mean that they themselves could not gain access to their accounts anymore. This could indicate that the situation of others gaining access is seen as worse than personally losing access. In the interviews, we did not investigate this further but added a question about what situation is worse to the survey.

**Asking Service to Delete an Account** Participants mentioned that if they lost access to their accounts permanently because they could not prove they were the legitimate owner, they might ask the service to delete their account without noticing that this step in itself requires the service to check the requesters' identity.

> P8: "I don't know which company I'm so attached to that I would necessarily spend hours chatting with chatbots, and I somehow think that's not productive at all. [...] So, at some point, I would rather just have my account deleted by email."

## 7.3 Survey

To get further insights into our research questions on a larger sample, we created a survey based on the results that we got in the interviews.

### 7.3.1 Methodology

We surveyed 95 German participants, as detailed in the following. We chose this sample size to get an initial view of this topic. Additionally, we did not plan any hypothesis testing, so we had no basis for a power calculation to specify a concrete sample size.

#### Recruitment

We recruited participants on Clickworker [27] in July and August 2023 in two batches. During the survey, we already excluded two participants who reported they did not use 2FA for at least one account.[9] We aimed for 100 responses but received 105 answers (5 participants answered all questions but did not proceed to the last "thank you"-page). To ensure the quality of our data, we included an attention check question and excluded all participants who did not answer it correctly (n = 10, these participants were not compensated), so we ended up with 95 participants. The survey was calculated to take ten minutes, and every participant got paid 2€, which equates to the minimum wage in Germany at that time. Due to the small sample size, the study is not representative of the German population.

#### Survey Content

The survey is divided into four different thematic parts: demographics and those described in the following. All answers without a natural order were presented randomized. The full survey text can be found in Appendix C.2.

**Details about 2FA Usage** Participants were asked for the specific area where they use 2FA (e.g., online shopping or social media) and were presented with example websites. Furthermore, we asked for the second factors that are in use and whether the participant had ever thought about or experienced losing the second factor. The interviews' results informed questions and answer possibilities.

**Knowledge about 2FA** In this part of the survey, we gave 16 statements that should be rated by the participants using a 5-point scale that ranged from "I agree" to "I disagree." Six statements concerned the actual recovery process and what the participant assumes or believes in this situation, e.g., "I am sure that the website will give me a way to regain access to my account." The other ten statements were related to 2FA in general, were correct or incorrect, and e.g. contained misconceptions we discovered in the interviews, e.g., "If I

[9] Interestingly, Clickworker demanded to use 2FA at that time [28].

use the fingerprint scanner/face recognition instead of a password, this counts as a second factor." Within this set of statements was an attention check question.

**Backup Methods and Responsibilities** Participants were presented with different possibilities to create a backup for their second factor: An alternative phone number, an alternative email address, and backup codes. They were asked to pick their favorite option and indicate how many of their accounts have such a backup. Following a theme from the interviews, we then asked whether it would be worse if an attacker got access to their account or if they lost access themselves.

Subsequently, we explored what participants thought about responsibility regarding account access and asked for their willingness to use personal information for account recovery. We then presented the participants with 15 personal and account-specific information used by some services for account recovery (based on findings by Amft et al. [10] and our own experiences from Chapter 6). Participants were asked to indicate for how many services they could provide this information.

### Analysis

We report descriptive statistics where applicable. Since the free-text answers were fairly simple and a codebook from the interviews could be used, answers were analyzed by one researcher with a second researcher being consulted when needed, as suggested by Ortloff et al. [132].

### Participants

The full demographics and overview of the participants' 2FA usage are given in Table 7.2. We recruited more male than female participants, and most considered themselves tech-savvy.

**Usage of 2FA** Like in the interviews, many participants reported using 2FA for their payment services, email, and device accounts (Google, Apple). Receiving codes via SMS was the most popular second factor, and almost half of the sample also used an authenticator app.

Thirteen participants stated that they had already experienced losing a second factor. Eight of them explained that they needed to contact the support to regain access. In two cases, it is unclear whether the participant was able to recover the account.

### Ethics

The survey followed the German data protection laws and the GDPR in the EU. Before the survey was started, the participants were informed about how the data would be processed and had to accept these terms to start the survey. All closed questions required an answer

| Demographics | Number of Participants | |
|---|---|---|
| Gender | Female: | 38 |
| | Male: | 57 |
| Age | 18-25: | 9 |
| | 26-35: | 30 |
| | 36-45: | 25 |
| | 46-55: | 14 |
| | 56 - 65 | 13 |
| | > 65 | 4 |
| Current Occupation | Student & Apprentice: | 7 |
| | Employed: | 79 |
| | Other: | 9 |
| Self-Describe as Tech-Savvy | No: | 25 |
| | Yes: | 63 |
| | Not disclosed | 7 |
| (Self-reported) Services with 2FA | Payment: | 61 |
| | Device accounts (Google, Apple): | 43 |
| | Retail: | 29 |
| | Social media: | 19 |
| | Communication: | 18 |
| | Other: | 4 |
| Second factor | SMS: | 69 |
| | Authenticator App: | 50 |
| | Email: | 27 |
| | Physical token: | 10 |
| | Other: | 3 |

**Table 7.2** – Demographics of survey participants (n = 95). Participants could select several services and second factors. Payment services do not include online banking.

but had the option “I don’t want to state.” We did not collect any personally identifiable information.

### 7.3.2 Results

In the following, we present our results, again ordered by our research questions.

#### RQ1: What Backup Strategies - If Any - Do Users Have for Their 2FA Accounts?

We asked participants for how many of the accounts they protect with a second factor they have another way to log in (e.g., backup codes stored on another device, Q9). While 37.9% were unsure, 29.5% selected "More than half of the websites." Only 6.3% claimed to have backups for all their accounts. A full overview is given in Figure 7.1.

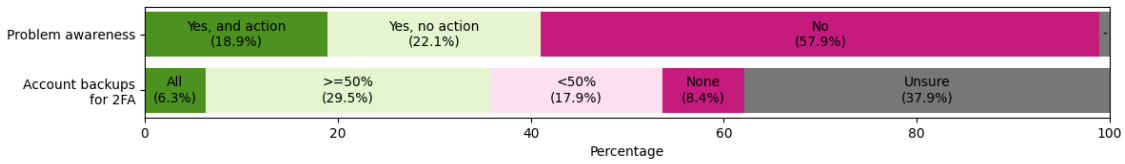


**Figure 7.1** – Answers of survey participants to whether they have ever thought about losing the second factor, and for how many of the accounts they potect with a second factor they are aware of a backup way to log in. Over half of the participants were not aware of the potential issue, and over a third did not know how many of their accounts they could access without the second factor.

As personal data or account information often helps to regain access, we presented the participants with several items that websites sometimes use or could use to check the legitimacy of the request and asked participants for how many accounts they would be able to provide that information (Q14). When looking at Figure 7.2, one can see that it seems that only very basic information can be easily answered by most participants for most of their accounts, such as the connected email address, phone number, username, or given name. Information that could be argued to be less easily obtained by an attacker, such as the date an account was created or the last login, was also harder for the participants. For example, for the account creation date, over half of the participants stated that they would not be able to provide this information for any of their accounts. We discuss this issue in Section 7.4.1.

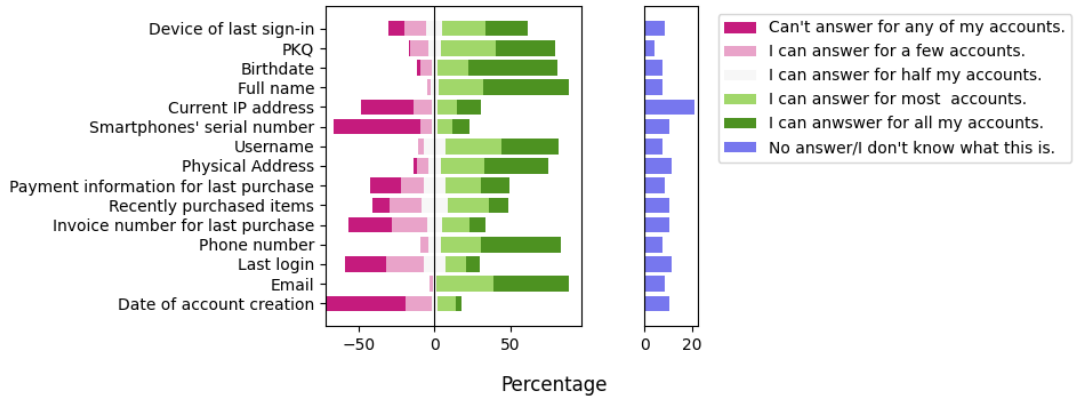


**Figure 7.2** – Answers of survey participants about what information they could answer for how many of the accounts they protect with a second factor. Especially basic information, such as the participant's name or birthdate, could be answered by most participants for most of their accounts.

In contrast to the interviews, the lack of depth in the survey makes it impossible to determine whether everyone would regain access to their accounts. Yet, we additionally asked whether participants had ever thought about the issue of losing their second factor (Q4). 55 participants stated they never did. Of those 39 who did, only 18 mentioned they looked

for a solution; see Figure 7.1 in the appendix.

So, even though we cannot evaluate the situation individually, it seems as if many participants would only regain access because they could use additional information and not because they have a strategy themselves, confirming the theme from the interview.

### RQ2: What 2FA Backup Mechanisms Do Participants Favor over Others?

Similar to the interview, we asked participants what backup possibility they would favor and shortly explained *alternative email address*, *alternative phone number*, and *backup codes* (Q8). We omitted the delegated account recovery app approach, as we found this to require too much text. Participants in the survey preferred a backup email address (47.4%), followed by backup codes (32.6%).

In the interviews, one of the favored approaches was to provide the website with an identity document, so we included a question of whether participants would be willing to do so (Q12). Interestingly, 44.2% stated they would not upload their identity document on *any* website. 33.7% stated they would upload their document on some websites. When asked how they differentiate (Q12.1), participants often reasoned with the importance of their accounts and trustworthiness and experience with the service in question.

We additionally asked for alternative backup approaches that we did not mention before (backup email address/phone number and backup codes) that participants would like to use to regain access (Q16). The most common theme was again to compare personal data (including PKQ) or provide the service with proof of identity.

Similar to the interviews, there does not seem to be one method that is clearly more favored by the participants than the others.

### RQ3 - What Expectations Do People Have of Websites Regarding Account Recovery?

We showed the participants' assumption statements regarding account recovery, which we captured in the interviews. We asked them to imagine that they lost their second factor and asked participants to indicate their level of agreement (Q6). Similar to the interviews, many participants (85.3%) fully or partially agreed that they expect to be able to contact the website's support, and 75.8% fully or partially agreed that they are sure a website will provide a possibility for them to regain access to their account (see Figure 7.3). The theme of personal information was also similar to the interviews: 66.3% fully or partially agreed that they would regain access if they provided personal information. UI wise, 73.7% agreed that they expect a help button, similar to the "password forgotten?"-button.

When asked about responsibility (Q11), 55.8% of the participants agreed (fully agree and partially agree) that they found it more secure if users are responsible for being able to access the accounts and that websites do not assist. 62.1% said the website should help. 52.6% selected both, potentially showing the trade-off that was also visible in the interviews.

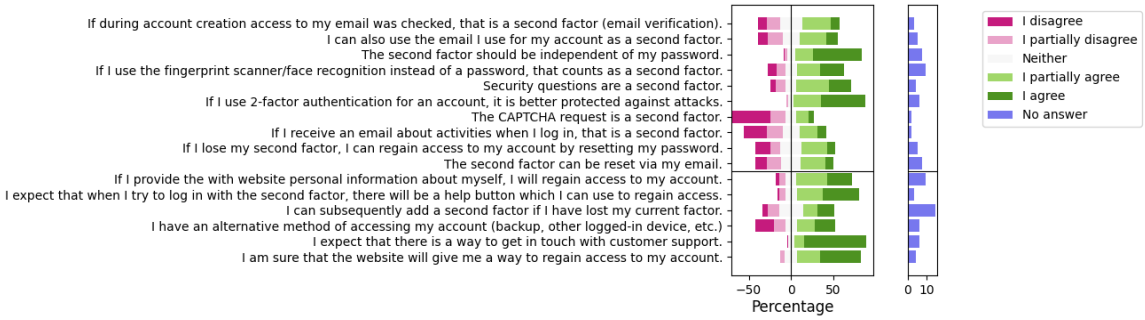


**Figure 7.3** – Knowledge survey participants had about 2FA and their assumptions regarding 2FA recovery. Most participants expect they can reach out to a service and that a service will offer them a possibility to regain access to their accounts.

### Additional Findings

**Misconceptions about 2FA** During the interviews, we captured some misconceptions, which we included in the survey to understand the participants' knowledge about 2FA (Q7). We also added correct statements and some that might be true on some websites but would generally not be seen as best practice (e.g., that a second factor can be recovered by resetting the password). The results are depicted in Figure 7.3. Around a third of the participants fully or partially agreed that a second factor could be recovered by resetting the password.

**Access by Strangers** As we saw that some participants in the interview first thought about unauthorized access of strangers if they lost their phone, we wanted to investigate this further (Q10). The data depicts a clear picture: 66.3% rated it to be significantly or somewhat worse if a stranger got access to an account, 29.5% rated the situations to be equally bad.

## 7.4 Discussion

We conducted 16 interviews and a survey with 95 participants to understand users' assumptions regarding losing a second factor for authentication purposes on websites. We also investigated users' preferences regarding backup possibilities. Even though we did not recruit a representative sample, we believe that our results can give valuable insights into users' expectations towards account recovery and can inform future work. In the following, we discuss our results in light of our research questions, resulting in recommendations for websites and directions for future work.

### 7.4.1 Perception of Recovery Options

We wanted to understand what backup methods participants used and how they were rated compared to each other. We found that there was a wide spread of preferred methods, as some participants were more interested in usability, while others valued security and privacy more. Still, many participants did not seem to have a backup method but expected to regain access by answering questions about themselves or favored this option compared to others. This approach is often implemented by services [70, 10]. Thus, we tried to get a deeper understanding of what information participants could provide exactly. For this, we found that only basic and easily obtainable information was in the top spots.

Some participants also mentioned personal knowledge questions, even though PKQ have proven to provide an unfortunate combination in previous studies: Users were often not able to recall their answers, yet their answers were often predictable [14, 150, 146].

It seems as if personal data and knowledge as a means for recovery are easy to understand for users. However, especially as users only seem to know basic information, this is not a secure approach. We encourage future research to understand if there is another approach that is more secure and similarly easy to understand (e.g., eIDs).

### 7.4.2 What Could Websites Do to Improve Users' Recovery Experience?

We think our findings can inform websites on how they could assist users with 2FA setup and account recovery and can support recommendations made by related work that analyzed recovery procedures without user studies. We assembled a few suggestions themed by the steps needed for account recovery, based on related work and our findings.

**Setup & Handling: Help Users Create a Good Backup** Many participants have never considered what would happen if they lost their second factor. To circumvent this issue, Amft et al. [10] recommends websites collect all information that is needed for account recovery during account setup and inform users about needed documents. Going one step further, we additionally noted that participants sometimes seemed to have difficulty implementing a backup, e.g., participants once downloaded backup codes but were not aware of the location, and not all participants who used an authenticator app with a backup functionality used it. Even though such backups are a good idea usability-wise, they may not be a solution for everyone, and some also provide attack vectors [75]. Still, it might make sense for websites to explain better what to do with a backup or where to store it best during 2FA registration. Höltervennhoff et al. [86] discussed users' strategies for dealing with recovery codes, finding that none of them is flawless. It is up to future research to understand what advice best helps users manage possible backups.

Another viable approach might be to encourage users to check if they still have access to their backups occasionally, as also noted by Amft et al. [10]. This was also something that the interview participants brought up. Yet, in a study by Das et al. [36], users did not always understand why websites did this. It remains to be researched if there is a way to make it clear and in what frequency it should be done.

**Setup: Allow More Than One Second Factor** Of the five interview participants aware of having backups, three used an additional second factor rather than a dedicated backup method. Even though this area might need more research, we believe that it might be a good idea for websites to allow adding more than one second factor. Currently, as found by Lyastani et al. [109], only 40% of the investigated websites do so.

**Set the Context: Help Users Assess Their Situation (or Do It for Them)** It seems that not all users are equally likely to lose access to their accounts if they lose their second factor. For example, if SMS codes are their second factor and they lose their phone, they can most likely order a new SIM card or reactivate the number on a new phone. On the other hand, this is not possible if a user uses an authenticator app without backups. Recovery also depends on how many devices users use to access their accounts. There are users whose main device is a smartphone, as mentioned by two participants in the interview. We thus believe there is no one-fits-all solution, and it seems to make sense that websites look at their users' general technological setup and social context. A starting point could be to differentiate between those users who will easily regain access and those who might have a harder time. The latter could then, e.g., be reminded about their backup possibilities more often.

**Starting the Recovery: Help for Self-Help** In Chapter 6, we found that several websites did not link to their most helpful FAQ pages on their login page when authentication failed, and Amft et al. [10] found that a quarter of the websites they analyzed did not give any information about recovery within their support pages. This practice was also brought up and criticized by our study participants. Linking to a helpful support page should be obvious, but further research is needed to see what can be done to assist developers and admins in implementing this.

To further increase the helpfulness of these pages, we found that the recovery approaches *not* mentioned by the participants could shed light on what elements websites could include in their FAQs: During the interviews, no participant mentioned that they might still be logged into the account on another device they could use to disable 2FA. It was also rarely mentioned that one could order a new SIM card with the same number (in case one receives SMS codes). Even though participants might remember such steps in an emergency situation, we recommend websites prompt users about these options.

As we saw, several participants were not sure whether they, in fact, had any backups for their accounts. It might help to support them in finding possible backups (e.g., by providing the name of the file containing the backup codes as done by Discord [39], allowing users to store a hint or reminding them of the time they implemented a backup).

We also observed one case where a participant lost access to their account as the computer's system time was incorrect, and thus their Yubikey did not work. As the participant had a background in IT, they eventually figured out that this was the problem. However, as login mechanisms get more technically sophisticated and thus potentially harder for non-experts to understand, ideas on how to solve log-in issues might become even more relevant in the future.

**Starting the Recovery: Offer (Helpful) Support** Contacting the support team or looking for a way to do so was the most frequent step participants mentioned when we asked them to evaluate what they would do. Even though many services offer customer support, we ([70], Chapter 6) and Amft et al. [10] also identified websites that only have support for certain user groups, only offer support for logged-in users, and websites that offered support but did not respond.

### 7.4.3 Users' Interpretation of the Word "2FA"

In addition to our research questions, we found that several participants (in the interviews and the survey) showed misconceptions about what 2FA is, e.g., believing CAPTCHAs, sign-up verification emails, or fingerprints instead of a password to fall under this category.

Additionally, the distinction between 2FA (as a security feature that asks for a second factor every time a device remembrance timeout has passed) and RBA (as something that is independent of the user's choices and where an additional proof of identity is only necessary if a certain risk factor is exceeded) did not seem to be present in all the participants' minds.

With these misconceptions, we add further knowledge to prior work, which has identified misconceptions regarding authentication and uncertainty about terms used for authentication measures [102, 5, 9, 99, 37, 86].

In general, we believe that users do not necessarily need to be aware of either the working of 2FA or that they use 2FA as a service if the user interface is solid enough to take precautions for account lockout for such users by, e.g., collecting data that can be used to recover the account. If users are unaware that they would need the second factor to log in (e.g., on a currently unknown device) and have no knowledge about possible recovery possibilities, websites need to prevent accidental lockouts. As seen in related work (see Section 2.3.2), this is currently not always the case.

We explicitly phrased our study in a way that it was not relevant if a user knew exactly what 2FA means, as we described the scenario in which a second factor (phone) is necessary to log in. Additionally, all participants remembered at least one account for which they believed to need another factor next to the password to log in, which was sufficient for our research questions. However, if future work wants to investigate different elements of 2FA further and needs to be sure to recruit only people who have 2FA enabled (as opposed to RBA), it might not be enough to ask participants whether they use 2FA.

### 7.4.4 Hypothetical Scenario

We were interested in how users would handle the loss of a second factor. As this is an extraordinary situation, we could not study it as participants encountered it. We thus decided on the hypothetical scenario of imagining losing the second factor based on the following reasons:

- We did not want to endanger real accounts and did not want to trigger lockouts. Thus, we did not want to play through the loss of a second factor for any of the participants' real accounts.

- Before the presented studies, we experimented with setting up dummy accounts based on real configurations of participants, which would have made a recovery attempt more realistic. However, we noted that there are several factors that are harder to mimic than simply choosing the same second factor, such as real user data stored on the account that might be helpful in recovery and metadata, such as known devices or times and locations at and from which a user normally logs in. In their work on risk-based account recovery, Büttner et al. [19], for example, noted that for Amazon, additional checks during account recovery were inconsistent. Even though previous work had a similar limitation ([70, 10]), we decided against this approach as this would have made support staff of the websites unconsenting study participants.
- We also considered only recruiting participants with previous experiences with account recovery. However, we started recruiting without this requirement to understand how common such issues are among the population. We quickly noticed that even those participants in our study who had experiences with loss and account recovery could often not completely recall how they regained access and what had to be done in detail (e.g., what information had to be shared with the service) and thus decided to keep the hypothetical scenario.

We believe that by first openly asking what participants would do and then also showing videos of non-working recovery attempts gave us a good understanding of what users would or would probably not try to do in case of access issues.

### 7.4.5 Limitations

Our work and results have to be interpreted in the light of the following limitations: We conducted interviews and a survey and asked about the hypothetical scenario of the user losing their second factor. We could thus only capture the first ideas of what participants would try to do, which were independent of the websites they secured with a second factor. It might be that participants have, in fact, a backup they were not aware of but that a website would remind them of.

The interview used a convenience sample recruited at our university, local supermarkets, and the Kleinanzeigen online community. The survey used a sample drawn from Clickworker. For the interview, we recruited only a small number of participants who used a second factor other than receiving an SMS code. Further work is needed to see whether our findings apply to a broader population.

During the interviews, participants only realized after a while that a backup they thought might work also depended on the second factor. During the survey, participants might not have had the time to think about this issue, and we could not direct the questions individually in that direction.

In addition, the delegated account recovery app included in the interviews was not included in the survey, as we felt it needed too much text to be properly explained. In the interviews, participants often did not rate the combination of an app and an identification document but reacted to one part alone.

# Chapter 8

# Conclusion

This thesis covered two topics aimed at improving account security and decreasing unauthorized access: password composition policies (PCPs) and two-factor authentication (2FA).

To explore the first topic, over 250 German companies were surveyed over a span of four years. This research allowed for an examination of how PCPs are chosen and the speed at which recommendation changes are adopted. In the first year, there was a high heterogeneity in the PCPs, along with a high prevalence of PCP elements that both the research community and NIST consider harmful and user-unfriendly, such as password expiry and character class requirements. At that time, the BSI included password expiry in its guidelines, which might explain its widespread use among companies.

In the subsequent years, following the BSI's removal of its recommendation for time-based password changes, the number of companies implementing password expiry decreased from 72.2% in 2019 to 45% in 2023. Participants who continued to use a regular expiry reasoned this with security improvements and adherence to additional guidelines from other institutions. Alternative checks were often not implemented due to resource constraints or technical hurdles.

For the second topic, 2FA, I focused on the recovery process and user assumptions. The aim was to understand how popular services guide users through 2FA setup and recovery when the second factor is inaccessible. Expert reviews of 78 services were conducted to analyze their approaches to informing users about the potential risks of 2FA, the availability of backup options, and the level of support provided during recovery. The results revealed that services do not seem to follow a standardized practice for 2FA setup or recovery, and the level of support varies greatly. The findings indicate that only a small percentage of services communicate the importance of having a fallback. Additionally, some services offer no assistance during the recovery process, leaving users to resolve the issue on their own.

To further understand user experiences with 2FA recovery, 16 interviews were conducted, and 95 participants were surveyed. The focus was on whether users currently have access to a backup, their expectations during recovery, their problem-solving approaches, and their preferred types of backups.

It was found that many participants lack a dedicated backup plan and assume that providing personal information to a service will allow them to regain access to their accounts. This

is often linked to the expectation that services will assist a user in need. Most often, expressed a shared sense of responsibility for account access: while they recognize their own responsibility in safeguarding the second factor, they also expect services to offer help if needed.

Based on these findings, this thesis provides recommendations for website providers to enhance the user experience when losing a second factor.

# List of References


[1] 1Password. Passkeys.directory. https://passkeys.directory/. Accessed: June 18, 2024.

[2] The 2factorauth Group. 2FA Directory. https://web.archive.org/web/20240313231245/https://2fa.directory/de/. Accessed: June 18, 2024.

[3] 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, New York, NY, USA, April 2020. Association for Computing Machinery.

[4] 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.

[5] Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[6] Agari. Anatomy of a compromised account. https://www.agari.com/resources/guides/anatomy-compromised-email-account, No year given. Accessed: May 26, 2023.

[7] Devdatta Akhawe, Johanna Amann, Matthias Vallentin, and Robin Sommer. Here's My Cert, so Trust Me, Maybe? Understanding TLS Errors on the Web. In *Proceedings of the 22nd International Conference on World Wide Web*, WWW '13, page 59–70, New York, NY, USA, 2013. Association for Computing Machinery.

[8] FIDO Alliance. FIDO2 - FIDO Alliance. https://web.archive.org/web/20240612193856/https://fidoalliance.org/fido2/. Accessed: June 18, 2024.

[9] National Cybersecurity Alliance. Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2023. https://staysafeonline.org/online-safety-privacy-basics/oh-behave/. Accessed: June 18, 2024.

[10] Sabrina Amft, Sandra Höltervennhoff, Nicolas Huaman, Alexander Krause, Lucy Simko, Yasemin Acar, and Sascha Fahl. "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 3138–3152, New York, NY, USA, 2023. Association for Computing Machinery.

[11] Apple. iCloud+ - Find My - Apple. `https://web.archive.org/web/20240617015517/https://www.apple.com/icloud/find-my/`. Accessed: June 18, 2024.

[12] Bitkom. Gestohlen oder verloren: Vier von zehn Personen ist schon mal das Handy abhandengekommen. `https://web.archive.org/web/20240304061753/https://www.bitkom.org/Presse/Presseinformation/Gestohlen-oder-verloren-Vier-von-zehn-Personen-ist-schon-mal-das-Handy-abhandengekommen`. Accessed: June 18, 2024.

[13] Cyber Security Cluster Bonn. Cyber Security Cluster Bonn. `https://web.archive.org/web/20240616185315/https://cyber-security-cluster.eu/`. Accessed: June 18, 2024.

[14] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike 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*, pages 141–150. International World Wide Web Conferences Steering Committee, 2015.

[15] Joseph Bonneau and Sören Preibusch. The Password Thicket: Technical and Market Failures in Human Authentication on the Web. In *WEIS*, 2010.

[16] Christiaan Brand. Google Online Security Blog: Google Authenticator now supports Google Account synchronization. `https://web.archive.org/web/20240708083412/https://security.googleblog.com/2023/04/google-authenticator-now-supports.html`, 2023. Accessed: July 08, 2024.

[17] William E. Burr, Donna F. Dodson, and W. Timothy Polk. Electronic Authentication Guideline - Recommendations of the National Institute of Standards and Technology. `https://web.archive.org/web/20231008120203/https://csrc.nist.gov/CSRC/media/Publications/sp/800-63/ver-10/archive/2004-06-30/documents/sp800-63-v1-0.pdf`. Accessed: July 17, 2024.

[18] 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.

[19] Andre Büttner, Andreas Thue Pedersen, Stephan Wiefling, Nils Gruschka, and Luigi Lo Iacono. Is It Really You Who Forgot the Password? When Account Recovery

Meets Risk-Based Authentication. In *International Conference on Ubiquitous Security*, pages 401–419. Springer, 2023.

[20] Andy C. How To Avoid Losing Your Phone. https://web.archive.org/web/20240708084247/https://www.mobiles.co.uk/blog/how-to-avoid-losing-your-phone/. Accessed: July 08, 2024.

[21] John L. Campbell, Charles Quincy, Jordan Osserman, and Ove K. Pedersen. Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. *Sociological Methods & Research*, 42(3):294–320, 2013.

[22] The National Cyber Security Centre. National Cyber Security Centre. https://web.archive.org/web/20240708084756/https://www.ncsc.gov.uk/. Accessed: July 08, 2024.

[23] Rahul Chatterjee, Joanne Woodage, Yuval Pnueli, Anusha Chowdhury, and Thomas Ristenpart. The TypTop System: Personalized Typo-Tolerant Password Checking. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 329–346, New York, NY, USA, 2017. Association for Computing Machinery.

[24] Sonia Chiasson and Paul C Van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography*, 77:401–408, 2015.

[25] Dave Childers. State of the auth 2021. https://web.archive.org/web/20240708090104/https://duo.com/assets/ebooks/state-of-the-auth-2021.pdf, 2021. Accessed: July 08, 2024.

[26] Yee-Yin Choong, Mary Theofanos, and Hung-Kung Liu. United States Federal Employees' Password Management Behaviors - a Department of Commerce case study. Technical Report NIST IR 7991, National Institute of Standards and Technology, April 2014.

[27] Clickworker. AI Training Data and other Data Management Services. https://web.archive.org/web/20240708092958/https://www.clickworker.com/. Accessed: July 08, 2024.

[28] Clickworker. Problems with App Login Confirmation (2-Factor Authentication). https://web.archive.org/web/20240708093227/https://support-workplace.clickworker.com/support/solutions/articles/80000949198-problems-with-app-login-confirmation-2-factor-authentication. Accessed: July 08, 2024.

[29] Jacob Cohen. A Coefficient of Agreement for Nominal Scales. *Educational and psychological measurement*, 20(1):37–46, 1960.

[30] 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.

[31] Morning Consult. IBM Consumer Survey: Security side effects of the pandemic. https://web.archive.org/web/20240704031456/https://filecache.mediaroom.com/mr5mr_ibmnews/191177/Pandemic%20Security%20Side%20Effects%20Global%20Survey_IBM%20Analysis.pdf. Accessed: July 08, 2024.

[32] Juliet M. Corbin and Anselm Strauss. Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology*, 13(1):3–21, 1990.

[33] Anastasia Danilova, Alena Naiakshina, Anna Rasgauski, and Matthew Smith. Code Reviewing as Methodology for Online Security Studies with Developers - A Case Study with Freelancers on Password Storage. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 397–416. USENIX Association, August 2021.

[34] 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.

[35] 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.

[36] Sanchari Das, Bingxi Wang, and L. Jean Camp. MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content. *CoRR*, abs/1908.05902, 2019.

[37] Sanchari Das, Bing xing Wang, Andrew Kim, and L. Jean Camp. MFA is A Necessary Chore!: Exploring User Mental Models of Multi-Factor Authentication Technologies. In *Hawaii International Conference on System Sciences*, 2020.

[38] Rose de Fremery. World Password Day: The History of Passwords. https://web.archive.org/web/20240708093646/https://blog.lastpass.com/posts/2023/04/world-password-day-the-history-of-passwords. Accessed: July 08, 2024.

[39] Discord. Lost Two-Factor Codes - Discord. https://web.archive.org/web/20240708093938/https://support.discord.com/hc/en-us/articles/115001221072-Lost-Two-Factor-Codes. Accessed: July 08, 2024.

[40] 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.

[41] 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.

[42] Let's Encrypt. Let's Encrypt - Stats. `https://web.archive.org/web/20240708094213/https://letsencrypt.org/stats/#growth`, 2022. Accessed: July 08, 2024.

[43] 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.

[44] FAZ. Nicht immer wieder das Passwort ändern. `https://web.archive.org/web/20240708094847/https://www.faz.net/aktuell/wirtschaft/bsi-verabschiedet-sich-vom-regelmaessigen-passwort-wechsel-16616730.html`, 2020. Accessed: July 08, 2024.

[45] Federal Office for Information Security (BSI). Umsetzungshinweise zum Baustein: ORP.4. Identitäts- und Berechtigungsmanagement. `https://web.archive.org/web/20240424034139/https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf?__blob=publicationFile&v=1`. Accessed: July 17, 2024.

[46] Federal Office for Information Security (BSI). IT-Grundschutz Compendium - Final Draft, 1 February 2019. `https://web.archive.org/web/20240316144441/https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-it-gs-comp-2019.pdf?__blob=publicationFile&v=1`, 2019. Accessed: July 17, 2024.

[47] Federal Office for Information Security (BSI). IT-Grundschutz-Kompendium 2. Edition 2019. `https://web.archive.org/web/20221027100737/http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf?__blob=publicationFile&v=5`, 2019. Accessed: July 17, 2024.

[48] Federal Office for Information Security (BSI). IT-Grundschutz-Kompendium Februar 2020. `https://web.archive.org/web/20240316215500/https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/`

IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=1, 2020. Accessed: July 17, 2024.

[49] Federal Office for Information Security (BSI). BSI - IT-Grundschutz. https://web.archive.org/web/20240717115902/https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, 2021. Accessed: July 17, 2024.

[50] Federal Office for Information Security (BSI). IT-Grundschutz Compendium - Final Draft, 1 February 2021. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf?__blob=publicationFile&v=4, 2021. Accessed: May 26, 2023.

[51] Federal Office for Information Security (BSI). IT-Grundschutz-Kompendium Februar 2021. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6, 2021. Accessed: April 04, 2024.

[52] Federal Office for Information Security (BSI). IT-Grundschutz Compendium - Final Draft, 1 February 2022. https://web.archive.org/web/20240717214705/https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2, 2022. Accessed: July 22, 2024.

[53] Federal Office for Information Security (BSI). IT-Grundschutz-Kompendium Februar 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf?__blob=publicationFile&v=3, 2022. Accessed: April 04, 2024.

[54] Federal Office for Information Security (BSI). IT-Grundschutz-Kompendium (Edition 2023). https://web.archive.org/web/20240316170507/https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.html, 2023. Accessed: July 22, 2024.

[55] Federal Office for Information Security (BSI). BSI - Organisation and structure. https://web.archive.org/web/20240717214737/https://www.bsi.bund.de/EN/Das-BSI/Organisation-und-Aufbau/organisation-und-aufbau_node.html, No year given. Accessed: July 22, 2024.

[56] Joseph L. Fleiss, Bruce Levin, and Myunghee C. Paik. *Statistical methods for rates and proportions*. John Wiley & Sons, 2013.

[57] Dinei Florêncio and Cormac Herley. Where do security policies come from? In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*, New York, NY, USA, 2010. Association for Computing Machinery.

[58] Canadian Centre for Cyber Security. Canadian Centre for Cyber Security. https://web.archive.org/web/20240708095206/https://www.cyber.gc.ca/en. Accessed: July 08, 2024.

[59] Federal Office for Information Security. BSI - Mission Statement. https://web.archive.org/web/20240515124342/https://www.bsi.bund.de/EN/Das-BSI/Leitbild/leitbild_node.html. Accessed: July 08, 2024.

[60] Federal Office for Information Security. Creating Secure Passwords. https://web.archive.org/web/20240708100101/https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html. Accessed: July 08, 2024.

[61] Federal Office for Information Security. Cyber security recommendations. https://web.archive.org/web/20240618182054/https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html. Accessed: July 08, 2024.

[62] Federal Office for Information Security. Two-factor Authentication. https://web.archive.org/web/20240708100844/https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html. Accessed: July 22, 2024.

[63] Federal Office for Information Security. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. https://web.archive.org/web/20240708105230/https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema_Kompendium.pdf?__blob=publicationFile&v=1, 2019. Accessed: July 22, 2024.

[64] Deen Freelon. ReCal2. https://web.archive.org/web/20240708105313/http://dfreelon.org/utils/recalfront/recal2/, No year given. Accessed: July 08, 2024.

[65] David Freeman, Sakshi Jain, Markus Dürmuth, Battista Biggio, and Giorgio Giacinto. Who Are You? A Statistical Approach to Measuring User Authenticity. In *NDSS*, volume 16, pages 21–24, 2016.

[66] Pilar Garcia. 10 - Pilar Garcia - Who are you again? Verifying user access rights in an encryption based system. https://web.archive.org/web/20240708105434/https://www.youtube.com/watch?v=JeV_rop5nmQ, 2019. Accessed: July 08, 2024.

[67] Anuj Gautam, Shan Lalani, and Scott Ruoti. Improving Password Generation Through the Design of a Password Composition Policy Description Language. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 541–560, Boston, MA, August 2022. USENIX Association.

[68] 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.

[69] Lisa Geierhaas, Anna-Marie Ortloff, Matthew Smith, and Alena Naiakshina. Let's Hash: Helping Developers with Password Security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 503–522, Boston, MA, August 2022. USENIX Association.

[70] Eva Gerlitz, Maximilian Häring, Charlotte Theresa Mädler, Matthew Smith, and Christian Tiefenau. Adventures in Recovery Land: Testing the Account Recovery of Popular Websites When the Second Factor is Lost. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 227–243, Anaheim, CA, August 2023. USENIX Association.

[71] Eva Gerlitz, Maximilian Häring, and Matthew Smith. Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 17–36. USENIX Association, August 2021.

[72] Eva Gerlitz, Maximilian Häring, Matthew Smith, and Christian Tiefenau. Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 191–210, Anaheim, CA, August 2023. USENIX Association.

[73] 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.

[74] 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.

[75] 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.

[76] GitHub. Informationen zur obligatorischen Zwei-Faktor-Authentifizierung. `https://web.archive.org/web/20240708141126/https://docs.github.com/de/authentication/securing-your-account-with-two-factor-authentication-2fa/about-mandatory-two-factor-authentication`. Accessed: July 08, 2024.

[77] GitHub. Top-500 npm package maintainers now require 2FA. https://web.archive.org/web/20240708141615/https://github.blog/changelog/2022-05-31-top-500-npm-package-maintainers-now-require-2fa/. Accessed: July 08, 2024.

[78] 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.

[79] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. "What was that site doing with my Facebook password?": Designing Password-Reuse Notifications. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1549–1566, New York, NY, USA, 2018. Association for Computing Machinery.

[80] Google. Google Authenticator. https://web.archive.org/web/20240708142604/https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2. Accessed: July 08, 2024.

[81] Paul A. Grassi. Publish#1. https://github.com/usnistgov/800-63-3/commit/3fb942e2f795f681155144d06933db28f29278e0#diff-c10a8efb34bad3a0b9a47880106e0f255f5f866f12fdcccbd73b7338ea82d301, 2016. Accessed: May 26, 2023.

[82] 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. https://doi.org/10.6028/NIST.SP.800-63b.

[83] Hana Habib, Jessica Colnago, William Melicher, Blase Ur, Sean Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Cranor. Password Creation in the Presence of Blacklists. *Proc. USEC*, page 50, 2017.

[84] Hana Habib, Pardis E. Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. User Behaviors and Attitudes Under Password Expiration Policies. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS) 2018*, pages 13–30, Baltimore, MD, August 2018. USENIX Association.

[85] Beatriz Henríquez. Mobile Theft and Loss Report - 2020/2021 Edition | Prey Blog. https://web.archive.org/web/20240708143849/https://preyproject.com/blog/mobile-theft-and-loss-report-2020-2021-edition. Accessed: July 08, 2024.

[86] Sandra Höltervennhoff, Noah Wöhler, Arne Möhle, Marten Oltrogge, Yasemin Acar, Oliver Wiese, and Sascha Fahl. A Mixed-Methods Study on User Experiences and Challenges of Recovery Codes for an End-to-End Encrypted Service. In *In 33rd USENIX Security Symposium*, 2024.

[87] Andy Homan. 44% of people lose their mobile. `https://web.archive.org/web/20240708150738/https://nuttag.com.au/blogs/news/44-of-people-loose-their-mobile`. Accessed: July 08, 2024.

[88] Hypr. Report: State of Authentication in the Finance Industry 2022. `https://web.archive.org/web/20240708151120/https://get.hypr.com/state-of-authentication-in-the-finance-industry-2022`, No year given. Accessed: July 08, 2024.

[89] Identico. We Protect Accounts. No Compromise. `https://web.archive.org/web/20240709130023/https://identeco.de/en/`. Accessed: July 09, 2024.

[90] Philip G. Inglesant and Martina A. Sasse. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, page 383–392, New York, NY, USA, 2010. Association for Computing Machinery.

[91] Hasso Plattner Institut. 123456789 ist das beliebteste Passwort 2023 in Deutschland. `https://web.archive.org/web/20240709130154/https://hpi.de/news/jahrgaenge/2023/123456789-ist-das-beliebteste-passwort-2023-in-deutschland.html`. Accessed: July 09, 2024.

[92] Hasso Plattner Institut. Identity Leak Checker. `https://web.archive.org/web/20240709130646/https://sec.hpi.de/ilc/`. Accessed: July 09, 2024.

[93] 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.

[94] Jurik Caspar Iser. Bundesamt hält regelmäßigen Passwortwechsel nicht mehr für notwendig. `https://web.archive.org/web/20240709131256/https://www.zeit.de/digital/datenschutz/2020-02/bsi-empfehlung-passwort-wechsel`, 2020. Accessed: July 09, 2024.

[95] Patrick G. Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie F. Cranor, and Julio Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *2012 IEEE Symposium on Security and Privacy*, pages 523–537. IEEE, 2012.

[96] Simon Kemp. Digital 2024: Global Overview Report. https://web.archive.org/web/20240709131456/https://datareportal.com/reports/digital-2024-global-overview-report. Accessed: July 09, 2024.

[97] Guemmy Kim. Making you safer with 2SV. https://web.archive.org/web/20240709132040/https://blog.google/technology/safety-security/reducing-account-hijacking/. Accessed: July 09, 2024.

[98] Saranga Komanduri, Richard Shay, Patrick G. Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie F. Cranor, and Serge Egelman. Of Passwords and People: Measuring the Effect of Password-Composition Policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2595–2604, New York, NY, USA, 2011. Association for Computing Machinery.

[99] 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.

[100] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. "If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 246–263, 2019.

[101] Arkose Labs. 70% Increase in Fraudulent Account Registrations Puts Digital Accounts in the Crosshairs, Arkose Labs Reports. https://www.businesswire.com/news/home/20210805005657/en/70-Increase-in-Fraudulent-Account-Registrations-Puts-Digital-Accounts-in-the-Crosshairs-Arkose-Labs-Reports, 2021. Accessed: May 26, 2023.

[102] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "It's Stored, Hopefully, on an Encrypted Server'': Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 91–108. USENIX Association, August 2021.

[103] LastPass. Emergency Access - Lastpass. https://www.lastpass.com/features/emergency-access. Accessed: February 07, 2024.

[104] Kevin Lee, Sten Sjöberg, and Arvind Narayanan. Password policies of most top websites fail to follow best practices. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 561–580, Boston, MA, August 2022. USENIX Association.

[105] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. Keepers of the Machines: Examining How System Administrators Manage Software Updates For Multiple Machines. In *Fifteenth Symposium on Usable Privacy and*

*Security (SOUPS 2019)*, pages 273–288, Santa Clara, CA, August 2019. USENIX Association.

[106] 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.

[107] Lookout. PHONE THEFT IN AMERICA. https://web.archive.org/web/20240519222907/https://transition.fcc.gov/cgb/events/Lookout-phone-theft-in-america.pdf. Accessed: July 10, 2024.

[108] Nate Lord. Uncovering Password Habits: Are Users' Password Security Habits Improving? (Infographic). https://web.archive.org/web/20240722124214/https://www.digitalguardian.com/blog/uncovering-password-habits-are-users%E2%80%99-password-security-habits-improving-infographic. Accessed: July 22, 2024.

[109] Sanam Ghorbani Lyastani, Sven Bugiel, and Michael Backes. A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites. In *Network and Distributed System Security (NDSS) Symposium 2023*, February 2023.

[110] Timo Malderle, Felix Boes, Gina Muuss, Matthias Wübbeling, and Michael Meier. Credential Intelligence Agency: A Threat Intelligence Approach to Mitigate Identity Theft. In Steven Furnell, Paolo Mori, Edgar Weippl, and Olivier Camp, editors, *Information Systems Security and Privacy*, pages 115–138, Cham, 2022. Springer International Publishing.

[111] Karl Mallach. About | Bitkom e.V. https://web.archive.org/web/20240228101917/https://www.bitkom.org/EN/About-us/About-us.html. Accessed: July 10, 2024.

[112] AbdelKarim Mardini and Guemmy Kim. Making sign-in safer and more convenient. https://web.archive.org/web/20240303022541/https://blog.google/technology/safety-security/making-sign-safer-and-more-convenient/. Accessed: July 10, 2024.

[113] 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.

[114] 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.

[115] Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth. "As soon as it's a risk, I want to require MFA": How Administrators Configure

Risk-based Authentication. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 483–501, Boston, MA, August 2022. USENIX Association.

[116] 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.

[117] Peter Mayer, Jan Kirchner, and Melanie Volkamer. A second look at password composition policies in the wild: Comparing samples from 2010 and 2016. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017*, pages 13–28, Santa Clara, CA, July 2017. USENIX Association.

[118] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie F. Cranor, Patrick G. Kelley, Richard Shay, and Blase Ur. Measuring Password Guessability for an Entire University. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 173–186, New York, NY, USA, 2013. Association for Computing Machinery.

[119] Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, and Matthew Smith. On Conducting Security Developer Studies with CS Students: Examining a Password-Storage Study with CS Students, Freelancers, and Company Developers. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[120] Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, Emanuel von Zezschwitz, and Matthew Smith. "If You Want, I Can Store the Encrypted Password": A Password-Storage Field Study with Freelance Developers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[121] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. Why Do Developers Get Password Storage Wrong? A Qualitative Usability Study. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 311–328, New York, NY, USA, 2017. Association for Computing Machinery.

[122] 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.

[123] Jakob Nielsen. 10 Usability Heuristics for User Interface Design. `https://web.archive.org/web/20240706211835/https://www.nngroup.com/articles/ten-usability-heuristics/`, 2021. Accessed: July 10, 2024.

[124] NIST Special Publication 800-57 Part 1: Recommendation for Key Management. https://web.archive.org/web/20240716140027/https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf, 2020. Accessed: July 22, 2024.

[125] NIST. NIST Special Publication 800-63: Digital Identity Guidelines - FAQ. https://web.archive.org/web/20240703095757/https://pages.nist.gov/800-63-FAQ/#q-b11, 2022. Accessed: July 22, 2024.

[126] Christoforos Ntantogian, Stefanos Malliaros, and Christos Xenakis. Evaluation of password hashing schemes in open source web platforms. *Computers & Security*, 84:206–224, 2019.

[127] Federal Office of Civil Protection and Disaster Assistance. Kritische Infrastrukturen - BKK. https://web.archive.org/web/20240615170006/https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html, No year given. Accessed: July 10, 2024.

[128] National Institute of Standards and Technology. About NIST | NIST. https://web.archive.org/web/20240615192005/https://www.nist.gov/about-nist. Accessed: July 10, 2024.

[129] Commission of the European Communities. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. https://web.archive.org/web/20240524081431/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361. Accessed: July 10, 2024.

[130] Federal Ministry of the Interior and Community of Germany. BMI - Ausweise & Pässe. https://web.archive.org/web/20240722125553/https://www.bmi.bund.de/DE/themen/moderne-verwaltung/ausweise-und-paesse/ausweise-und-paesse-node.html. Accessed: July 22, 2024.

[131] Federal Ministry of the Interior and Community of Germany. BundID. https://web.archive.org/web/20240410162338/https://id.bund.de/en/. Accessed: July 10, 2024.

[132] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. Different Researchers, Different Results? Analyzing the Influence of Researcher Experience and Data Type During Qualitative Analysis of an Interview and Survey Study on Security Advice. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[133] OWASP. Authentication cheat sheet. https://web.archive.org/web/20240606045022/https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html. Accessed: July 10, 2024.

[134] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. Beyond Credential Stuffing: Password Similarity Models Using Neural Networks. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 417–434, May 2019.

[135] Vinay Pamnani. Minimum password age. `https://web.archive.org/web/20240428235601/https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/minimum-password-age`. Accessed: July 10, 2024.

[136] Vinay Pamnani. Password must meet complexity requirements. `https://web.archive.org/web/20240428235613/https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements`. Accessed: July 11, 2024.

[137] THE EUROPEAN PARLIAMENT and THE COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2015/ of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. *Official Journal of the European Union*, 2015.

[138] 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.

[139] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 295–310, New York, NY, USA, 2017. Association for Computing Machinery.

[140] Dieter Petereit. BSI rät jetzt von regelmäßigem Passwort-Wechsel ab. `https://web.archive.org/web/20240227142627/https://t3n.de/news/bsi-raet-regelmaessigem-ab-1249147/`, 2020. Accessed: July 10, 2024.

[141] 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.

[142] Sören Preibusch and Joseph Bonneau. The Password Game: Negative Externalities from Weak Password Practices. In *International Conference on Decision and Game Theory for Security*, pages 192–207. Springer, 11 2010.

[143] Have I Been Pwned. API v3. https://web.archive.org/web/20240711120010/https://haveibeenpwned.com/API/v3, No year given. Accessed: July 10, 2024.

[144] Have I Been Pwned. Pwned websites. https://web.archive.org/web/20240711120152/https://haveibeenpwned.com/, No year given. Accessed: July 11, 2024.

[145] 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.

[146] Ariel Rabkin. Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, SOUPS '08, page 13–23, New York, NY, USA, 2008. Association for Computing Machinery.

[147] 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.

[148] 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.

[149] Sena Sahin, Suood Al Roomi, Tara Poteat, and Frank Li. Investigating the Password Policy Practices of Website Administrators. In *2023 2023 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1437–1454, 2023.

[150] 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*, pages 375–390. IEEE Computer Society, May 2009.

[151] Stuart Schechter, Serge Egelman, and Robert W. Reeder. It's Not What You Know, But Who You Know: A social approach to last-resort authentication. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, page 1983–1992, New York, NY, USA, 2009. Association for Computing Machinery.

[152] Jürgen Schmidt. Nur fünf Zeichen fürs Banking-Passwort? https://web.archive.org/web/20240711120517/https://www.heise.de/ratgeber/Nur-fuenf-Zeichen-fuers-Banking-Passwort-4935773.html. Accessed: July 11, 2024.

[153] Jürgen Schmidt. Passwörter: BSI verabschiedet sich vom präventiven, regelmäßigen Passwort-Wechsel. https://web.archive.org/web/20240711120645/https://www.heise.de/news/Passwoerter-BSI-verabschiedet-sich-vom-praeventiven-Passwort-Wechsel-4652481.html, 2020. Accessed: July 11, 2024.

[154] Seth Schoen. Let's Encrypt Brings Free HTTPS to the World: 2015 in Review. https://web.archive.org/web/20240711120859/https://www.eff.org/de/deeplinks/2015/12/lets-encrypt-project-comes-fruition-2015-review, 2015. Accessed: July 11, 2024.

[155] Tobias Seitz, Manuel Hartmann, Jakob Pfab, and Samuel Souque. Do Differences in Password Policies Prevent Password Reuse? In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI '17, pages 2056–2063, 05 2017.

[156] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. Can Long Passwords Be Secure and Usable? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2927–2936, New York, NY, USA, 2014. Association for Computing Machinery.

[157] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip S. Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing Password Policies for Strength and Usability. *ACM Transactions on Information and System Security (TISSEC)*, 18(4):13, May 2016.

[158] Richard Shay, Saranga Komanduri, Patrick G. Kelley, Pedro G. Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*, pages 1–20, New York, NY, USA, 2010. Association for Computing Machinery.

[159] Sigstore. Sigstore. https://web.archive.org/web/20240711121002/https://www.sigstore.dev/, No year given. Accessed: July 11, 2024.

[160] Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen K Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger. MD5 Considered Harmful Today: Creating a rogue CA certificate. In *25th Annual Chaos Communication Congress*, number CONF, 2008.

[161] Statista. Most convenient Multi-Factor Authentication (MFA) methods worldwide in 2021. https://web.archive.org/web/20240711121117/https://www.statista.com/statistics/1303617/convenient-global-mfa-methods/, 2021. Accessed: July 11, 2024.

[162] Vlasta Stavova, Vashek Matyas, and Mike Just. Codes v. People: A Comparative Usability Study of Two Password Recovery Mechanisms. In Sara Foresti and Javier Lopez, editors, *Information Security Theory and Practice*, volume 9895, pages 35–50. Springer International Publishing, 2016.

[163] Jeremiah D. Still and Lauren N. Tiller. Exploring Understanding and Usage of Two-Factor Authentication Account Recovery. In Matteo Zallio, Carlos Raymundo Ibañez, and Jesus Hechavarria Hernandez, editors, *Advances in Human*

*Factors in Robots, Unmanned Systems and Cybersecurity*, pages 223–231, Cham, 2021. Springer International Publishing.

[164] Elizabeth Stobert and Robert Biddle. The Password Life Cycle: User Behaviour in Managing Passwords. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 243–255, Menlo Park, CA, July 2014. USENIX Association.

[165] Nick Summers. Do you really need to change your password every 90 days? `https://web.archive.org/web/20240717113015/https://blog.1password.com/should-you-change-passwords-every-90-days/`, 2022. Accessed: July 17, 2024.

[166] Joshua Tan, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-Strength, Minimum-Length, and Blocklist Requirements. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, page 1407–1426, New York, NY, USA, 2020. Association for Computing Machinery.

[167] Christian Tiefenau, Maximilian Häring, Katharina Krombholz, and Emanuel von Zezschwitz. Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 239–258. USENIX Association, August 2020.

[168] Christian Tiefenau, Emanuel von Zezschwitz, Maximilian Häring, Katharina Krombholz, and Matthew Smith. A Usability Evaluation of Let's Encrypt and Certbot: Usable Security Done Right. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 1971–1988, New York, NY, USA, 2019. Association for Computing Machinery.

[169] Tranco. Information on the Tranco list with ID X5KYN. `https://web.archive.org/web/20240717113142/https://tranco-list.eu/list/X5KYN/1000000`, 2022. Accessed: July 17, 2024.

[170] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. "I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security (SOUPS) 2015*, pages 123–140, Ottawa, July 2015. USENIX Association.

[171] Kamile Viezelyte. Juggling security: How many passwords does the average person have in 2024? `https://web.archive.org/web/20240717113250/https://nordpass.com/blog/how-many-passwords-does-average-person-have/`. Accessed: July 17, 2024.

[172] W3C. W3C TAG: Securing the Web. `https://web.archive.org/web/20240717113352/https://www.w3.org/2001/tag/doc/web-https`, 2015. Accessed: July 17, 2024.

[173] W3Techs. W3techs: Historical yearly trends in the usage statistics of site elements for websites. https://w3techs.com/technologies/history_overview/site_element/all/y, 2022. Accessed: May 26, 2023.

[174] Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, CODASPY '18, page 196–203, New York, NY, USA, 2018. Association for Computing Machinery.

[175] Ding Wang and Ping Wang. The Emperor's New Password Creation Policies. In *European Symposium on Research in Computer Security*, pages 456–477. Springer, 11 2015.

[176] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 175–188, Denver, CO, June 2016. USENIX Association.

[177] 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.

[178] WhatsApp. About two-step verification - WhatsApp Help Center. https://web.archive.org/web/20240717113912/https://faq.whatsapp.com/1278661612895630. Accessed: July 17, 2024.

[179] Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 176–186, New York, NY, USA, 2010. Association for Computing Machinery.

[180] Verena Zimmermann and Nina Gerber. "If It Wasn't Secure, They Would Not Use It in the Movies" – Security Perceptions and User Acceptance of Authentication Technologies. In Theo Tryfonas, editor, *Human Aspects of Information Security, Privacy and Trust*, Lecture Notes in Computer Science, pages 265–283. Springer International Publishing, 2017.

# Appendix A

# Password Composition Policies in German Companies

This appendix gives additional information for the work presented in Chapter 3, Chapter 4 and Chapter 5.

## A.1 Survey

The survey was adapted to new situations over the years. To indicate that a question was included in a year, we will use the following taxonomy:

- †, if a question was part of the original questionnaire (Chapter 4) in **2019**.
- ⋆, if the questions was included in `PCP20`.
- ⋄ for questions included in `PCP22`.
- $\bigtriangledown$ for questions included in `PCP23`.

If no year is specified, the question was asked in all versions of the survey.

### Accounts

- Q1 Is there a company-wide account per user, that is managed centrally? (e.g., for logging into the workstation, communication platform, email or the like.)
  *Yes / No*
- $Q2^{\bigtriangledown}$ Which user management do you use? (e.g. Microsoft Active Directory)
  *[Free Text]*

If Q1 equals yes:

- Q3a What can this account be used for? (Multiple answers possible.)
  *Email / Workstations / Communication platform (SharePoint, Slack, etc.) / VPN into corporate network / Access to shared corporate data (e.g., Active Directory) / Other: [Free text]*

`< Page break >`

- Q3b Which methods can be used to log in? Please check the applicable.
  *Password or PIN / Biometrics (e.g., Fingerprint, Face recognition) / Hardware Token (e.g. Smartcard, Token, Smartphone) / Device Certificates*$^{\diamond}$
- Q3c Is there any other method in use that is not listed?
  *Yes, the following: [Free text] / No*

If more than one method is listed in Q3b:

- Q4a You stated, that there are several methods in use that enable your employees to log in. Are the methods used in combination (e.g., 2FA)?
  *Yes, the methods are used in combination (2FA) / No, the employees can choose one of the methods / Other: [Free text]/ I do not know / I do not wish to make a statement*

If only one method is listed in Q3b:

- *Q4b*$^{\triangledown}$ Do you make use of any kind of two-factor authentication?
  *Yes, using the following techniques: [Free Text] / No / I do not know / I do not wish to make a statement*

`< Page break >`

### Passwords

You stated that there is no company-wide account with which the employees can log into several services.
The following questions regard the email accounts of your employees and their passwords (Webmail, IMAP, POP3, etc.).
*Or*
You stated, that your employees use passwords/PINs to log in. The following questions regard these passwords/PINs.

- *Q5*$^{\dagger\star\diamond}$ How are passwords handled?
  *Users can choose them themselves / Passwords are created by a system, and users* ***cannot change*** *them / Passwords are created by a system and* ***need to be changed*** *by the user*$^{\star\diamond}$*/ I don't want to make a statement / Other: [Free text]*

- Q6 What specification (also called password policy) do passwords need to fulfill (e.g., at least x characters, new password needs to be selected after x days, etc.)

  This question is the main focus of our research. Please be as detailed as possible. If possible and allowed, please copy your specification into the following text box. At this point, we want to remind you, that the data is managed anonymously. It will not be possible to identify your company.
  *[Free text]*

- Q7 Are these specifications enforced by the system?
  *Yes / No / There are no specifications / I do not know / I do not wish to make a statement / Partially: [Free text]*

- $Q8^{\diamond}$ In case there is a password expiry in use: Why?
  *[Free text]*

- Q9 Optional: What reasons spoke against the introduction of a password policy?
  *[Free text]*

`< Page break >`

- $Q10^{\triangledown}$ Do you feel it is best practice to require employees to change their passwords on a regular basis (e.g., once a year)?
  *Yes / No / Other: [Free Text]*

`< Page break >`
In previous studies, we have seen that employees in many companies in Germany have to change their passwords on a regular basis. In the following, we would like to learn more about the possible reasons that speak in your eyes for or against using such a time-controlled change of passwords.

- $Q11^{\triangledown}$ Are employees technically forced to change their password?
  *Yes, after a fixed time interval (days/months/years): [Free Text] / Yes, if there is a suspicion that the password has become known / No, never / Other: [Free Text]*

- $Q12^{\triangledown}$ If employees need to change their password regularly (after a fixed time interval): Why?
  *[Free Text]*

- $Q13^{\triangledown}$ In case employees had to change their password regularly (after a fixed time interval) in the past, but this rule has now been abolished: Why was this changed?
  *[Free Text]*

`< Page break >`

- $Q14^{\triangledown}$ Since 2020, the BSI has recommended relying on password compromise detection instead of recurring password change prompts (after a fixed time interval). If you do this: How do you check if passwords are compromised?

If not: are there reasons that prevent you from doing so? (e.g., technical, structural, or timing reasons).
*[Free Text]*

`< Page break >`

- Q15 Are users prevented from picking passwords that belong to the most common passwords?
  *No / Other: [Free text] / I do not know / I do not wish to make a statement / Yes*$^{\dagger}$ */ Yes, examination through*$^{\star\diamond}$*: [Free text])*
- *Q*16$^{\star\diamond\triangledown}$ Do you make use of a Blocklist/Denylist of elements that are not allowed to be used in a password? (e.g. words from the dictionary or sequences of numbers) *Yes, the following elements cannot be used in passwords: [Free text] / No / There are no specifications / I do not know / I do not wish to make a statement*
- *Q*17$^{\star\diamond}$ Which Unicode characters can be used in passwords? *All / a-z / A-Z / 0-9 / All special characters / Special characters, except: [Free text] / Chinese characters / Arabic characters / Emojis / Other: [Free text] / I don't know / I do not want to make a statement*
- *Q*18$^{\star\diamond\triangledown}$ Are there additional password policies for different users? (e.g. System administrators) *Yes / No / I do not know / I do not wish to make a statement*
- *Q*19$^{\star\diamond\triangledown}$ Optional: How do the different password policies differ? *[Free text]*

`< Page break >`
The following questions still regard the passwords which are used in your company.

- Q20 Who created the specifications (password policies) for the passwords?
  *Myself / My predecessor / Somebody else: [Free text]/ I do not know / I do not wish to make a statement / There are no specifications*
- Q21 What are the specifications based on? (Multiple answers possible.)
  *Targeted Training*$^{\star\diamond\triangledown}$ */ Own Know−how*$^{\star\diamond\triangledown}$ */ Standards defined by own company*$^{\star\diamond\triangledown}$ */ Industrial Standards*$^{\star\diamond\triangledown}$ */ Expert panels / Exchange with other companies / NIST (National Institute of Standards and Technology) / BSI (Bundesamt für Sicherheit in der Informationstechnik) / OWASP (Open Web Application Security Project) / Other: [Free text] / I do not know / I do not wish to make a statement*
- *Q*22$^{\star\diamond\triangledown}$ When were the password policies changed last? *[Free text]*
- *Q*23$^{\star\diamond}$ What changes were made during the last modification? *[Free text]*
- *Q*24$^{\triangledown}$ Which changes were made?
  *[Free Text]*
- *Q*25$^{\star\diamond\triangledown}$ What caused the change? *[Free text]*

- Q26 How do the password policies impact the user-friendliness of the authentication system?
  *1: Very negative – 5: Very positive*
- Q27 How do the password policies impact the security of the authentication system?
  *1: Very negative – 5: Very positive*
- Q28 How often do passwords cause problems in your company (e.g., forgotten passwords, etc.)?
  *1: Very rarely – 5: Very often*

`< Page break >`

- $Q29^{\star\diamond}$ This year, the BSI published new recommendations for password policies. Have you already dealt with them? *Yes / No / I do not know / I do not wish to make a statement*
- $Q30^{\star\diamond}$ Was your password policy adapted due to the new recommendations or are you planning a change? *Yes / No / I do not know / I do not wish to make a statement*

`< Page break >`

- Q31 Is there a policy that specifies how the passwords are stored in the system (hash function, length of the salt, etc)?
  *Yes / No / I do not know / I do not wish to make a statement*
- Q32 Is there a process that initiates an update of the policy on how to store passwords?
  *Yes / No / I do not know / I do not wish to make a statement*
- Q33 Optional: How are stored passwords protected? We are particularly interested in the hash and salt functions that are used.

  We want to remind you that the data is gathered anonymously and we are not able to link it to your company.
  *[Free text]*

`< Page break >`

### Biometric Authentication

You stated, that your employees use biometrics to log in. The following questions regard this method.

- Q34 What kind of biometrics are in use?
  *Fingerprint / Iris / Face recognition / Other: [Free text]/ I do not wish to make a statement*

- Q35 How does the biometric authentication impact the user-friendliness of the authentication system?
  *1: Very negative – 5: Very positive*
- Q36 How does the biometric authentication impact the security of the authentication system?
  *1: Very negative – 5: Very positive*
- Q37 How often does the use of biometric authentication cause problems?
  *1: Very rarely – 5: Very often*
- Q38 Optional: Do you wish to provide us with additional information about this topic?
  *[Free text]*

`< Page break >`

### Hardware Token

You stated, that your employees use a hardware token to authenticate. The following questions regard this token.

- Q39 Does the token support FIDO2?
  *Yes / No / I am not sure / I do not wish to make a statement*
- Q40 How does the token impact the user-friendliness of the authentication system?
  *1: Very negative – 5: Very positive*
- Q41 How does the token impact the security of the authentication system?
  *1: Very negative – 5: Very positive*
- Q42 How often does the usage of the token cause problems?
  *1: Very rarely – 5: Very often*
- Q43 Optional: Do you wish to provide us with additional information about this topic?
  *[Free text]*

`< Page break >`

### Passwordless

- $Q44^{\triangledown}$ There are efforts (e.g., by the Fido Alliance) to completely abolish passwords. What is your opinion of these efforts (also with regard to their feasibility in the company where you work)?
  *[Free Text]*

`< Page break >`

### Demographics

- $Q45^{\dagger\star\diamond}$ Please check the conditions which apply to your company. (Multiple answers possible.)
  *There are employees who can access their emails outside the company network /*
  *There are employees who can access their emails using a web login /*
  *There are employees who do not need to know the password for accessing their emails, e.g., as the email-client is pre-configured*

- Q46 Is there any additional security for emails? (e.g., encryption in combination with a smart card)
  *Yes, obligatory / Yes, voluntary / No / I do not wish to make a statement*

- $Q47^{\star\diamond\triangledown}$ What is your companies' field of work? *Automobile Industry / Banks and financial services / Education and research / Services / Retail / Energy industry / Logistics / Telecommunication / Pharmaceutical industry / Tourism / Insurance / Healthcare Marketplace / Other: [Free text] / I do not wish to make a statement*

- $Q48^{\star\diamond\triangledown}$ Is your company an operator of critical infrastructure or is it affected by regulations for operators of critical infrastructure? *Yes / No / I do not know / I do not wish to make a statement*

- $Q49^{\triangledown}$ Is your company certified with a certification relevant to IT security (e.g., PCI-DSS, ISO 27001,..)?
  *Yes, the following: [Free Text] / No, but we intend to / No / Other: [Free Text] / I don't know / I do not wish to make a statement*

- $Q50^{\triangledown}$ Are there any legal regulations that require you to have any of the previous certifications?
  *Yes the following: [Free Text] / No / Other: [Free Text] / I do not wish to make a statement*

- $Q51^{\star\diamond\triangledown}$ Where is your companies' headquarter? (Country) *[Free text]*

- Q52 How many employees work in your company?
  *1-9 / 10-49 / 50-249 / 250-499 / 500-999 / 1000 or more / Not sure / I do not wish to make a statement*

- Q53 How many desktop clients do you manage?
  *1-9 / 10-49 / 50-249 / 250-499 / 500-999 / 1000 or more / Not sure / I do not wish to make a statement*

- Q54 How many employees in your company work full-time on IT security topics?
  *0 / 1 / 2-5 / 6-10 / 11-20 / 21 or more / Not sure / I do not wish to make a statement*

- $Q55^{\star\diamond\triangledown}$ What is your position? *Administrator / ISO / CISO / CTO / CSO / Support / Other: [Free text] / I do not wish to make a statement*

- $Q56^{\star\diamond\triangledown}$ How many years of experience do you have in this or related positions? *Under 1 year / 1-3 Years / 4-9 Years / 10 or more years / I do not wish to make a statement*

- $Q57^{\star\diamond\triangledown}$ Is one (or more) of the following situations true for your company when looking at the last 5 years? (MC) *A password of an employee was guessed and used to attack the company (Ransomware, theft,..) / Several passwords have been stolen from the database / None of the above / I do not know / I do not wish to make a statement / Further / Other: [Free text]*

`< Page break >`

- $Q58^{\star\diamond\triangledown}$ Have you already participated in this survey last year?
  *Yes / No / I do not know /I do not wish to make a statement*
- Q59 How satisfied are you with your authentication system?
  *1: ☹ – 5: ☺*
- Q60 Has this questionnaire motivated you to update parts of your authentication system in the near future? If yes, which parts?
  *Password Policies / Security measures for stored passwords / Adding biometrics / Adding hardware token / No / Other: [Free text]*

## A.2 Additional Figures and Tables - 2019

| **Company Size** | **No. of Participants per No. of Managed Clients** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **0-9** | **10-49** | **50-249** | **250-499** | **500-999** | **>= 1000** | **n.a.** |
| 1-9 | 6 | 1 | | | | | |
| 10-49 | 2 | 9 | | | | | 1 |
| 50-249 | | | 11 | 1 | | | 1 |
| 250-499 | | | 1 | 7 | | | 1 |
| 500-999 | | | | | 6 | 1 | |
| >= 1000 | 2 | | | | 5 | 23 | 3 |
| No answer | | | | | | | |

**Table A.1** – Number of participants who manage a certain number of clients, split by company size. Empty fields indicate 0. n.a. = No answer was given by the participant.

| | Element | Account Policies n= 64 | Mail Policies n= 13 | Additional Policies n = 4 |
|---|---|---|---|---|
| **Minimal Length** | 6 | 3 | 2 | - |
| | 8 | 33 | 4 | - |
| | 9 | 1 | - | - |
| | 10 | 11 | 2 | - |
| | 12 | 9 | 1 | - |
| | 14 | 2 | 1 | - |
| | 15 | 1 | - | - |
| | 16 | - | - | 3 (Admin) |
| | 20 | - | 1 | 1 (Passphrases) |
| | 30 | - | 1 | - |
| | Unspecific | 1 | - | - |
| | N.A. | 3 | 1 | - |
| | **Any minimal length** | 61 | 12 | 4 |
| **Maximal Age (Days)** | 30 | 2 | - | - |
| | 42 | - | 1 | - |
| | 45 | - | - | 1 (Admin) |
| | 56 | 1 | - | - |
| | 60 | 3 | - | - |
| | 90 | 22 | 4 | - |
| | 120 | 1 | - | - |
| | 180 | 9 | 2 | - |
| | 360 | 1 | - | - |
| | 365 | 6 | 1 | - |
| | Explicitly not | 2 | - | - |
| | N.A. | 17 | 5 | 3 |
| | **Any maximal age** | 45 | 8 | 1 |
| **Character Classes (>= 1 each)** | S | 1 | - | - |
| | 2 (L, D) | - | 1 | - |
| | 2 (D, S) | 2 | - | - |
| | 3 (C, D, S) | 3 | - | - |
| | 3 (C, Lc, S) | 3 | - | - |
| | 3 (C, Lc, D) | 7 | 1 | 1 (Admin) |
| | 3 (L, D, S) | 2 | - | - |
| | Any 3 out of 4 | 16 | 2 | - |
| | Any 3 out of 5 (incl. Unicode) | 1 | - | - |
| | 4 (C, Lc, D, S) | 15 | 3 | 1 (Admin) |
| | 4 (at least 2 each) | 1 | 1 | - |
| | 4 (C and Lc: at least 1; D+S: at least 2) | 1 | - | - |
| | Unspecific | 5 | 1 | 1 (Admin) |
| | N.A. | 7 | 4 | 1 |
| | **Any character requirement** | 57 | 9 | 3 |

**Table A.2** – Number of policies with the different elements of "minimal length", "maximal age" and "character classes". The four standard character classes are: Lowercase (Lc), Capital (C), Digit (D), and Special character (S). If letter was not further specified, this is abbreviated with L

## A.3 Additional Tables - 2020 to 2023

| | | Has PW Expiry | No PW Expiry | p | OR |
|---|---|---|---|---|---|
| H3: Critical Infrastructure | Yes | 5 | 3 | 1.0 | 0.83 |
| | No | 28 | 14 | | |
| H4: Company Size | <500 | 14 | 9 | 1.0 | 1.29 |
| | >=500 | 16 | 8 | | |
| H5: Last policy change | Before BSI changes | 9 | 1 | 0.3 | 0.14 |
| | After BSI changes | 19 | 15 | | |
| H6: Technical compromise check | Yes | 13 | 12 | 0.4 | 0.27 |
| | No | 20 | 5 | | |

**Table A.3** – Contingency table for H3-6: *Company characteristics or the use of certain policy elements influence whether the companies use a password expiry in 2023.* The results are corrected using a Bonferroni-Holm correction.

| | PCP19 | PCP20 | PCP22 | PCP23 |
|---|---|---|---|---|
| **Pw** | 100.0 | 100.0 | 100.0 | 97.5 |
| **Pw + Bio** | 14.8 | 17.3 | 25.4 | 25.0 |
| **Pw + Token** | 38.9 | 50.0 | 57.1 | 53.8 |
| **Pw + Bio + Token** | 11.1 | 13.5 | 19.0 | 17.5 |
| **Token (no Pw + Bio)** | 0 | 0 | 0 | 1.2 |

**Table A.4** – Percentage of participants who mentioned that their companies use the different possibilities to login. Pw = Passwords are in use; bio = Biometrics are in use; Token = Hardware token are in use

| | Code | PCP20 $n = 52$ | PCP22 $n = 63$ | PCP23 $n = 80$ | ICR |
|---|---|---|---|---|---|
| Character classes | 1 | 2 | 1 | 1 | - |
| | 2 | 2 | 3 | 1 | 0.79 |
| | 3 | 23 | 25 | 33 | 1 |
| | 4 | 16 | 19 | 15 | 1 |
| | Imprecise | 3 | 5 | 9 | 0.47 |
| | Special | 0 | 1 | 2 | - |
| | Total | 46 (88%) | 54 (86%) | 61 (76%) | |
| | Not mentioned | 4 | 6 | 10 | 0.79 |
| | Explicitly not | 0 | 0 | 1 | - |
| Minimum length | 5 | 1 | 0 | 0 | - |
| | 6 | 4 | 1 | 1 | - |
| | 7 | 0 | 0 | 1 | - |
| | 8 | 18 | 20 | 19 | 1 |
| | 9 | 1 | 1 | 2 | 1 |
| | 10 | 16 | 14 | 12 | 1 |
| | 11 | 0 | 2 | 1 | 1 |
| | 12 | 8 | 16 | 24 | 1 |
| | 14 | 0 | 2 | 5 | 1 |
| | 15 | 0 | 1 | 4 | - |
| | 16 | 1 | 0 | 2 | - |
| | 64 | 1 | 0 | 0 | - |
| | Imprecise | 0 | 2 | 1 | - |
| | Total | 50 (96%) | 59 (94%) | 72 (90%) | |
| | Not mentioned | 0 | 1 | 0 | - |
| Password expiry (days) | 14 | 0 | 1 | 0 | - |
| | 30 | 1 | 0 | 2 | - |
| | 42 | 1 | 1 | 0 | 1 |
| | 60 | 0 | 0 | 1 | - |
| | 64 | 0 | 0 | 1 | - |
| | 90 | 12 | 8 | 5 | 1 |
| | 120 | 0 | 0 | 1 | - |
| | 168 | 0 | 1 | 0 | - |
| | 180 | 6 | 2 | 9 | 1 |
| | 230 | 0 | 1 | 0 | - |
| | 360 | 0 | 0 | 1 | - |
| | 365 | 5 | 6 | 6 | 1 |
| | 540 | 1 | 0 | 0 | - |
| | 720 | 0 | 0 | 1 | - |
| | Imprecise | 1 | 2 | 1 | - |
| | Total | 27 (52%) | 22 (35%) | 28 (35%) | |
| | Not mentioned | 18 | 25 | 26 | 1 |
| | Explicitly not | 5 | 13 | 18 | 1 |
| | No policy given | 2 | 3 | 8 | - |

**Table A.5** – Codebook of participants' elements of password composition policies (Q6) and how often they occurred. For calculating the ICR, answers from both years were merged. Some codes were not covered in the documents that were used to calculate the inter-coder reliability and indicated as "-" in the table.

| Code | Example | Occurrence in PCP23 |
|---|---|---|
| Demanded by ... | | |
| ... Institutions | "PCI DSS (Credit card security) requirement" | 5 |
| ... Customer (contracts) | "was embedded in customer contracts in the past" | 3 |
| ... Own company | "In-house or internal definition" | 4 |
| Is best practice | "Recommendation by BSI" | 2 |
| To increase security | "Improve password security", "Ensure that there are no passwords that are too old and no insecure hash algorithms are used." | 17 |
| Currently changing | "We still have the setting but are in discussion rather to increase the complexity, but not to force a change (except in case of loss). Still need to convince the auditor. " | 1 |
| Alternative not implemented | "Because there is currently no other technical solution." | 4 |
| Inertia | "Still exists from history" | 5 |

**Table A.6** – Codebook of the reason for using password expiry (Q12)

| Code | Example | Occurrence in PCP23 |
|---|---|---|
| Employee check | "Our detection of compromise has so far been the sole responsibility of the employee." | 6 |
| Check: Dark web monitoring | "Dark Web Monitoring" | 4 |
| Check: Compare to leak database | "On the relevant websites we check whether passwords have been compromised" | 8 |
| Check: Anomaly detection | "Detection of compromise by technical means (e.g., logon location)." | 16 |
| No check: Lack of.. | | |
| ..technical measures | "Technically not yet possible, corresponding recognition systems are still missing" | 9 |
| ...and unclear how | "We do not know any practicable method" | 3 |
| ...organizational measures | "organizational feasibility" | 5 |
| ...resources (time, money) | "There would also be a lack of time and staff resources to look into this" | 7 |

**Table A.7** – Codebook of the reason for using password expiry (Q14)

# Appendix B

# 2FA Account Recovery of Popular Websites

This appendix gives additional information for the work presented in Chapter 6.

## B.1 Website Analysis

### B.1.1 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. trend-micro.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 | ○ | ○ | ○ | - | ○ | ○ |
| 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 | ● |

| Service | Second Factor | Setup | | | | Recovery | |
|---|---|---|---|---|---|---|---|
| | | Hint | Backup | Force | Shown in... | Link to Support | Suggests Using Backup |
| 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 B.1** – 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.

# Appendix C

# Users' Expectations Towards 2FA Recovery

This appendix gives additional information for the work presented in Chapter 7.

## C.1 Interview Guideline

The interview was semi-structured, based on the following guideline. For actual circumstances (current 2FA, experiences, and current backups), we kept asking until we felt that participants shared everything they could recall. The structure was not fixed. For example, if a participant brought up a topic before its appearance on our list, we talked about that, if possible.

**Demographics**

- Q1: What is your age?
- Q2: What is your current profession?
- Q3: What is the highest level of education?
- Q4: How did you become aware of the study?
- Q5.1: Would you consider yourself tech-savvy?
- Q5.2: If yes, do you have (professional) experience in the area of / are you interested in cyber security?
- Q6: What end devices do you own or use? (special focus on smartphone, laptop/pc, tablet)

**Explanation of 2FA**

- It was explained that 2FA is used in addition to the username and password. The example of online banking was given, with the user receiving a code or notification that must be confirmed. The participant was asked if they had any questions.
- Q7 Do you use 2FA?
- Q7.1 If yes, where?
- Q7.2 What is the second factor?
- Q7.3 What do you have to do to log in?
- Q7.4 Why did you enable 2FA? Was it proposed to you, or did you actively look for it?

**Previous Experience**

- Q8 Did you ever lose your second factor?
- Q8.1 Please tell me about it.
- Q8.2 Can you remember what you had to do to regain access?
- Q8.3 Were any of these experiences without the use of customer service or for accounts without the knowledge of your personal information (for example, Instagram with only an account name instead of your full name)?
- Q9 If no: What process do you expect if you lose access to the second factor?
- Q10 If the answer included personal information: Does every account for which you use 2FA also store some personal information about you?
- Q11 Would you have any idea what to do / how to regain access if you did not have any contact and/or personal information?

**Scenario Presentation**

- The participant is shown two example scenarios from two different websites: a) duration roughly 40 seconds, where a user is caught in an infinite loop while trying to get assistance, b) no login is possible. For each video:
- Q12 What impression do you get from watching these videos?
- Q13 What do you think went wrong?
- Q14 Do you have suggestions for improvements?
- Q15 What would you do in such a situation if you were trying to recover your account?

**Backup possibilites**

- We explained the concept of different backup possibilities: Secondary Phone/email (own or from a trusted person), backup codes, delegated account recovery via an app and an identification document
- Q16 What are your thoughts on these?
- Q16.1 Which do you find best for recovery? Why?
- Q16.2 Do you use one of these for your accounts?
- Q17 Do you have any other ideas or preferences on how you would want to regain access?

**Responsibility**

- Q18 Who do you think is responsible for ensuring access to the account? Do you think it should be similar to a forgotten password, where you can reset the password, and the provider sends you (most often) an email? Or do you think that should be different for the second factor, and you should take care of possible backups yourself?
- Q19 Would you feel responsible? How?
- Q20 Do you believe the website operators should communicate possible issues better?

**Debriefing** We asked whether the participant had any questions. We mentioned that many websites help a user but that it might make sense to check recovery methods regularly and check for device dependencies.

## C.2 Survey

If answers did not have a natural order, they were presented randomly.

**Query 2FA**

- Q1: Do you use 2-factor authentication for an online service? [Choose one.]
  *-Yes*
  *-No*
  *-I don't know*
  *-I prefer not to answer.*

**Details 2FA**

- Q2: Where do you use 2-factor authentication? [Multiple responses possible.]
  *-Social-Media (Instagram, Facebook,...)*
  *-Financial Services (PayPal, ApplePay,...)*
  *-Online-Banking*
  *-Online-Shopping*
  *-Device Accounts (AppleID, Google account, Microsoft,...)*
  *-Messenger Services (Email, Discord,...*
  *-Other (Please fill out)*

- Q2.1: You have indicated that you are using 2FA for **a financial service (e.g. PayPal, ApplePay,...)**. Please state the **main reason** why you use 2FA there. [Choose one.]
  *-Was already preset / was mandatory*
  *-Recommendation from family/friends*
  *-I've had bad experiences without 2-factor authentication (data theft, etc.)*
  *-Website suggestion*
  *-I hope this will give me more security*
  *-Other (Please fill out)*
  *-I prefer not to answer.*

- Q2.2: You have indicated that you are using 2FA at an **online shop**. Please state the **main reason** why you use 2FA there. [Choose one.]
  *-Was already preset / was mandatory*
  *-Recommendation from family/friends*
  *-I've had bad experiences without 2-factor authentication (data theft, etc.)*
  *-Website suggestion*
  *-I hope this will give me more security*
  *-Other (Please fill out)*
  *-I prefer not to answer.*

- Q2.3: You have indicated that you are using 2FA for a **Social media service (e.g. Instagram, Facebook,...)**. Please state the **main reason** why you use 2FA there. [Choose one.]
  *-Was already preset / was mandatory*
  *-Recommendation from family/friends*
  *-I've had bad experiences without 2-factor authentication (data theft, etc.)*
  *-Website suggestion*
  *-I hope this will give me more security*
  *-Other (Please fill out)*
  *-I prefer not to answer.*

- Q2.4: You have indicated that you are using 2FA for a **Messenger Service (Email, Discord,...)**. Please state the **main reason** why you use 2FA there. [Choose one.]
  *-Was already preset / was mandatory*
  *-Recommendation from family/friends*

*-I've had bad experiences without 2-factor authentication (data theft, etc.)*
*-Website suggestion*
*-I hope this will give me more security*
*-Other (Please fill out)*
*-I prefer not to answer.*

- Q2.5: You have indicated that you are using 2FA for a **Device Account (AppleID, Google account, Microsoft,...)**. Please state the **main reason** why you use 2FA there. [Choose one.]
*-Was already preset / was mandatory*
*-Recommendation from family/friends*
*-I've had bad experiences without 2-factor authentication (data theft, etc.)*
*-Website suggestion*
*-I hope this will give me more security*
*-Other (Please fill out)*
*-I prefer not to answer.*

- Q3: What second factor do you use with the prior mentioned websites or services? [Multiple answers possible, please select all methods that you use for at least one account]
*-SMS-Codes*
*-Email*
*-Authenticator-Apps*
*-Physical factor (key, card, USB stick,...)*
*-One-Time-Password*
*-Other (Please fill out)*
*-I prefer not to answer.*

- Q4: Have you ever thought about losing your second factor? [Choose one.]
*-Yes, and I did nothing*
*-Yes, and I looked for a solution.*
*-No.*
*-I prefer not to answer.*

- Q5: Have you ever experienced the loss of a second factor? Please describe briefly how and whether you could regain access to your secured accounts: [Text answer]

**2FA Knowledge**

- Q6: Imagine you lose your second factor (e.g., the cell phone you use to receive a code) and therefore **no longer have access to your account**. Please choose how much the following statements apply to you: [*-I disagree, I partially disagree, Neither, I partially agree, I agree, No answer*]

- Q6.1: I have an alternative method to access my account (backup, another registered device, etc.)
- Q6.2: I can later add a second factor if I have lost my current one.
- Q6.3: I expect that when I try to log in with the second factor, there will be a help button (similar to the one when you forget your password) that will give me access again.
- Q6.4: I am sure that the website will give me a way to regain access to my account.
- Q6.5: If I provide the website with personal information about myself, I will regain access to my account.
- Q6.6: I expect that there is a way to get in touch with customer support.

- Q7: The following statements refer to **2-factor authentication in general**. Please select how much you agree with each statement: [*-I disagree, I partially disagree, Neither, I partially agree, I agree, No answer*]
- Q7.1: To help us monitor the quality of our data, please select "I partially agree."
- Q7.2: If I use the fingerprint scanner/face recognition instead of a password, that counts as a second factor.
- Q7.3: If I lose my second factor, I can regain access to my account by resetting my password.
- Q7.4: I can also use the email I use for my account as a second factor.
- Q7.5: The second factor can be reset via my email.
- Q7.6: If, during the account creation, it was verified that I had access to my email address, that is a second factor (email verification).
- Q7.7: Security questions are a second factor.
- Q7.8: If I get an email about the activity when I log in, that's a second factor.
- Q7.9: The Captcha query is a second factor.
- Q7.10: If I use 2-factor authentication on an account, it is better protected against attacks.
- Q7.11: The second factor should be independent of my password.

**Personal Data**

- Most websites offer additional options that can be set up as an alternative method to the current second factor. Please select which alternative would be best for you. With this chosen method you could still log in if you don't have access to your actual second factor.
  **Alternative phone number:** A phone number of friends or family to whom the code could be sent.
  **Alternative email address:** An email address that is not yet linked to the account used. This could be your own email or, again, belong to friends or family.
  **Backup codes/one-time passwords:** These codes often consist of a string of characters and can be saved after setting up two-factor authentication. If you don't have access to your account, you can use this instead enter the code. Each code is valid once.

- Q8: Please select your **preferred** method: [Choose one.] *-Alternative phone number*
  *-Alternative email address*
  *-Backup codes/one-time passwords*
  *-I prefer not to answer.*

- Q9: Imagine losing your cell phone. How many accounts do you still have an alternative way to access? (You still have the app on another device, backup codes on another device, etc.) [Choose one.]
  *-None*
  *-Less than half*
  *-More than half*
  *-All of them*
  *-I'm not sure.*

- Q10: Which situation is worse for you? You permanently lose access to one of your accounts or a stranger gets access to the account. [Choose one.]
  *-Losing access is significantly worse.*
  *-Losing access is somewhat worse.*
  *-Both are equally bad.*
  *-Someone else gaining access is somewhat worse.*
  *-Someone else gaining access is significantly worse.*
  *-I prefer not to answer.*

**Responsibility**

- Q11: Currently, you are often responsible for your second factor, which means that **if you lose the second factor and have not set up an alternative method, you will no longer have access to your account.** Please select below how much

you agree with the following statements regarding this fact: [*-I disagree, I partially disagree, Neither, I partially agree, I agree, No answer*]

- Q11.1: I find it more secure.
- Q11.2: I can't understand it, the website is supposed to help me.
- Q11.3: I feel responsible for my second factor.

- Q12: Some websites offer you to upload your ID so that the personal data stored on the website can be compared. Would that be an option for you? [Choose one.]
  *-Yes, on some websites where I use two-factor authentication.*
  *-Yes, on all websites where I use two-factor authentication.*
  *-No, I wouldn't do that on any website.*
  *-I prefer not to answer.*
- Q12.1: You have selected that you would only be willing to upload your ID to some websites. Please briefly explain **which websites** you would not upload your ID to **and why**: [Text answer.]

- Q13: On how many websites where you have set up 2-factor authentication have you stored personal data? (Full name, date of birth, address, bank details, etc.) [Choose one.]
  *-None*
  *-Less than half*
  *-More than half*
  *-All of them*
  *-I'm not sure.*

- Q14: Some websites require you to provide one or more pieces of information about yourself or your account in order to regain access to your account after losing the second factor. Please indicate if you can answer the following information **for your accounts. If you don't know what this is**, please select "I don't know what this is." [*I can't answer for any account, I can answer for a few accounts, I can answer for half the accounts, I can answer for most accounts, I can answer for all accounts, I don't know what this is, I prefer not to answer.*]
- Q14.1: Complete (specified) address
- Q14.2: Own/specified first and last name
- Q14.3: (Specified) date of birth
- Q14.4: Username of the account
- Q14.5: List of items that were recently purchased (e.g., when shopping online)
- Q14.6: Date of the last successful login

- Q14.7: Mobile phone number associated with the account
- Q14.8: Email address with which I log in
- Q14.9: Cell phone serial number (without physical access to your cell phone)
- Q14.10: Device used for the last login, including operating system
- Q14.11: Security questions (if you have set them up, e.g., your mother's maiden name)
- Q14.12: Current IP address
- Q14.13: Invoice number from the last purchase (e.g., when shopping online)
- Q14.14: Payment information for the last purchase (e.g., last 4 digits of the Credit card or exact day of debit)
- Q14.15: Date the account was created

- Q15: Some websites require you to answer one or more questions to regain access to your account after losing the second factor. Please give an estimate of how easy it is **for another person to answer this question for you. If you don't know what this is**, please select "I don't know what this is." [*Strangers can acquire this information (e.g., over public social media profiles), Acquaintances can answer this about me, People close to me can answer this (Partner, Family, Best friends), No one else can answer this, I don't know what this is, I prefer not to answer*]
- Q15.1: Complete (specified) address
- Q15.2: Own/specified first and last name
- Q15.3: (Specified) date of birth
- Q15.4: Username of the account
- Q15.5: List of items that were recently purchased (e.g., when shopping online)
- Q15.6: Date of the last successful login
- Q15.7: Mobile phone number associated with the account
- Q15.8: Email address with which I log in
- Q15.9: Cell phone serial number (without physical access to your cell phone)
- Q15.10: Device used for the last login, including operating system
- Q15.11: Security questions (if you have set them up, e.g., your mother's maiden name)
- Q15.12: Current IP address
- Q15.13: Invoice number from the last purchase (e.g., when shopping online)

- Q15.14: Payment information for the last purchase (e.g., last 4 digits of the Credit card or exact day of debit)
- Q15.15: Date the account was created

- Q16: Is there a way you would like to regain access to your account? This means which data you would like to compare or which methods you would find best. [Choose one.]
  *-I would like the following options: Text answer*
  *-I prefer not to answer.*

- Q17: Before this survey, did you realize that many websites cannot help users if the second factor is lost? [Choose one.]
  *-Yes.*
  *-No.*
  *-I prefer not to answer.*

- Q18: Do you think it is sufficiently communicated that many websites have no way of helping users with the loss of the second factor? [Choose one.]
  *-Yes.*
  *-No.*
  *-I prefer not to answer.*

- Q19: Can you think of a way to feel responsible for your second factor? [Choose one.]
  *-Yes, I could imagine that.*
  *-No, I think the websites should take over that.*
  *-Only under certain circumstances.*
  *-I prefer not to answer.*
- Q19.1: You chose that you would only feel responsible under certain conditions. Please explain what the requirements would be: [Text answer.]

- Q20: Would you like a different type of communication regarding the handling of when the second factor is lost? [Multiple choices possible.]
  *-A large popup when setting up two-factor authentication.*
  *-Regularly reviewing my alternative login methods.*
  *-No.*
  *-Other. [Text answer.]*
  *-I prefer not to answer.*

**Demographics**

- Q21: Thank you for your answers so far. We would like to find out more about you in the following questions. How old are you? [Choose one.]
  *-Under 18*
  *-18-25*
  *-26-35*
  *-36-45*
  *-46-55*
  *-56-65*
  *-Over 65*
  *-I prefer not to answer.*

- Q22: What is your current main profession? [Choose one.]
  *-Student (School)*
  *-Student (University)*
  *-Employed*
  *-Retired*
  *-Other [Text answer.]*
  *-I prefer not to answer.*

- Q23: Would you describe yourself as interested in technology? [Choose one.]
  *-Yes.*
  *-No.*
  *-I prefer not to answer.*

- Q24: Which gender do you identify with? [Choose one.] *-Female*
  *-Male*
  *-Non-binary*
  *-Other [Text answer.]*
  *-I prefer not to answer.*