"Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication

KAROLA MARKY, University of Glasgow, Scotland, Technical University of Darmstadt, Germany, Keio University, Japan
KIRILL RAGOZIN and GEORGE CHERNYSHOV, Keio University, Japan
ANDRII MATVIIENKO, MARTIN SCHMITZ, and MAX MÜHLHÄUSER, Technical University of Darmstadt, Germany
CHLOE EGHTEBAS, Technical University of Munich, Germany
KAI KUNZE, Keio University, Japan

Two-factor authentication (2FA) is a recommended or imposed authentication mechanism for valuable online assets. However, 2FA mechanisms usually exhibit user experience issues that create user friction and even lead to poor acceptance, hampering the wider spread of 2FA. In this paper, we investigate user perceptions of 2FA through in-depth interviews with 42 participants, revealing key requirements that are not well met today despite recently emerged 2FA solutions. First, we investigate past experiences with authentication mechanisms emphasizing problems and aspects that hamper good user experience. Second, we investigate the different authentication factors more closely. Our results reveal particularly interesting preferences regarding the authentication factor "ownership" in terms of properties, physical realizations, and interaction. These findings suggest a path towards 2FA mechanisms with considerably better user experience, promising to improve the acceptance and hence, the proliferation of 2FA for the benefit of security in the digital world.

CCS Concepts: • **Security and privacy → Usability in security and privacy**.

Additional Key Words and Phrases: Two-Factor Authentication, Human Factors, Usability, User Experience

1 INTRODUCTION

Two-factor authentication (2FA) is a widely recommended authentication mechanism for the protection of valuable online assets. In general, there are three groups of authentication factors [25, 42]: The first group relies on the *knowledge* of some information that users have to provide for authentication. Such information can be a password or a personal identification number (PIN). The second group of authentication factors is based on something that is *owned* by users. This could be a physical token, such as a credit card. Finally, the third group *inherence* relies on an intrinsic, unalienable, and characteristic feature that uniquely identifies individual users. Various biometric features can be used for this purpose, such as fingerprints, gait, voice, or face features.

Each group of authentication factors – and each factor itself – alone is not sufficient to deliver adequate security for valuable assets. Authentication mechanisms based on knowledge or ownership could be obtained by a third party to impersonate users. Password databases of digital services might be leaked or hacked. Furthermore,

Authors' addresses: Karola Marky, karola.marky@glasgow.ac.uk, University of Glasgow, Scotland, Technical University of Darmstadt, Germany, Keio University, Japan; Kirill Ragozin; George Chernyshov, Keio University, Japan; Andrii Matviienko; Martin Schmitz; Max Mühlhäuser, Technical University of Darmstadt, Germany; Chloe Eghtebas, Technical University of Munich, Germany; Kai Kunze, kai@kmd.keio.ac.ja, Keio University, 4-1-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8526, Japan.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.
1073-0516/2022/1-ART1 $15.00
https://doi.org/10.1145/3503514

Just Accepted

passwords might be obtained through phishing, shoulder surfing, or man-in-the-middle attacks [20, 27, 55]. Access tokens might get stolen. Biometric authentication is susceptible to mimicry attacks [34]. Most fingerprint sensors only use fingerprint partials that can be mimicked without much effort [47]. Authentication mechanisms based on inherence are often based on probabilistic algorithms and therefore require a fallback mechanism. 2FA means that factors from two groups are combined to form an authentication mechanism. The combination mitigates the weaknesses detailed above. Despite the obvious enhancement of security, current realizations of 2FA typically exhibit issues from a user's perspective. Issues start with overall misconceptions regarding the security benefit of 2FA [12, 18, 24, 45, 60]. Users are generally willing to follow a longer authentication process in exchange for more security [31, 45]. However, if this benefit is not evident, users prefer single-factor authentication [12, 18, 45, 60]. Further issues are rooted in poor usability in the setup process of specific 2FA tokens [46], poor integration among different operating systems [5, 46, 60] requiring users to own multiple 2FA devices, and poor usability of the authentication process itself [9, 18, 61].

Even if setup and authentication would offer good usability, there is one further barrier that might hinder users in interacting with 2FA mechanisms: user experience. It has been demonstrated that users can effectively interact with provided 2FA approaches, however, they perceive the duration of 2FA procedures as too long [9, 18, 61]. Hence, it is challenging for users to afford the required time for several authentication procedures within their daily routines [7]. Another aspect related to user experience is the integration of 2FA into everyday life. Users criticize the usage of non-personalized single purpose devices [60], and would even switch service providers due to 2FA mechanisms [35]. In sum, 2FA loses its security benefit if the provided mechanisms do not consider, security perceptions of users, usability, user experience, and the integration of 2FA in the users' daily lives and routines. Furthermore, providers might even lose customers due to the poor user experience of 2FA.

In this paper, we investigate two-factor authentication from the user's perspective, revealing key requirements that are not well met today despite recent 2FA solutions. We collect qualitative data about 2FA approaches and authentication factors through semi-structured interviews from 22 experienced and 20 inexperienced 2FA users. In particular, we investigated problems related to usage, user experience, and availability. Further, we closely investigated user preferences regarding authentication factors, general perceptions of 2FA, and considerations and expectations regarding the second authentication factor.

Our results confirm and extend existing usability and user experience studies of 2FA, showing that users, for instance, perceive existing procedures as too long and too complicated making it challenging for them to integrate 2FA into their daily routines. Our results further reveal particularly interesting user preferences and expectations regarding the authentication factor *ownership* in terms of properties, physical realizations, and interaction. Users criticized missing customization options of ownership-based approaches. Further, 2FA approaches that either require network or Internet connections, might lead to account lockouts. Additionally, we show points of failure of existing 2FA mechanisms and means to address them. In our study, we evaluate general user perceptions that are not specific to a concrete 2FA mechanism but to the interaction with 2FA mechanisms in general.

Our findings suggest a path towards 2FA mechanisms with considerably better user experience. Following this path is promising to lower user friction and improve the acceptance of 2FA ultimately resulting in a proliferation of 2FA for the benefit of security in the digital world. To pave this way, we contribute a detailed set of user experience-related properties that users expect about a second authentication factor. From our results, we derive requirements and recommendations for 2FA mechanisms that can be tailored to the users' interaction needs and expectations.

Research Contributions. The main contributions of our work are as follows:

(1) **An in-depth study of user perceptions regarding 2FA.** We contribute an in-depth study of 2FA with 20 inexperienced and 22 experienced participants. Our study confirms that both perceived usability and

Just Accepted

perceived security are crucial factors for accepting the usage of 2FA schemes. We demonstrate problems experienced by users that lead to user friction, a rejection of 2FA or even a reduction of authentication factors.

(2) **In-depth investigation of second-factor properties.** Prior work has mainly focused on investigating existing approaches for realizing 2FA. In our work, we also specifically investigate user perceptions of a second factor independently from a specific approach for realizing 2FA. Users are willing to spend extra effort for the sake of security, but the limitations of existing solutions can lead to frustration, lockouts from accounts, and even provider change. Our results shed light on these limitations and pave a way to lower user friction ultimately improving the user experience of 2FA.

(3) **Recommendations for user experience and customization improvements.** We conclude with requirements for the design of the second authentication factor to mitigate a reduction of factors and to support usability and user experience. Our requirements offer a high degree of customization and availability of the second factor while maintaining security and providing means to furthermore mitigate shoulder-surfing during mobile usage. These recommendations serve as a path to better user experience of 2FA ultimately resulting in security benefits in the digital world.

The remainder of this paper is structured as follows. Section 2 provides background information about two-factor authentication and existing investigations thereof. This is followed by a description of the methodology that we applied in our investigation in Section 3. The results of the study are described in Section 4. The following Section 5 discusses the results from the interview study and provides a basis for the recommendations in Section 6. Next, Section 6.3 applies the recommendations to state-of-the-art solutions that provide two-factor authentication. The paper is concluded in Section 7.

2 BACKGROUND & RELATED WORK

In this section, we first provide background information about *two-factor authentication*. Next, we detail related work that investigated *usability* before summarizing publications that investigated the *introduction of 2FA in institutions*.

2.1 Two-Factor Authentication

Since service providers store the passwords in a database, this database might be attacked and leaked. Passwords might also be stolen from users by observing password entry or phishing attacks. To mitigate such attacks, a second authentication factor has been proposed: Two-factor authentication (2FA). A common example of 2FA is used in the scope of payments in supermarkets: a PIN (knowledge) is combined with a credit-card (ownership).

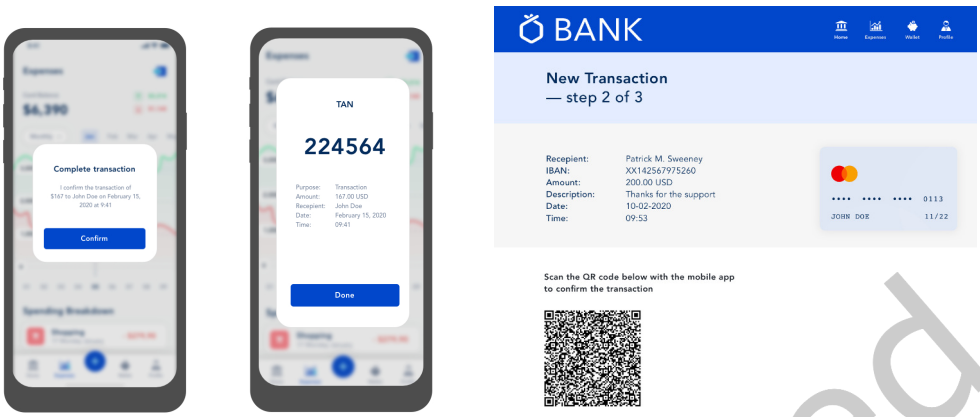
2FA schemes have also been developed for Internet-based transactions. Those schemes can rely on a physical token that generates one-time passwords (e.g., DUO Security Token [50], or Fido U2F [11]). They can furthermore rely on text messages, e-mail notifications, or apps on mobile devices. Previous work has explored a variety of these schemes.

Before the interview study, we collected a set of 2FA approaches that are commonly used for online banking. We used the resulting list of approaches as a basis for discussion during the interviews.

To find 2FA approaches for our investigation, we used an official list of banks in Europe[1]. Based on this list, we searched the respective bank's website for 2FA approaches that are provided by the bank for authentication and the authorization of transactions. The search resulted in a total of 14 different approaches for 2FA provided by banks. We proceeded by clustering similar approaches into categories. Hereby, we focused on the specific tasks that the users have to perform to successfully authenticate. This resulted in the categories of 1) **push**, 2)

[1]Using 2FA for authentication and transaction for online banking is mandatory in the European Union since 2019 [10].

Just Accepted



(a) (b)

Fig. 1. Depictions of the 2FA approaches as user interfaces. (a) Transaction confirmation with Push Approach (left) and OTP Approach (right), and (b) Display of the QR-code on the banking website.

one-time password (OTP[2]) entry, and 3) **scan**. In each category, the user commences by opening the banking website on their personal computer. Then, they enter their login data consisting of their account number and a password or PIN. From here, the interaction differs in each approach.

2.1.1 Push. Using the push approach, the user has to switch to an Internet-enabled second device, mostly a mobile device (e.g. a smartphone). The user unlocks an app on the device with a PIN or password. Then, the app displays information about the login that the users want to perform on the personal computer, including a timestamp. Below this information, the user finds a button for authorizing the login. After *pushing the button*, the user can access their account on the personal computer. Consequently, the interaction required from the user is pressing a button on a second Internet-enabled device. Fig. 1a depicts a possible interface for the push approach on the left.

2.1.2 OTP Entry. In the OTP entry approach, the user receives a one-time password (OTP) over a second channel. The second channel could be given by another device, such as a smartphone. The OTP could, for instance, by received via text message or by an app. After receiving the OTP, the user *manually enters* the OTP into the banking website. The second channel can be via text message, an OTP generator, or a mobile app. Using an OTP approach, the interaction required from the user is entering an OTP that was required from a second channel. Fig. 1a depicts a possible interface for the OTP approach on the right.

2.1.3 Scan. The scan approach is also based on an OTP. The banking website displays an optical code, such as a barcode, a flicker-code, or a QR-code to the user (see Fig. 1b). The user *scans* this code with a second device that has scanning capabilities, such as a smartphone. Based on the data from the code, the second device computes an OTP. The user *enters* this OTP into the banking website. Using the scan approach, the required interactions from the user are scanning the QR-code with a second device and entering the generated OTP into the banking website.

[2]Whenever we mention OTP throughout this paper, this refers to one-time passwords and not to one-time pads.

Just Accepted

To authorize a transaction, the user first has to be authenticated. Then, the user enters transaction data, such as the account number of the recipient. Finally, the user interacts with the specific 2FA approach as detailed above.

2.1.4 Further 2FA Approaches. Besides the 2FA approaches detailed above there are several approaches for realizing 2FA that have been used in Germany in the past or are used in other countries. The remainder of this section explains further 2FA approaches for online banking since those were mentioned by the interview participants from the investigation reported in Section 4.

OTP Lists are lists with numbered one-time passwords. Those lists are typically printed on paper and distributed via postal mail. The bank provides the number of the required one-time password to the users, and they respond with it. Using OTP lists, the second factor is the ownership of the one-time password.

Security cards are similar to OTP lists. Security cards have tables with numbered columns and rows. The one-time password is built by the user by combining the contents of specific cells to a password. The bank requests the content of specific cells from the users.

Other options to distribute one-time passwords are **text messages** received on a mobile phone, **e-mail notifications**, or **apps** on mobile devices as detailed above [31]. In these examples, the second factor is the ownership of the e-mail address, a phone number, or a specific mobile device.

Another common approach is to use a dedicated card reader as an OTP generator - denoted as **chipTAN**[3]. In particular, the device scans a flicker code from the computer screen and then calculates a one-time password based on the scanned information and the debit card. Before revealing the one-time password, the device displays information related to the transaction, such as the transferred amount and the recipient's account number. If the flickering code cannot be scanned, the user can enter the information manually.

2.2 Usability of Authentication

Human factors have been extensively investigated in the scope of several authentication approaches. Since passwords form the predominant method for authentication [53], they have been investigated thoroughly by a plethora of works (e.g., [29, 54, 57]). Users often follow poor password hygiene. They use passwords that are simple to guess or reuse identical passwords among multiple accounts [54, 57, 59]. Furthermore, users also struggle to remember their passwords locking them out of their accounts [29]. Still, due to the easy deployment of passwords, they are unlikely to vanish soon [5, 66]. A usable configuration for enabling 2FA that is technologically robust, however, has not been realized yet [5, 65].

In general, research that investigated the usability of two-factor authentication mechanisms produced mixed results. On the one hand, investigations showed that although 2FA mechanisms were perceived as more secure than single-factor authentication, users preferred single-factor authentication based on usability [45] and the time needed for authentication [26]. On the other hand, some studies demonstrate the usability of 2FA mechanisms [16, 18, 36]. For instance, De Cristofaro *et al.* investigated one-time passwords via text messages, OTP generators, and smartphone apps in an online study [18]. The participants in this study perceived the presented 2FA mechanisms as highly usable. Their results furthermore indicate that besides usability, trustworthiness, and the required cognitive effort are key aspects for defining the adoption of 2FA mechanisms [18]. These results are related to specific 2FA mechanisms and to characteristics of individual users, such as age or background [18]. Further studies showed that participants are willing to adopt 2FA for sensitive online accounts for security reasons [45]. Pratama et al. uncovered a relation between the banking account balance and the willingness to use 2FA [44]. Participants with higher amounts of money in their savings were more likely to employ 2FA.

The usage of 2FA mechanisms can be divided into two phases: 1) setup and 2) day-to-day usage. Reynolds *et al.* conducted two studies that investigated the YubiKey token [46]. They found that setup and day-to-day usage

[3]TAN refers to Transaction Authorization Number.

Just Accepted

exhibit differences in the scope of usability. In particular, the setup process was perceived as less usable. Similar findings were reported by Ciolino *et al.* who also demonstrated that users perceive the setup of tokens to be less usable than setting up text messages [7]. Reese *et al.* investigated the setup procedure of five approaches for 2FA: 1) text messages, 2) time-based one-time passwords, 3) pre-generated one-time passwords, 4) push notifications, and 5) YubiKey tokens [45]. Some participants reported difficulties setting up YubiKey tokens and time-based one-time passwords. Text-messages, pre-generated one-time passwords, and push notifications were perceived as easy to set up. A similar study was conducted by Acemyan *et al.* [2]. They investigated: 1) one-time passwords based on text messages, 2) the Google Authenticator App, 3) YubiKey tokens, and 4) push notifications. Acemyan *et al.* show that the investigated 2FA mechanisms are difficult to use, and the complicated setup discourages users from continuing the usage of 2FA after the setup. These results differ from Reese *et al.* although both studies are similar. A possible explanation for that might be that Reese *et al.* conducted two studies for each usage phase with different participants while Acemyan *et al.* conducted one.

Difficulties during the 2FA setup have also been shown for the YubiKey token by Das *et al.* [12]. Ghorbani *et al.* investigated user perceptions of YubiKey tokens as a possibility for password-less single-factor authentication [23]. While the usability was rated high, participants feared losing the token. Das *et al.* investigated the YubiKey token as part of 2FA [16]. After a first study that uncovered usability issues of the YubiKey, they investigated a refined version. While the refined version offered improved usability, the study reveals that users still are hesitant adopting 2FA based on passwords and the YubiKey. Reasons for that are based on a concern of losing the hardware token and thus similar to the results from Ghorbani *et al.* [23].

Krol *et al.* investigated 2FA in the scope of online banking [35]. In particular, they investigated 1) card readers, 2) one-time password generators, 3) text messages, 4) phone calls, and 5) smartphone apps throughout a usage period of 11-days. The participants were interviewed in the beginning and at the end and were asked to write a diary about their online transactions. One-time password generators were perceived as a substantial extra effort since they are new additional devices that have to be carried and possess usability issues. This confirms a previous study by Weidmann *et al.* [60]. Weir *et al.* investigated three different types of physical tokens [61]. Participants in their study favored devices for 2FA based on their usability rather than security properties. Another study by Weir *et al.* [62] showed that familiarity with 2FA has a high impact on the users' willingness to use it. This might be a possible explanation for the mixed results for existing usability studies.
2FA often requires two different devices to operate together. Methods for device pairing have been investigated and found that a system's operability can impact the security perception of its users [30]. An investigation of older adults shows that adoption issues of tokens are rooted in compatibility issues [13].

Karapanos *et al.* propose a scheme that authenticates the user based on recording sound in the user's environment and on a user-worn device [32]. Based on the sound, the authentication mechanism can judge whether a user is close to the device they intend to authenticate at. Karapanos *et al.*'s mechanism was perceived as more usable than Google's authentication app.

2.3 Two-Factor Authentication in Real-World Interactions

The introduction of 2FA has been investigated in several contexts and institutions, meaning that researchers investigated the transition from single-factor to two-factor authentication. Users prefer or choose devices that they already own over new additional physical tokens [60]. Colnago *et al.* investigated the introduction of the Duo 2FA token at Carnegie Mellon University [9]. Authenticating with a 2FA mechanism also took longer compared to single-factor authentication [9]. However, if users have positive experiences with 2FA, they might even use it for accounts that do not require it [9, 19]. Users even reported that using Duo 2FA was easier than expected. Abbott and Patil conducted a series of online surveys on a university with mandatory 2FA usage [1]. In general, the acceptance of 2FA was not impacted by the obligation to use it, however, the frequency of usage impacted

Just Accepted

acceptance. Golla *et al.* investigated different messages to aim to nudge Facebook users to switch to 2FA [24]. Their results show that messages targeting the users' sense of individual responsibility, personalized messages that include user information, and messages that assist users in adjusting their mental model of 2FA are promising to boost adoption.

2.4 Summary

Each of the presented works investigated specific approaches for providing two-factor authentication in different domains. We build upon these previous works, focusing on ways of improving usability of second authentication factors. We did not tie these properties to a specific existing 2FA approach since specific existing solutions have been widely investigated, instead we collected generic properties that could be used to inform the design of a range of different 2FA approaches. Despite recently emerged solutions for 2FA and their investigation of usability, user experience and adoption, the users' perspective is not well reflected on state-of-the-art mechanisms. With our work, we highlight the current frustration of users with 2FA solutions that might lead them to insecure behavior or even provider change. With our findings, we create a path to better user experience of future 2FA solutions ultimately delivering the security benefit given by 2FA to the digital world.

3 METHODOLOGY

To investigate the participants' experiences with 2FA mechanisms in online banking we conducted an interview study with 42 participants. We opted for semi-structured interviews because they offer a degree of standardization while allowing flexibility to gain a deeper understanding at the same time. For the full interview guide, we refer the reader to Appendix A.1.

3.1 Pilot Interviews

Before determining the final set of interview questions, we conducted two pilot interviews. After that, we adapted the wording of questions to improve clarity. The results from the pilot interviews are not included in this paper.

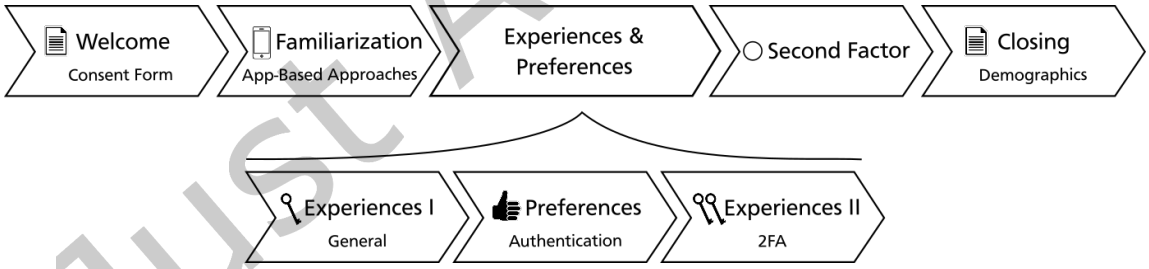


Fig. 2. Procedure of the semi-structured interviews.

3.2 Interview Procedure

Our interviews were divided into three major parts: a) online banking authentication, b) two-factor authentication, and c) considerations and preferences about the second authentication factor. The first part was particular to nudge the participants to start talking about their experiences. With the progression of the interviews, the introduced topics became less specific and were not connected to online banking any longer. The specific procedure of the semi-structured interviews was as follows (see also Fig. 2):

Just Accepted

3.2.1 Welcome. We welcomed the participants to our lab and commenced by detailing the study's procedure, the consent form, and the data protection policy. The participants were asked to read and sign the consent form. We also explained that the interview will be recorded and that the audio file will be transcribed before analysis.

3.2.2 Familiarization. Next, we presented mock-ups of the 2FA mechanisms to the participants, such that they can familiarize themselves with them. The mock-ups were viewed by the participants through screen-sharing of a presentation including screenshots. If the participants had any questions regarding the procedure *how* the respective 2FA approach worked, the examiner answered them. Questions on *why* the approach worked were post-phoned to after the interview.

3.2.3 Experiences I: Authentication Approaches. We started the interview by asking the participants which authentication approaches they have used for their online banking. Based on their reported experiences, we asked for their opinion about each approach, whether anything went wrong during usage, and about aspects that the participants particularly (dis)liked. If the participants used an approach in the past, we asked why they had stopped using it.

3.2.4 Preference for Authentication Approaches. Based on their experiences, we asked the participants about their favorite approach for authentication in the scope of online banking. The participants were asked to explain their answers.

3.2.5 Experiences II: 2FA Approaches. Until then, we did not mention 2FA approaches specifically. Thus, the participants could also mention other authentication approaches based on single factors. At this point in the interview, we intentionally explained that 2FA is mandatory in some countries in the scope of online banking to focus the interview on 2FA. We established an understanding of the term with the participant based on examples. Based on that, we specifically asked for experiences with 2FA, which included experiences in domains different from online banking. Analogously to the experience with authentication approaches, we asked whether anything went wrong during usage, about aspects the participant particularly (dis)liked, and why the participants had stopped using it.

3.2.6 Second Authentication Factor: Expectations and Properties. In this part of the interview, we focused on the representation and location of the second authentication factor. We asked the participants which properties they would expect from a second authentication factor. Then, we asked where they would expect or prefer the second authentication factor to be. We did not restrict the participants to anything based on realization options, instead, we encouraged them to express their preferences freely.

3.2.7 Closing. The participants were asked to provide demographics and to fill out the ATI scale questionnaire, which assesses the participants' affinity for technology [22]. They could give final comments and ask questions about the study. Finally, the examiner reimbursed the participants.

3.3 Recruitment and Participants

We recruited 42 participants via mailing-lists, social networks, flyers, posters, word-of-mouth, and snowball sampling. Each participant received an online shopping voucher roughly equivalent to 10 USD as compensation. Participation was restricted to users of online banking. Half of the participants were from European countries (Germany, France, and the UK), the other half were from Asian countries (China, Japan, Taiwan, and South Korea). In 2019, banks in the European Union were required to use 2FA for login procedures and the authorization of transactions. Hence, the participants had different experiences with online banking including a time-frame during which 2FA was not required by law in the European Union. The term "authentication" was not mentioned in the invitation to the study.

Just Accepted

Our participants were on average 27.29 years old ($SD = 4.08$, $Median = 27$, $Min = 19$, $Max = 36$). About half of the participants identified as female ($N = 18$), 23 identified as male, and one participant preferred not to say. The ATI scale ranges from 1 to 6, where 6 indicates the highest affinity for technology. Our sample demonstrated an average of 3.82 ($SD = 0.72$, $Min = 2.44$, $Max = 5.33$).

3.4 Data Analysis

Before the analysis, all interviews were transcribed into written form. Then, we analyzed the transcripts in two sessions applying thematic analysis [6]. The analysis consisted of open and axial coding with two coders. First, the coders familiarized with the data and chose four representative interviews to develop the code book. Next, they followed an open coding process on these four interviews. Then, the researchers compared their coding results in a review meeting to establish a code book. Disagreements regarding code allocations were resolved by discussion and agreeing on a final code for the respective statements. For the codebook, the reader is referred to Table 5 in Appendix B. Next, each coder applied the coding tree to half of the interview transcripts. In order to ensure consistency between the two coders that coded the two different subsets, a random subset of four interviews was coded by both coders to determine the inter-rater reliability as recommended by McDonald *et al.* [40]. To determine the inter-rater reliability, we calculated Cohen's κ which was 0.876 referring to "almost perfect agreement" [8]. In case the coding of a statement was unclear to a coder, the statement was marked for discussion in a review meeting. In order to ensure coding quality and objectiveness, one coder reviewed all coded transcripts and marked ambiguities for discussion. To make sure not to overlook findings, the coders agreed to mark statements for discussion in case they considered it to be an aspect that was not yet considered in the code book. In a final meeting, potential ambiguities were resolved and new codes were discussed. All new codes created during this phase were related to 2FA approaches that the participants mentioned using[4].

3.5 Limitations

This section reflects the limitations of the interview study. As a first limitation, one could argue that our sample was rather young. Thus, the findings of the study might not be representative. A second limitation based on the composition of our sample is that it primarily consisted of participants with a medium to high affinity for technology. Consequently, we cannot make conclusions about users with low affinity for technology. A third limitation based on the composition of our sample is based on our recruitment strategy. We intentionally targeted end-users that are users of online banking. However, end-users might not be familiar with threat models and security attacks and might therefore underestimate them. Further, some participants based their security perception on the difficulty of using the presented 2FA mechanisms. Another limitation might be given by the connection to online banking that we made to provide a tangible scenario to the participants. To mitigate this, we also interviewed the participants about their experiences in domains other than online banking. However, most reported experiences were directly related to financial transactions. Based on the qualitative investigation method, quantitative conclusions based on the number of mentions cannot be made. This furthermore means that frequencies of mentions in our exploratory study cannot be considered to be representative of the overall population of 2FA users. Although, we grouped the participants into experienced and inexperienced users, comparisons between those groups based on frequencies of mentions cannot be made due to the qualitative nature of our study. We provide such frequencies in the result section to give the readers an impression on how often specific aspects were mentioned.

[4]In particular the codes *other_gaming* and *other_devices* were introduced. The "other" refers that participants used 2FA for another purpose than banking.

Just Accepted

3.6 Ethical Considerations

In each study, we followed the guidelines of the ethics committees at the authors' institutions. Therefore, we limited the collection of personal data to a minimum to preserve the privacy of the participants. Before the interview, each participant signed a consent form. The consent form had a paragraph about the study's data protection policy. Our study complied with strict national privacy regulations and the EU's General Data Protection Regulation (GDPR). The consent form was stored separately from all other data such that collected data cannot be linked to participants' identities. In the data set, each participant received a randomly assigned identifier. The consent form furthermore informed the participants that participation is voluntary and that they can abort any time without fearing negative consequences.

Before the analysis, all audio files from the interviews were transcribed into written form. Statements from the participants that contained personal information were replaced by neutral placeholders[5]. All audio files were deleted after transcription.

Our institution is located in a country without a requirement for following a formal process involving an institutional review board for the kind of user study we conducted. We used a video calling service that we hosted on a server at our institution. All interviews were conducted over this service. All documents that required a signature from the participant were submitted to the examiner digitally. The interview period was from December 2019 until March 2020.

4 RESULTS

This section reports the results from the coding analysis. Section 4.1 describes the participants' *experiences with using 2FA*. Results about *preferences* can be found in Section 4.2. Next, Section 4.3 provides specific *problems* when using 2FA. The following three sections (4.4, 4.5, and 4.6) detail the results regarding the *second authentication factor*. Finally, Section 4.7 lists *further findings*. We provide sample comments from the participants and also report the authentication mechanism that the comment refers to, if possible. For this, we use the terminology introduced in Section 2.

When presenting our results, we include frequencies of mentions to give the reader an impression of how often the respective topic came up during the interviews. Due to the qualitative and exploratory nature of our study, however, these frequencies should not be considered representative of the general population of 2FA users.

4.1 Experiences with 2FA

At the beginning of the analysis, the participants were clustered into experienced and inexperienced users based on the following criteria: reported frequency of usage, knowledge of existing methods, and current usage.

Twenty-two participants reported using 2FA at least once every other week. Furthermore, they have been using it for longer than two years. Of the remaining 20 participants, nine only used 2FA for one-time verification purposes, such as opening new accounts, eleven reported having used 2FA in the past or infrequently (less than one transaction per month).

As a result, the sample consists of 22 experienced users who use 2FA mechanisms on a frequent and regular basis and 20 less experienced users, labeled as inexperienced users, who use 2FA mechanisms rarely or in the past. In the remainder of this section, the experienced participants are abbreviated with *ex* and the inexperienced ones with *iex*.

Furthermore, we asked the participants which specific approaches they (have) used in the scopes of 1) *online banking* and 2) *further domains*.

[5]For instance, the statement *"my friend George from London uses 2FA."* would have been anonymized to *"my friend [name] from [city name] uses 2FA"*.

Just Accepted

4.1.1 2FA in Banking. When we asked the participants which specific approaches for realizing 2FA they used for online banking, they could give multiple answers. Of the experienced participants, nine reported using a chipTAN device, which is used in combination with the debit card. In particular, the device can scan a flicker code from the computer screen and then calculates a one-time password based on the scanned information and the debit card. Before revealing the one-time password, the device displays information related to the transaction. Twelve participants stated to have used a scan approach based on a mobile app (ex=9, iex=3), seven (ex=5, iex=2) reported to use the push approach, and 17 used one-time passwords based on text messages (ex=7, iex=10). Four participants (ex=0, iex=4) used security cards. Finally, five participants reported having used one-time passwords that they receive by e-mails (ex=0, iex=5).

4.1.2 2FA in Other Domains. We furthermore asked them whether they use 2FA approaches in other domains. Seventeen participants (ex=11, iex=6) reported to use 2FA for other financial transactions, such as PayPal. Six stated to use 2FA for their gaming account (ex=4, iex=2). One experienced participant used it for their health insurance. Another experienced participant even used it for unlocking their laptop.

4.2 Preferences of Authentication Approaches

When we asked the participants about their preferences regarding authentication mechanisms, we could cluster the participants' answers into two groups based on their experience with using 2FA mechanisms. Those who used 2FA, in general, favored a 2FA approach and considered a trade-off between security and usability. This consideration lets them sacrifice usability and convenience for the sake of security. Inexperienced users, in general, preferred not to use a 2FA approach since they perceived it to be too cumbersome or too time-consuming.

4.2.1 Presented Approaches. We then asked the participants about the presented app-based approaches. The inexperienced participants tended to prefer the push approach since this was easiest to use, and the changes between devices were lowest:

> *"The style of authentication that you confirm just by clicking, you don't have to type. Other ones were too complex."* (P14, iex, push)

> *"It was just clicking a button. It doesn't need any other actions like scanning a QR-code. It's simple. [...] some people might feel insecure. For me, it's okay because it's easier."* (P15, iex, push)

The experienced participants, however, preferred the OTP approach. When asked to explain their answer, they stated additional security:

> *"The OTP, because I think it's a good middle course. When you use the QR-code, you need the camera. That's less secure because someone could spy on that and forward it to a third party."* (P11, ex, OTP entry)

Some participants in both groups favored the scan approach for different reasons based on security and usability. P21 stated the following about a chipTAN device that combines a debit card with the scan approach:

> *"The security that a transaction is only possible if you have my card and not just a PIN, which can be hacked or copied somehow. I like the fact that I know for sure that I don't have to enter anything manually. So everything is done automatically, recorded via the code, which I also like. Yes, and of course, it is also fast in itself."* (P21, ex, scan)

> *"I kind of like that scanning code makes sure that you are physically next to the computer. You probably know better than I do, but for me, it's not too much back and forth, and it feels more secure."* (P4, iex, scan)

Just Accepted

Experienced participants, in general, did not hesitate to sacrifice usability for security, while inexperienced participants did. That indicates that besides usability and security perceptions, personal experiences form an important impact factor for the acceptance and willingness to use 2FA mechanisms.

4.2.2 General Preferences. In the interview part "experiences I", we asked the participants about any 2FA mechanism, participants tended to substitute passwords as the first factor by biometric factors, such as fingerprint or face recognition, since those cannot be forgotten:

> *"I like facial recognition as one condition [factor]."* (P19, iex, face-ID)

> *"I love the fingerprint and the face thing. I use that a lot for every online banking transaction."* (P20, iex, fingerprint)

One participant voiced a generally negative attitude about 2FA even if it contributes to security:

> *"Honestly, I hate double authentication. It takes too much [...] I'm not a huge fan of it, it's very inconvenient for me."* (P20, iex, text messages, security card, e-mail)

4.3 Experienced Problems

When we asked the participants about problems that they experienced with (two-factor) authentication mechanisms, they stated a range of problems that are common for PINs and passwords. Most participants stated to have forgotten their PIN or password or mistyped it. As a consequence, accessing the accounts was not possible. Furthermore, one-time passwords were copied incorrectly.

Several experienced participants did not report problems beyond PIN and password memorability. Participants that used one-time passwords distributed by SMSes reported problems receiving the SMS in time due to a poor or foreign cell phone network:

> *"I can remember one case where I was abroad. Somehow the SMS did not arrive in the foreign network, and I had problems to authenticate myself."* (P7, ex, text messages)

Several participants in the experienced group reported the usage of one-time password generators (chipTAN). Frequent problems with such generators were broken generators or empty batteries:

> *"I had it a few times that the battery of the device ran out and then I could not make any more transfers. Who has such button batteries at home?"* (P7, ex, chipTAN)

> *"The calculator ran out of battery at some point, and I couldn't just change the batteries, it was kind of complicated and then it broke, and the bank wouldn't send a new device. It was a bit of a struggle with the technology."* (P3, ex, chipTAN)

That also happened to users of smartphone apps:

> *"Sometimes I have to pay something, and I don't have my phone charger with me. Then, I cannot do it because it relies on another thing to be working."* (P20, iex, app)

Participants using the scan approach mentioned to have had problems with scanning the codes on several screen types:

> *"Nah, it's just annoying to hold it up to the screen until it detects these codes exactly and it stops all the time in between."* (P12, ex, scan)

One participant reported a loss of a security card that is needed for authentication:

> *"Yeah. However, I think the [security] card was horrible. The card was gone, and I couldn't log in and any more."* (P19, iex, security card)

Just Accepted

Table 1. Overview of the second authentication factor properties captured in our interview study.

Property	Explanation
Usability	second factor should have excellent usability
Mobility	usage of second factor should be location-independent
Connectivity	no network connection required for second factor
Energy Sources	second factor should not rely on energy sources or be chargeable with standard chargers
Security	second factor should offer secure interaction

Finally, participants reported problems with the setup of 2FA. While the setup worked in general, the participants perceived the duration and number of required steps are overly long. One participant reported to have stopped using 2FA right away due to usability reasons:

> *"I actually didn't like trying it. It was a bit too much for me. I only can use a password."* (P18, iex, security card)

4.4 Second Factor Considerations: Properties

When we interviewed the participants about their expectations towards a second factor, they mentioned a range of similar properties. These properties were mostly independent of the participants' experiences with 2FA. Table 1 provides a summary of these results.

4.4.1 Usability. Almost all participants stated that usability is a key factor for them when using the second authentication factor. The factor should be easy to use and not be restricted to a specific location:

> *"It should be easy to understand, described in a way that I know what to do."* (P6, ex)

> *"It should be convenient, easy to use. I want to have fun using it."* (P3, ex)

This confirms results from previous studies of specific 2FA approaches showing that usability is a key factor in the scope of 2FA [1, 12, 18, 19, 23].

4.4.2 Mobility. The majority of participants wished the second factor to be mobile such that it can be used on-demand in any location.

Some participants mentioned that the second factor should be available as an app on their mobile devices. The main reason for that was that the participants already own these and devices, and it is not necessary to introduce any new item:

> *"I would definitely want to continue using the smartphone. Because one has that anyway. So I think it's incredibly annoying when you need 5000 devices and then you forget one, when you go on vacation [...] and don't have it with you, then you're immediately stuck. So, the smartphone is with you anyway, so I think that's a very good second factor."*
> (P14, ex)

> *"I carry my cellphone with me anyway. It is in my pocket already."* (P9, iex)

However, participants were also aware of the limitations of mobile devices as a second authentication factor. Depending on the security model, the mobile device should not be the second factor if it is also used for banking. Several participants reported that their bank allows this, however, does not recommend it:

> *"You always have to have two devices if you want to do something. What I'll say now is contradictory to the first thing I said about security, but it's annoying. So it would be cooler if you had something that*

Just Accepted

you always have with you. Well, a smartphone is something you always have with you normally. But a watch or something else. I'll put it this way. It's just annoying if you have two devices in your hand or you have to have two devices to do something, but at the same time, it's more secure, and then you feel good again." (P19, ex)

Another limitation of the smartphone was that the device is a central point of failure:

"Now, everything depends on your cellphone. If you lose your cellphone, you lose so many things. So, I want this function to get away from the cellphone." (P17, iex)

Even if the second factor is not an app on a mobile device, it should still be mobile. Sample comments given by the participants are:

"For me, it's a trade-off. It should not be on the smartphone because I think it's too dangerous, but it also shouldn't be anything bulky that I don't want to carry. I don't want to be restricted to my home, you know." (P4, iex)

On the other hand, one participant stated that the second factor is not required to be mobile since they would prefer to keep it at home in a safe place:

"I prefer something I can keep in my desk at home. If I need to pay something right away, I can also use a payment provider like [name of payment provider]." (P2, iex)

4.4.3 Connectivity. The next group of considerations is connected to the connectivity of the second factor meaning whether it is possible for it to access the Internet or other networks. Two major themes emerged in this scope. First, participants expressed that the second factor should *not* be connected to the Internet or other networks for either security or availability reasons. They imagined the second factor to be a stand-alone device that can be used without network connections. For instance, the participants stated:

"For me, it should be uncoupled from any network. A connection to the phone number is okay in general, but it is relatively easy to get the phone number of someone." (P4, iex)

"It should not be dependent on the cell phone network [...] it already happened that I needed a verification code over SMS and that is rather obstructive if you are somewhere where with no reception." (P1, ex)

4.4.4 Energy Sources. This group of considerations is connected to energy sources of devices, such as batteries. Several participants wished the second factor to be independent of any energy source. This was related to negative experiences with one-time password generators that ran out of battery and needed special batteries. If the second factor needed an energy source, participants stated that they wish to use chargers identical to those of their mobile devices. However, participants favored a second factor that is independent of such energy sources. When asked for examples, participants mentioned NFC and RFID chips:

"It should be fast somehow and secure [...] those cards that can be read by the smartphone and can be used any time. " (P21, ex, NFC, RFID)

Further statements about energy sources can be found above in the subsection about reported *problems*. One participant would even use a chip that is implanted under their skin:

"There are great technical things like RFC rings and so on, the ones you hold on RFC readers that can read information from the ring you wear, automatically or something. Or biohacking, you can put a chip under your skin, and then it works. I would find it cool in that direction, but I don't think that the world, mankind is ready for it, [laughs]. So in that direction, I say it would be one thing I personally would use, but not many people can do that." (P19, ex)

Just Accepted

Table 2. Design considerations for the physical representation of the 2FA device captured in our study.

Representation Property	Explanation
No Extra Device	second factor should not be a dedicated extra device
Everyday Objects	second factor should be integrable into everyday objects
Customization	second factor should be customizable matching the user's preferences

4.4.5 Security. Many participants also stated a need for security, as an essential property of the second authentication factor:

> *"I don't know I would go for something that's very difficult to fake."* (P14, iex)

> *Security, user friendliness, hmmm which property would I like? Good functionality.* (P15, ex)

> *Additionally to my password, I configured that I can use my fingerprint and scan face such that such that I have three possibilities to combine. For me, that feels more secure.* (P20, ex)

Further statements about security have already been mentioned in several other subsections within this results section.

4.5 Second Factor Considerations: Interaction

Although we did not specifically ask the participants about interactions with the physical representation of the second authentication factor, several participants named properties that specifically target it.

4.5.1 In-Pocket Interaction. Some participants stated that they would like to interact with the second-factor device while it is in their pockets. In doing so, the interaction is less obvious for an observer:

> *"That's the thing. It's you use it everywhere someone you see it like in a train someone could watch you do it. I want something that I can use in my pocket."* (P22, ex)

> *"A silent gestures or so would be good. [after being asked for clarification] Something I can do, but I don't have to look at the screen. Like the fingerprint, that one I can do in my pocket, but more sophisticated."* (P6, iex)

4.5.2 Further Interactions. One participant stated the wish to solve a challenge based on a physical puzzle as part of the second factor:

> *"Solving a puzzle."* (P17, ex)

4.6 Second Factor Considerations: Physical Representation

In the final part of the interview, we asked participants about possible physical representations of the second factor that they would like to have (see Table 2 for an overview). We did not limit this based on any constraints such that the participants can freely express their opinions.

4.6.1 No New Extra Device. Participants frequently mentioned that the second factor should not be a new dedicated extra device specific for each provider. This is connected to the statements from participants that wished to use one of their mobile devices since they already own them. When asked to explain their answers, participants mentioned being afraid to lose the device and stated fear of requiring too many extra devices:

Just Accepted

> *"I wouldn't like another device because right now I have to take care of the [one-time password generator] token. And if it gets lost, it's very difficult to get another one."*
> (P16, iex, OTP entry)

Two participants also mentioned the cost of such 2FA-devices:

> *"I would say it is important that it is always available, or often. If the availability is not given, it should be replaced as fast as possible and as low cost as possible."* (P7, ex)

> *"One generator costs a lot between 20 and 25$ I guess."* (P8, ex)

Biometrics were frequently mentioned as an option to be independent of an additional device or password. However, a sensor is required to capture the biometric data:

> *"A bio feature I would say. A face scan, fingerprint, or retina. But I'm not sure if that is secure, but it's convenient."* (P15, iex)

> *"A way to ensure that you are the person that that is that is manipulating cell phone, so maybe your face recognition or finger recognition system."* (P16, iex)

4.6.2 Everyday Objects. Several participants stated that they would like to integrate and hide the second factor in an everyday object. In doing so, the physical representation is not obviously connected to authentication for an observer:

> *"Yes, but relatively small and compact so that you can always have it with you. If it is a different device than the smartphone, then something very flat which you can hold perhaps even on the smartphone, which does not belong, however, to the smartphone. I do not know, such a bizarre idea would be a phone case."* (P11, ex)

Since wallets are located in which bank cards and similar objects are stored already, participants wished for an object that could be stored in the wallet:

> *"I think there are sometimes cards like that. I think those are actually quite appealing because they're easy to transport and put away. So, something in card form, which perhaps even resembles a bank card."*
> (17, ex)

Another group of participants mentioned the wish to integrate the second factor into an accessory, such as key rings, rings, chains, or bracelets:

> *"I would like a ring. Maybe that's too small. I don't know. Or a chain or a bracelet, something pretty that I can wear."* (P7, iex)

> *"Some kind of accessory or so."* (P9, iex)

Wearers of glasses mentioned that if possible, they would like to integrate an authentication device into their glasses because it is impossible for them to forget:

> *"I kinda like to put it in my glasses somehow. That would be really cool."* (P1, iex)

> *"There are four things I always have with me. Keys, wallet, smartphone, and my glasses. Keys and wallet are already targets for thieves and the smartphone also. My glasses would remain. I think there already are kind of smart glasses. I would use that."* (P22, ex)

4.6.3 Customization. Furthermore, the participants mentioned missing customization options of existing approaches. If they have to use (new) devices offered from the provider, they are limited in terms of shapes and colors:

> *"My bank offers custom colors for the bank card that is very nice and should also be for the authentication thing."* (P2, iex)

Just Accepted

"My Yubikey works well, no problems with that but it's kinda ugly." (P21, ex, Yubikey)

4.7 Further Security-Related Findings

Besides the findings connected to our research questions, we found additional common topics mentioned in the interviews that were related to security.

4.7.1 Security Perceptions. Although we did not specifically ask about security, several participants mentioned security-related aspects. When we asked the participants about their preferences, those who favored the scan approach considered this approach to be the most secure because the number of steps that users have to perform would be related to security. Furthermore, they expressed that scanning the QR-code ensures that users are physically next to the device used for banking. On the other hand, the push approach was considered the least secure. For instance, P11 stated:

> *"Because with the other [approaches] you read something on one device and then you have to enter it on the other one. Here, it is only like this that you press a button, and then the data is sent back. Simply like that, and you don't have to enter manually at the PC again. That is simply more back and forth with the others."* (P11, ex, push, scan)

Furthermore, the information that 2FA approaches displayed to the users seemed to impact their security perceptions positively. One participant commented on the location of the authentication attempt:

> *"This mechanism also tells you that you are at [name of location]. So it tells you so, for example, at the time of the transaction that you are, I don't know in [name of other location]. So you know, it's not you."* (P14, ex, app)

4.7.2 Behavior that Impacts Security. When we asked participants about their usage of 2FA mechanisms, several of them stated to use a 2FA app in combination with a banking app. Five of them did this, although their bank particularly advised against it. Three participants tried to do that, but their banks' app had an integrated check whether both apps are installed.

Some participants reported the need for a security card from their bank. The security card has a credit card size and shows a table with different characters and numbers. When performing a login, the banking website asks for two symbols of specific columns that change. One participant reported to have a picture of this card on their phone:

> *"My bank has this card you need for the login. I don't use a wallet any longer because everything fits in the phone case, so I took a picture of the card."* (P5, iex, security card)

5 DISCUSSION

In this section, the results of the semi-structured interviews and the resulting requirements are discussed. The discussion furthermore serves as a basis for the final recommendations in the following section.

5.1 Mobile 2FA Solutions

A prominent theme throughout the results is that the usage of 2FA should not restrict user mobility. This finding is related to the availability of the second authentication factor. Participants in prior user studies showed that availability of the second authentication factor might be an issue [45, 60]. Thirty-five percent reported not to have immediate access to the second factor when needed because the second factor interfered with habits [45]. Our investigation confirms the importance of availability and extends this aspect by the users' wishes not to be

Just Accepted

restricted to a specific location or environment when authentication is required. Such a restriction, however, creates user frustration since users cannot fulfill their goals without being authenticated as our results show. Consequently, mobile 2FA solutions would be required. There are several possibilities to enable such mobile solutions as well as important aspects that have to be considered when offering mobility.

5.1.1 Mobile Devices as Second Factor. Personal mobile devices might be a viable solution for second-factor devices that can read NFC data or QR-codes. The adoption of mobile device apps in the scope of online banking reinforces this aspect. However, mobile device apps as a second authentication factor also mean that the mobile device should not be used for banking (or the respective main task). This weakens security and could even reduce authentication factors completely. Participants reported to either have tried using banking and 2FA apps on one device or actively use them. This indicates that, in general, the usage of both apps on one device should be technically prevented to deliver adequate security.

5.1.2 Internet and Network Independence. Many providers of 2FA assume that devices are ubiquitously connected to the Internet or the phone network [48]. Participants in our study reported having been locked out from their accounts due to Internet or network issues. Although we mainly investigated settings in which authentication is required for Internet-based services, the assumption of Internet connectivity could also impact offline services. This could be technical devices that require authentication but are either not connected to the Internet, or the users do not want them to be connected, e.g., a smart TV. Having such devices rely on the Internet or (cellphone) network might place unnecessary restrictions on users and impact access to the devices. Consequently, dependence on network or Internet should be needed in scenarios in which using the Internet or network is required for interaction in the first place.

There already are solutions that offer OTPs without requiring a network or Internet connection except for during the setup, such as time-based OTPs (TOTP) that are generated on the device. Using such an approach introduces the tradeoff that recovery from loss becomes more important. Consequently, it should be possible to recover access to the account if a device or token is lost, this finding has also been reported by related work [5, 16].

5.1.3 Fully Mobile Solutions. Current approaches for realizing 2FA are mainly designed for usage in combination with a personal computer. However, the ongoing digitization impacts the behavior of Internet users, which is also reflected by our sample. Mobile solutions should work without the need for a personal computer. Consequently, the second authentication factor must not be the mobile device since this device is already used for the respective main task.

Several participants reported that their 2FA devices rely on unusual batteries or on the cellphone network, which has impacted their accounts' access. Thus, energy sources and network requirements[6] greatly impact the effectiveness of 2FA. Many devices that do not rely on networks currently have no option to be recharged easily, and the vendors of the devices are scarce. Although prior work has already concluded that such devices need standardization, the current state-of-the-art devices are not standardized in a way that fulfills user needs. Furthermore, the size of several devices limits their portability. Hence, the second authentication factor should not rely on an extra device that requires an active energy source. Instead, it should be readable by a mobile device. Another crucial aspect for mobility is related to scalability. The current 2FA situation is widely fractured among different solutions. Different service providers offer different solutions despite attempts to establish standards for 2FA, such as the OAuth 2 standard [28] or the Yubikey [63]. As a consequence, users might in the worst case require one 2FA device (or app) for each service similar to the way they require passwords. As demonstrated in our study and related work [5], users do not wish to carry extra devices. The current deployment situation does not scale well for different accounts if something different from a smartphone app or text messages are used.

[6]Note that there are several possible locations in which Internet access is possible while access to the cellphone network is not.

Just Accepted

This situation demands solutions that are scalable and allow usage with a variety of different accounts without creating a single point of failure like single-sign-on solutions do [58].

5.1.4 Security Considerations for Fully Mobile Solutions. The mobility of devices introduces several challenges from a security perspective. Since this investigation's focus is on the user side, the security considerations given here only represent a fraction of security-related aspects. Even if the second authentication factor would be a smart card or something similar that is not part of the mobile device but can be read by it, attacks similar to those on OTP lists or replay attacks on the sensor could be performed. Thus, if the second authentication factor is somehow captured by a mobile device, a challenge that the users perform or nonces should be included to mitigate the aforementioned attacks. Another security-related aspect of fully mobile 2FA is a higher likelihood of shoulder surfing attacks. Several participants in our study also reflected this aspect. Therefore, fully mobile solutions should encompass means to mitigate these attacks or inform users about them.

5.2 Everyday Objects for Authentication

Another common theme of our study was the wish that everyday objects can be used for authentication since carrying more devices is inconvenient and might collide with user habits. Previous studies of specific solutions, such as printed OTP lists, tokens, and even mobile devices, showed that user habits interfere with availability [45]. Several studies have demonstrated that 2FA should not require users to carry anything [5] not even a token [35, 60]. Yet, solutions to reduce the burden from users primarily focus on using mobile devices which introduce new attack surfaces as discussed above. Since passwords will unlikely be eliminated as the first authentication factor [65], inherence would be a solution to allow users not to carry anything. However, inherence has several drawbacks, such as fallback authentication, defeating the benefits of 2FA [56]. Consequently, the second authentication factor likely has to rely on ownership. Another important aspect in this context is that one specific 2FA mechanism or device is likely not to be a one-size-fits-all solution for a large share of users. As also shown by Colnago *et al.* [9], users want to tailor authentication to the specific protected asset. Having an everyday object as the second factor was perceived as a possible solution to these issues by users even though that would potentially introduce a new item. Specific objects could be chosen and customized by the users shifting the purpose from a standalone authentication device to something that better integrates into users' daily lives, such as accessories. Using an everyday item might even enhance security by breaking the obvious connection to authentication and offering more discreetness. Such objects do not necessarily have to be mobile. For instance, users could have an everyday authentication object that they can hide between regular objects on their desks or similar.

There are several possibilities to realize everyday objects for authentication. RFID or NFC chips could be integrated into everyday items and turn them into authentication devices that do not need energy sources. Another possibility is using 3D-printed items, which can be turned into passive sensors that can recognize a range of different interactions [39, 49]. Such items would only function in combination with a touchscreen device. Considering that all smartphones and tablets contain touchscreens, such devices might be a promising solution. Furthermore, the usage of 3D-printed shapes might allow for customization by users. This could be a personal key ring, pendant, or eyeglasses frame. The concept 3D-Auth realizes these aspects by custom 3D-printed items for authentication [39]. The usage of specific items, however, also requires means to cope with situations where the items are lost.

5.3 Authentication Interactions

The third common theme in our study is that users wish to have better alternatives to passwords and PINs due to memorability issues. Biometric authentication mechanisms, such as face-ID or fingerprints, have already been deployed by several 2FA app providers. As stated above, those are based on probabilistic schemes that require fallback authentication mechanisms that are often passwords or PINs. Some participants expressed the wish

Just Accepted

to authenticate in a discreet way, such as performing some interactions in a pocket. This confirms previous investigations that proposed 2FA should be resilient to physical observation [5]. Yet, current solutions resistant to observation are based on hiding or obfuscation content on a screen [21].

Based on that, we argue that specific authentication interactions might be a viable solution. E.g., gestures are already commonly used for unlocking mobile devices and are memorable [51] because they leverage muscle memory. Other authentication mechanisms that already leverage gestures are, for instance, based on gazes [33]. However, gestures are limited to flat surfaces and can be susceptible to smudge attacks [4]. Because of that, we propose interactions for authentication. An interaction could be given by turning parts of an object similar to configuring a combination lock or pressing parts of the object. For instance, 3D-printed items can already register different types of simple interactions with them, such as rotating, tilting, or squeezing [49]. Such interactions could be used as authentication sequences. Several realizations for authentication by interactions have been proposed in related work. For instance, *TangibleRubik* uses the manipulation of a Rubik's Cube as authentication interaction [41] and *bend passwords* use a flexible PVC sheet with integrated bend sensors [38]. Such interactions might be possible realizations for authentication interactions. The concept 3D-Auth proposes an interaction space of five different categories for authentication interactions that were perceived as easy-to-use by study participants [39].

5.4 Security Perceptions

In line with previous investigations [12, 18, 45, 60], our results furthermore reveal that participants consider security to be essential for 2FA mechanisms. However, the results also show that users might perceive the security of a specific 2FA mechanism to be different from the actual level of security provided. For instance, participants considered fingerprints to be highly secure, although current fingerprint sensors are susceptible to mimicking attacks since they are based on partial fingerprints only [47]. The importance of security perceptions has also been demonstrated and highlighted by related work, e.g., [12, 18, 24] showing that security perceptions of users are crucial in the scope of 2FA. Consequently, besides the actual level of security that is objectively provided by the 2FA mechanism, the perceived level of security by users should be considered when choosing or implementing 2FA mechanisms.

6 FINAL RECOMMENDATIONS AND STATE-OF-THE-ART-SOLUTIONS

Based on the results of the interview study, we first distill five recommendations for the interaction design of 2FA and four recommendations related to security. Both sets aim to enhance user experience, usability, and customization of 2FA. With these recommendations, we aim to pave a way to lower user friction when interacting with 2FA mechanisms ultimately improving the user experience of 2FA. We aim to start a transition from current solutions that are mainly used because they are mandatory or lack alternatives to user-friendly solutions that are adopted because users feel empowered by them ultimately delivering real security benefits from 2FA to the digital world. Next, we discuss to which extent state-of-the-art solutions fulfill these recommendations demonstrating the need for further investigations. Table 3 provides an overview of similar recommendations from related work that we also mentioned in the previous section.

6.1 Recommendations for Interaction Design

(1) **Enable fully mobile solutions.** Based on our study, we conclude that the mobile 2FA approaches enabling location-independence are crucial for users. If these solutions are based on mobile devices, the second authentication factor should be external from them.

Just Accepted

(2) **Provide independence from energy sources.** The second authentication factor should be completely independent of energy sources. If such independence is not possible, the device should be rechargeable with commonly used cables and plugs.
(3) **Provide network independence.** The second factor should be independent of the cellphone network and, if possible, from the Internet.
(4) **Enable integration into everyday objects.** For an ideal approach, 2FA devices or items should be integrated into everyday objects that the users can choose, such as pendants or bracelets. If such an integration is not possible, the object should fit other everyday objects, such as key rings or smart cards placed in a wallet.
(5) **Offer personalization options.** 2FA objects should be customizable. Users should be able to choose visual properties. These properties could, for instance, be colors, shapes, or even custom objects like custom jewelry.
(6) **Offer scalable solutions.** Since the ownership factor is likely to persist as the second authentication factor, 2FA solutions should be scalable to a variety of different accounts by different providers.

6.2 Recommendations for Security

(1) **Enable recovering from loss.** If the authentication mechanism is based on the possession of a specific item or TOTP, the user might lose. Hence, there should be options for the users to cope with losing information or items that are needed for successful authentication.
(2) **Consider the security perception of users.** The main purpose of 2FA is securing assets. Besides the objective security that could be analyzed by experts, it is crucial to consider the security perceptions of users.
(3) **Design for covert interaction.** 2FA objects should offer usage in a covert way, such as interactions in the pocket. If covert interactions are used, observers cannot determine whether a user currently performs an authentication-related action.
(4) **Design for discreetness.** 2FA objects should not obviously be connected to authentication. If a user does not interact with an object, an observer should not be able to determine its purpose.

Table 3. Overview of our recommendations and their connection to related work.

Recommendation	Similar Recommendations from Related Work
Fully mobile solution	2nd factor availability [45, 60]
Energy source independence	2nd factor availability [60]
Network independence	-
Everyday objects	nothing-to-carry [5], no additional token [35, 60]
Personalization	one size does not fit all [9]
Scalability	-
Loss recovery	resilient-to-loss [16]
Security perceptions	[12, 18, 45, 60, 61]
Covert interaction	resilient-to-physical-observation [5]
Discreetness	resilient-to-physical-observation [5]

6.3 Discussion of State-of-the-Art Solutions

The previous section provides six recommendations for the interaction design of 2FA. This section discusses to what extent state-of-the-art solutions fulfill these recommendations demonstrating the need for further investigations. In this discussion, we did not include security perceptions because those are highly dependent on the context and specific realization of the 2FA solution. Overall, some recommendations involve some kind of

Just Accepted

trade-off with other recommendations. Consequently, it is challenging to realize all recommendations to a similar degree when implementing a 2FA mechanism. We consider such trade-offs when discussing the state-of-the-art solutions.

Considering the first recommendation of **fully mobile solutions**, the second authentication factor should consider using alternative devices for 2FA rather than the device used for the main task Several mobile apps offer mobility. Depending on the algorithm for obtaining the OTP, apps might require access to the network to retrieve the OTP. This is also true for text messages, emails, and phone calls that are accessed from mobile phones to obtain OTPs. Timed-based OTP (TOTP) solutions generate the OTP locally on the device and do not require any network. However, those solutions do not always offer **coping with loss**[7].

In the scope of online banking, for instance, several banks provide fully mobile solutions by offering two apps – one for banking and one for 2FA. This substantially weakens security and consequently is not a viable solution if both apps are installed on the same device. ChipTAN devices are mobile and can be used in combination with a mobile device. Current realizations of chipTAN devices require **unusual batteries** that cannot be charged. Furthermore, these devices fulfill no recommendation besides mobility. The **recovery of loss** here depends on the specific device. If the device is a card reader, another device can be used as long as the user has access to the debit or smart card. **Scalability** is quite difficult with chipTAN because a smart card is required for the account. Consequently, users would need one smart card per account.

OTP lists or security cards could be used in this context and would even fulfill the recommendations considering **network** and **energy source independence**. These solutions, however, suffer from security issues since they might easily be copied or stolen and **cannot easily be recovered if lost**. If obtained by an adversary, OTP lists and security cards can directly be used to impersonate users. Furthermore, users might take pictures of the lists or cards and store them on their phones, which was reported by our participants. Finally, OTP lists and security cards do not scale well since one list or card respectively would be needed per account.

The second authentication factor could also be another technical device, such as a second smartphone or a smartwatch [37]. Depending on the specific realizations, neither smartphones nor smartwatches provide **network and energy source independence**. A state-of-the-art example for a single-purpose authentication device are Yubikeys [63], which do not require an **energy source** and are compatible with mobile devices [36]. They can be used as a key ring and thus is integrable into **everyday objects**. The device is small enough to fit in a pocket, therefore it likely offers **covert interaction**. On the flip side, the Yubikey NEO is not discreet since it is a single-purpose authentication device, it currently does not offer **personalization options** besides custom colors and **cannot be recovered if lost**. Considering **scalability**, Yubikeys are widely supported but add a single item that is used for different accounts.

Besides technical devices, several biometric features of the user, such as fingerprints, or face measurements, could be used as a second factor. Biometrics are **mobile**, do neither require **network nor energy**. Biometric features **cannot be lost**. Although the user's appearance might change over time, algorithms can adapt to that. However, once comprised, biometrics are challenging to replace. Considering scalability aspects, biometrics can be used for multiple accounts, but that would be similar to using one password among different accounts from a security perspective.

The concept 3D-Auth [39] offers authentication based on passive 3D-printed objects. They do not require **energy** or **network sources** because they are based on the principle of capacitive sensing. A secret capacitive structure embedded in the object represents the authentication factor ownership. Based on physical interactions with the object, capacitive dots in the object bottom form an authentication pattern that can be sensed by a touchscreen. 3D-Auth is hence limited to touchscreen devices. Users can choose the scope of the object but are limited to shapes that offer enough space for the conductive dots. 3D-Auth items can be **recovered in case**

[7]Several solutions provide a backup code during setup in case the device is lost.

Just Accepted

Table 4. Overview of the recommendations and their connection to state-of-the-art techniques for providing 2FA. The symbols meanings are as follows:

- = fulfills the recommendation
- = fulfills the recommendation in specific contexts/configurations
- = fulfills the recommendation, but is not resilient-to-theft
- = fulfills the recommendation, but is difficult to replace if stolen
- = fulfills the recommendation, if smartphone/tablet/PC considered as everyday object
- = fulfills the recommendation by one static item
- = can be part of a key ring or wallet
- = if used for authentication/authorization only and not for main task
- = requires batteries
- = requires Internet
- = requires cell-phone network

For the security perceptions, we list related work that investigated the mechanism if available.

			Recommendations									
			Fully mobile solution	Energy source independence	Network independence	Everyday objects	Personalization	Scalability	Covert interaction	Discreetness	Loss recovery	Security Perception
Technique	OTP-based	text message	✓	✓	✓	✓	-	✓	-	-	✓	[18, 45]
		email-based	✓	✓	✓	✓	-	✓	-	-	✓	-
		phone calls	✓	✓	✓	-	-	✓	-	-	✓	-
		chipTAN	✓	✓	✓	-	-	-	-	-	✓	[61, 64]
	Paper-based OTP	pre generated OTPs (e.g., list)	✓	✓	✓	-	-	-	-	-	-	[45]
		security card	✓	✓	✓	-	-	-	-	-	-	-
	Hardware-Token	TOTP token (e.g., Duo) [26, 50]	✓	✓	✓	✓	-	✓	-	-	-	[60]
		Yubikey [63]	✓	✓	✓	✓	✓	✓	✓	-	-	[12, 45, 60]
		Pico [52]	✓	✓	✓	✓	-	✓	-	-	-	[43]
		3D-Auth [39]	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
		RFID chip	✓	✓	✓	✓	-	✓	-	✓	-	-
	Biometric	fingerprint	✓	✓	✓	-	-	✓	-	-	N/A	[64]
		face-ID	✓	✓	✓	-	-	✓	-	✓	N/A	[64]
		voice	✓	✓	✓	-	-	✓	-	-	N/A	[64]
		iris [17]	✓	✓	✓	-	-	✓	-	✓	N/A	[64]
	Environment	sound-based [32]	✓	✓	✓	✓	-	✓	-	✓	-	-
	Smartphone-based	app: push-based	✓	✓	✓	✓	-	✓	-	-	-	[18, 45]
		app: OTP-based	✓	✓	✓	✓	-	✓	-	-	-	[18, 45]
		app: TOTP-based	✓	✓	✓	✓	-	✓	-	-	-	[45]
		app: scan-based	✓	✓	✓	✓	-	✓	-	-	-	[64]

Just Accepted

of loss if the user has access to the 3D-printing file. Considering scalability, 3D-Auth items might be used for different accounts, which in turn would result in a single item being used for multiple accounts. However, users might create different interaction-based "passwords" for each accounts using the same item.

An overview of the state-of-the-art solutions discussed above and the degree to which they fulfill our recommendations is given by Table 4. Overall, each of the discussed solutions only partially fulfills the requirements described above. Solutions that are widely used, such as chipTAN generators or tokens, have been demonstrated to be usable for individual accounts [16, 18, 36]. Such devices are already used by a variety of providers, e.g., banks. However, what currently deployed devices miss is a better integration into users' daily lives by accommodating user needs considering mobility, customization, and interaction. Fulfilling the requirements proposed by us would result in 2FA solutions that improve the integration in the users' daily lives.

6.4 Directions for Future Work

In this section, we discuss opportunities for future work.

6.4.1 Deploying Specific Solutions. Considering the personal needs of individual users, there likely is no one-size-fits-all solution for 2FA that perfectly aligns with the needs of each individual. Related work, as well as our work, also shows these aspects based on the variety of aspects that were considered by participants. Consequently, future work should consider the deployment of specific solutions that consider our recommendations. When investigating specific solutions scalability aspects are important to consider since the number of daily authentication procedures is likely to increase in the future, mechanisms should 1) be scalable to fit the number of daily authentications while 2) not weakening security, e.g., by creating single points of failure..

6.4.2 Adoption of 2FA. Our study results reveal that it can be challenging to motivate users using 2FA in domains where 2FA is not mandatory. Educational videos explaining the benefits of 2FA [3] or information messages [24] might contribute to adoption. Further related work investigated the impact of social aspects on the adoption of authentication mechanisms. Das *et al.* investigated authentication-based security of Facebook users revealing that it is more likely that users adopt more secure features if their friends use them [15]. Simple displaying that friends use the more secure feature was shown to be most effective in this context [14]. Hence, social aspects could impact the adoption of 2FA which should be investigated by future work.

6.4.3 Recovery of Loss. Many mechanisms also offer options for recovery from loss such as backup passwords or reconstruction files. However, users might even lose these backup options or do not have access to them. Hence, future work should investigate reconstruction mechanisms and means to store them securely such that 1) users have access to them when needed and 2) not weaken the security of authentication.

7 CONCLUSION

Two-factor authentication is a security mechanism used in practice to enhance the security of important accounts, e.g., in online banking. In this paper, we investigated user perceptions and expectations of different 2FA mechanisms revealing key user requirements that are not well met in state-of-the-art solutions. Our sample consisted of experienced and inexperienced 2FA users who reported their experiences, preferences, and problems using 2FA. We further investigated the second authentication factor more closely regarding possibilities for its physical realization, and properties showing that current state-of-the-art solutions integrate poorly in the users' daily lives. Based on our investigation, we provide ten final recommendations for two-factor authentication based on interaction design and security considerations from the users' perspective. Besides mere usability, our recommendations consider hedonic aspects of user experience that have the potential to motivate users to use two-factor authentication and foster its adoption even in domains in which 2FA is not mandatory. Consequently, we aim to motivate a transition from current solutions that come with a lot of user frustration to novel 2FA solutions that offer enhanced user experience and integrate better into the users' daily lives ultimately improving security in the digital world.

Just Accepted

Current state-of-the-art solutions only partially realize the recommendations. Our work can serve as a basis for several streams of future works. Specific realization possibilities that implement our requirements and recommendations form an integral part of future work. Within this scope, the security properties of the realization possibilities should be designed and investigated. Furthermore, human factors, including usability, user experience, and trust should be evaluated thoroughly since those might impact security properties like the installation of 2FA and banking apps on the same device. While our recommendation specifically targets user experience and aims to boost the adoption of 2FA - especially in contexts where 2FA is not mandatory - future work should investigate the impact of our recommendations on user experience and adoption.

ACKNOWLEDGMENTS

This research work has been funded by the Horst Görtz Foundation, by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 251805230/GRK 2050; 326979514/3DIA) and JST CREST Grant No. JPMJCR16E1 Experiential Supplements. This research was also supported, in part, by the Engineering and Physical Sciences Research Council (grant number EP/V008870/1). The authors would further like to thank Kira Bleck and Florian Krell who supported the data acquisition of the study.

REFERENCES

[1] Jacob Abbott and Sameer Patil. 2020. How Mandatory Second Factor Affects the Authentication User Experience. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376457

[2] Claudia Ziegler Acemyan, Philip Kortum, Jeffrey Xiong, and Dan S Wallach. 2018. 2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62, 1 (2018), 1141–1145. https://doi.org/10.1177/1541931218621262

[3] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *International Journal of Human–Computer Interaction* 33, 11 (2017), 927–942.

[4] Adam J. Aviv, Katherine L. Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the USENIX Workshop on Offensive Technologies (Woot, Vol. 10)*. USENIX Association, Berkeley, CA, US, 1–7.

[5] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, Piscataway, NJ, USA, 553–567. https://doi.org/10.1109/SP.2012.44

[6] Virginia Braun and Victoria Clarke. 2012. Thematic Analysis. (2012).

[7] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. 2019. Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 339–356. https://www.usenix.org/conference/soups2019/presentation/ciolino

[8] Jacob Cohen. 1960. A Coefficient of Agreement for Nominal Scales. *Educational and Psychological Measurement* 20, 1 (1960), 37–46.

[9] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. ACM, New York, NY, USA, Article 456, 11 pages. https://doi.org/10.1145/3173574.3174030

[10] European Commission. 2016. Payment Services (PSD 2) - Directive (EU) 2015/2366. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366. [Online; accessed: 22-August-2020].

[11] Alexei Czeskis and Juan Lang. 2015. Fido nfc protocol specification v1. 0. *FIDO Alliance Proposed Standard* (2015), 1–5.

[12] Sanchari Das, Andrew Dingman, and L. Jean Camp. 2018. Why Johnny Doesn't Use Two Factor a Two-Phase Usability Study of the Fido u2f Security Key. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*. Springer, Cham, Switzerland, 1–20. https://doi.org/10.1007/978-3-662-58387-6_9

[13] Sanchari Das, Andrew Kim, Ben Jelen, Joshua Streiff, L. Jean Camp, and Lesa Huber. 2020. Why Don't Older Adults Adopt Two-Factor Authentication?. In *Proceedings of the SIGCHI Workshop on Designing Interactions for the Ageing Populations - Addressing Global Challenges*. SSRN, Rochester, NY, USA, 1–5.

[14] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2014. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale,

Just Accepted

Arizona, USA) *(CCS '14)*. Association for Computing Machinery, New York, NY, USA, 739–749. https://doi.org/10.1145/2660267.2660271

[15] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 1416–1426. https://doi.org/10.1145/2675133.2675225

[16] Sanchari Das, Gianpaolo Russo, Andrew C. Dingman, Jayati Dev, Olivia Kenny, and L. Jean Camp. 2018. 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* (Orlando, Florida, USA) *(STAST '17)*. Association for Computing Machinery, New York, NY, USA, 28–39. https://doi.org/10.1145/3167996.3167997

[17] John Daugman. 2009. How Iris Recognition works. In *The Essential Guide to Image Processing*. Elsevier, 715–739.

[18] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2014. A Comparative Usability Study of Two-Factor Authentication. In *Proceedings of the Workshop on Usable Security (USEC '14)*. Internet Society, Reston, VA, USA, 10 pages. https://doi.org/10.14722/usec.2014.23025

[19] J. Dutson, D. Allen, D. Eggett, and K. Seamons. 2019. Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. In *Proceedings of IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. IEEE, Piscataway, NJ, USA, 119–128.

[20] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 4254–4265. https://doi.org/10.1145/3025453.3025636

[21] Habiba Farzand, Kinshuk Bhardwaj, Karola Marky, and Mohamed Khamis. 2021. The Interplay between Personal Relationships & Shoulder Surfing Mitigation. In *Proceedings of the Mensch und Computer 2021 (MuC '21)*.

[22] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human-Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150 arXiv:https://doi.org/10.1080/10447318.2018.1456150

[23] S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel. 2020. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *Proceeedings of the IEEE Symposium on Security and Privacy (SP)*. IEEE, Piscataway, NJ, USA, 268–285.

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

[25] Paul A. Grassi, James L. Fenton, and Michael E. Garcia. 2017. *Digital Identity Guidelines [Including Updates as of 12-01-2017]*. Technical Report. NIST Special Publication 800-63-3.

[26] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking. *Computers & Security* 30, 4 (2011), 208–220.

[27] Cormac Herley and Paul Van Oorschot. 2011. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy* 10, 1 (2011), 28–36.

[28] Auth0 Inc. 2021. OAuth 2 Standard Documentation. https://auth0.com/docs/ (accessed 31-Oxtober-2021).

[29] Philip G. Inglesant and M. Angela Sasse. 2010. 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)*. ACM, New York, NY, USA, 383–392.

[30] Iulia Ion, Marc Langheinrich, Ponnurangam Kumaraguru, and Srdjan Čapkun. 2010. Influence of user perception, security needs, and social factors on device pairing method choices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS 2010)*. USENIX Association, Berkeley, CA, US, 1–13.

[31] Devriş İşler, Alptekin Küpçü, and Aykut Coskun. 2019. User Perceptions of Security and Usability of Mobile-Based Single Password Authentication and Two-Factor Authentication. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, Cham, Switzerland, 99–117.

[32] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. 2015. Sound-Proof: Usable Two-factor Authentication Based on Ambient Sound. In *Proceedings of the USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Berkeley, CA, US, 483–498.

[33] Christina Katsini, Yasmeen Abdrabou, George E. Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–21. https://doi.org/10.1145/3313831.3376840

[34] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Augmented Reality-Based Mimicry Attacks on Behaviour-Based Smartphone Authentication. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services* (Munich, Germany) *(MobiSys '18)*. Association for Computing Machinery, New York, NY, USA, 41–53. https://doi.org/10.1145/3210240.3210317

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

Just Accepted

Internet Society, Reston, VA, USA. https://doi.org/10.14722/usec.2015.23001

[36] Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas. 2016. Security Keys: Practical Cryptographic Second Factors for the Modern Web. In *International Conference on Financial Cryptography and Data Security*. Springer, Cham, Switzerland, 422–440.

[37] Wei-Han Lee and Ruby Lee. 2016. Implicit Sensor-Based Authentication of Smartphone Users with Smartwatch. In *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016* (Seoul, Republic of Korea) *(HASP 2016)*. Association for Computing Machinery, New York, NY, USA, Article 9, 8 pages. https://doi.org/10.1145/2948618.2948627

[38] Sana Maqsood, Sonia Chiasson, and Audrey Girouard. 2016. Bend Passwords: Using Gestures to Authenticate on Flexible Devices. *Personal Ubiquitous Comput.* 20, 4 (Aug. 2016), 573–600. https://doi.org/10.1007/s00779-016-0928-6

[39] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 2020. 3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376189

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

[41] Martez Mott, Thomas Donahue, G. Michael Poor, and Laura Leventhal. 2012. Leveraging Motor Learning for a Tangible Password System. In *Extended Abstracts of the CHI conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI EA '12)*. ACM, New York, NY, USA, 2597–2602. https://doi.org/10.1145/2212776.2223842

[42] Lawrence O'Gorman. 2003. Comparing Passwords, Tokens, and Biometrics for User Authentication. *Proc. IEEE* 91, 12 (2003), 2021–2040. https://doi.org/10.1109/JPROC.2003.819611

[43] Jeunese Payne, Graeme Jenkinson, Frank Stajano, M. Angela Sasse, and Spencer Max. 2016. Responsibility and Tangible Security: Towards a Theory of User Acceptance of Security Tokens. In *Proceedings of the Workshop on Usable Security (USEC '16)*. Internet Society, Reston, VA, USA, 10 pages. https://doi.org/10.14722/USEC.2016.23003

[44] Ahmad R. Pratama and Firman M. Firmansyah. 2021. Until you have something to lose! Loss aversion and two-factor authentication adoption. *Applied Computing and Informatics* (2021).

[45] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A usability study of five two-factor authentication methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Berkeley, CA, US.

[46] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. 2018. A tale of two studies: The best and worst of yubikey usability. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*. IEEE, Piscataway, NJ, USA, 872–888.

[47] Aditi Roy, Nasir Memon, and Arun Ross. 2017. MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems. *IEEE Transactions on Information Forensics and Security* 12, 9 (2017), 2013–2025. https://doi.org/10.1109/TIFS.2017.2691658

[48] M. Angela Sasse, Charles C. Palmer, Markus Jakobsson, Sunny Consolvo, Rick Wash, and L. Jean Camp. 2014. Helping You Protect You. *IEEE Security & Privacy* 12, 1 (2014), 39–42.

[49] Martin Schmitz, Martin Herbers, Niloofar Dezfuli, Sebastian Günther, and Max Mühlhäuser. 2018. Off-Line Sensing: Memorizing Interactions in Passive 3D-Printed Objects. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. ACM, New York, NY, USA, Article 182, 8 pages. https://doi.org/10.1145/3173574.3173756

[50] DUO Security. 2019. Security Tokens. https://duo.com/product/trusted-users/two-factor-authentication/authentication-methods/security-tokens. [Online; accessed: 22-August-2020].

[51] Michael Sherman, Gradeigh Clark, Yulong Yang, Shridatt Sugrim, Arttu Modig, Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. 2014. User-Generated Free-Form Gestures for Authentication: Security and Memorability. In *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services* (Bretton Woods, New Hampshire, USA) *(MobiSys '14)*. Association for Computing Machinery, New York, NY, USA, 176–189. https://doi.org/10.1145/2594368.2594375

[52] Frank Stajano. 2011. Pico: No More Passwords!. In *Proceedings of the International Workshop on Security Protocols*. Cham, Switzerland, 49–81. https://doi.org/10.1007/978-3-642-25867-1_6

[53] Statista. 2018. Cybersecurity & Cloud 2018. https://de.statista.com/statistik/studie/id/58204/dokument/cybersecurity-und-cloud/ (accessed 1-September-2020).

[54] Elizabeth Stobert and Robert Biddle. 2014. The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 243–255.

[55] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. A Comparison of Perceived and Real Shoulder-Surfing Risks Between Alphanumeric and Graphical Passwords. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 56–66.

[56] Christian Tiefenau, Maximilian Häring, Mohamed Khamis, and Emanuel von Zezschwitz. 2019. " Please enter your PIN"–On the Risk of Bypass Attacks on Biometric Authentication on Mobile Devices. *arXiv preprint arXiv:1911.07692* (2019).

Just Accepted

[57] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 123–140.
[58] Guilin Wang, Jiangshan Yu, and Qi Xie. 2012. Security analysis of a single sign-on mechanism for distributed computer networks. *IEEE Transactions on Industrial Informatics* 9, 1 (2012), 294–302.
[59] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding Password Choices: How Frequently Entered Passwords Are Re-used Across Websites. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 175–188.
[60] Jake Weidman and Jens Grossklags. 2017. I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. In *Proceedings of the Annual Computer Security Applications Conference* (Orlando, FL, USA) *(ACSAC 2017)*. ACM, New York, NY, USA, 212–224. https://doi.org/10.1145/3134600.3134629
[61] Catherine S. Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. 2009. User Perceptions of Security, Convenience and Usability for Ebanking Authentication Tokens. *Computers & Security* 28, 1-2 (2009), 47–62. https://doi.org/10.1016/j.cose.2008.09.008
[62] Catherine S. Weir, Gary Douglas, Tim Richardson, and Mervyn Jack. 2009. Usable Security: User Preferences for Authentication Methods in eBanking and the Effects of Experience. *Interacting with Computers* 22, 3 (2009), 153–164.
[63] Yubico. 2019. YubiKey NEO. https://support.yubico.com/support/solutions/articles/15000006494-yubikey-neo. [Online; accessed: 22-August-2020].
[64] Verena Zimmermann and Nina Gerber. 2017. "If It Wasn't Secure, They Would Not Use It in the Movies"–Security Perceptions and User Acceptance of Authentication Technologies. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 265–283.
[65] Verena Zimmermann and Nina Gerber. 2020. The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies* 133 (2020), 26–44.
[66] Verena Zimmermann, Nina Gerber, Peter Mayer, Marius Kleboth, Alexandra von Preuschen, and Konstantin Schmidt. 2019. Keep on rating–on the systematic rating and comparison of authentication schemes. *Information & Computer Security* 27, 5 (2019), 621–635. https://doi.org/10.1108/ICS-01-2019-0020

Just Accepted

A APPENDIX

In this section, we provide the interview guide for our study and the codebook used during analysis.

A.1 Interview Guide

(1) Welcome and Consent
- Welcome to our interview study. The interview is part of a research project about authentication. We will talk about your experiences with different authentication mechanisms. Your participation in the study is voluntary and the study can be aborted at any time, I do not need to know any reason for this. The data collected until then will be destroyed. There will be no negative consequences for you. The interview is audio-recorded. Before the analysis, the audio file will be transcribed. If case you mention any information that could be used to establish a link to your identity, we remove this information during transcription and replace it by neutral placeholders.
- I would ask you to read this information sheet about the interview. If there are any questions, please let me know.
- **Action:** Provide link to information sheet, participant provides signed PDF.
- Thanks for the consent form. We will now proceed with the interview. I will always explicitly tell you when I start or stop the audio recording.
- **Action:** Start recording
- I start the recording. Do you agree with the recording? If so, please tell me.

(2) Familiarization
- There are several ways to log into online banking accounts and approve transactions. In the first part of the study, I would like to go through three possibilities with you. For this, I will briefly share my screen

with you so that I can show you a presentation. We will talk about these three possibilities but also about other authentication mechanisms that you have used.
- **Action:** Presentation of three approaches detailed in Section 2 in counterbalanced random order. The participants saw a presentation that was presented by screen-sharing.
- Do you have any questions about the approaches that you have just seen?

(3) Experiences I
- We now start the interview, we are interested in your personal opinion such that we can make authentication better. Hence, there are no wrong answers.
- I have just shown three authentication mechanisms for online banking, now I would like to know a bit more about your opinion on them.
- Have you ever used any of these authentication mechanisms for your online banking or others? Which one(s) have you used? (If another mechanism is mentioned the participant is asked to describe it).
- **Action:** For each mechanism, ask:
  - What is your opinion about this mechanism?
  - Was there anything you liked about using it? Was there anything you didn't like about using it?
  - Has anything gone wrong in the past when using the mechanism?
  - (If the participant has used it in the past) Why don't you use the mechanism anymore? Are there any specific reasons for that?

(4) Preferences
- Suppose you could choose any of the three presented mechanisms for online banking, which one would you like to use? Can you explain why you would choose this mechanism? What are the reasons for not using the other mechanisms?
- The three presented mechanisms are not the only options for authentication. If you had a free choice, which would you prefer to use? Please explain why?

(5) Experiences II
- In some countries, users of online banking must use two factors for authentication, it is required by law. Often, this is a password or PIN in combination with a freshly generated transaction number - this is called two-factor authentication. The reason for this is that the second factor increases security. There are different options for the second factor, it can be the apps that we looked at earlier, but there are also other devices that look similar to a calculator. (Participant can also ask questions about 2FA, the examiner made sure that participants understood what 2FA is).
- Have you used this type of authentication before?
- What have you used it for? (Online Banking, something else)
- What are your experiences with it?
- Was there anything you liked about using it? Was there anything you didn't like about using it?
- Has anything gone wrong while using 2FA in the past?
- (If someone does not use 2FA at all) Why not?

(6) Second Factor
- As mentioned earlier, using 2FA requires two authentication factors. If you had a free choice of how the second factor is designed, what would you like to use?
- What characteristics do you think the second factor should have? (ask for reasons in each case)
- Is there anything design-related that a second factor should have?

(7) Closing
- Do you have any other comments or suggestions for us?
- I stop the recording
- **Action:** Stop recording

Just Accepted

- I have sent you a link to a questionnaire in the chat. Please, fill out the questionnaire and let me know once you are done.
- Thanks for your participation.

Just Accepted

B CODEBOOK

In this section, we provide the codebook used during the interview analysis.

Just Accepted

Category	Code	Description
Experiences	banking_push	Usage of push approach for banking
	banking_scan	Usage of push approach for banking
	banking_textmessage	Usage of text messages for banking
	banking_securitycard	Usage of security card for banking
	banking_email	Usage of e-mails for banking
	banking_other	Usage of an approach for banking
	other_financial	2FA used for other financial transactions (e.g., PayPal)
	other_gaming	2FA used for gaming
	other_onlineservices	2FA used for online services
	other_devices	2FA used for devices
Preferences	ease_of_use	The mechanism is easy to use
	complexity	The mechanism is complex
	availability	The mechanism is available for the participant (e.g., free, based on already owned devices)
	security	The mechanism seems secure
	no_password	Preference of alternatives to passwords
	personal_dislike	Participant does not like 2FA in general
Problems	network_unavailable	The network was not available
	energy_issue	The 2FA device ran out of energy
	technical_issue	Component required for 2FA did not work (e.g., phone camera)
	security_issue	User mentions security issue (e.g., giving OTP list to other person)
	lost_item	An item required for 2FA was lost (e.g., OTP generator)
	resource_issues	Resources required for 2FA are too high (e.g., time)
2nd Factor	usability	The second factor should be easy-to-use
	mobility	Usage of second factor should be location-independent
	connectivity	no network connection required for second factor
	energy_sources	second factor should not rely on energy sources or be chargeable with standard chargers
	security	second factor should offer secure interaction
	interaction	An interaction mentioned by the participant
	interaction_secret	interaction should not be observable by other
	no_new_device	Devices for 2FA should already by in possession of the user
	everyday_device	Devices for 2FA should not be obvious, 2FA should be integrated in everyday items
	customization	Devices for 2FA should be customizable (e.g., forms, colors, location)

Table 5. Codebook used to analyze the interviews.

Just Accepted