Authentication Inconsistencies Across Online Services: A Multi-Scenario Security Analysis

Andre Büttner[1(✉)], Nils Gruschka[1], Sverre Stafsengen Broen[1], and Daniela Pöhn[2]

[1] University of Oslo, Gaustadalléen 23B, 0373 Oslo, Norway
{andrbut,nilsgrus}@ifi.uio.no
s.s.broen@usit.uio.no
[2] Universität der Bundeswehr München, RI CODE, Werner-Heisenberg-Weg 39, 85579 Neubiberg, Germany
daniela.poehn@unibw.de

Abstract. Online services are integral to modern life, supporting activities such as communication, commerce, and travel. These services typically require user authentication, traditionally relying on user ID and password combinations. However, this approach is increasingly vulnerable to attacks such as phishing. Many services have adopted stronger authentication mechanisms, including multi-factor authentication, risk-based authentication, and passkeys.
Despite extensive research on login procedures, limited attention has been given to these post-login authentication processes. This paper presents a first study investigating the interplay between multi-factor authentication and context-specific authentication for ten popular online services. The results indicate that various authentication methods and behaviors can be observed across different scenarios and services.

Keywords: Online services · multi-factor authentication · authentication · security.

1 Introduction

Online services have become an essential part of our daily lives. Many aspects, such as communication, social networking, shopping, banking, or travel planning, are nearly unthinkable without mobile apps or online services. Most services require creating an account, including exchanging authentication credentials to identify ourselves when revisiting the services.

Traditionally, authentication to online services was done by logging in with a user ID (often an email address) and a shared secret (typically a password). However, attacks on this scheme have become increasingly frequent and sophisticated [31]. Widespread examples are email phishing [16] and credential stuffing attacks using leaked password lists [23]. In response to these threats, many online services have implemented additional security measures, such as second- or multi-factor authentication (2FA, MFA), risk-based authentication (RBA), or passkey authentication [15]. While these measures can increase security and

Paper presented and published at EDId '25.
This version of the contribution has been accepted for publication, after peer review (when applicable) but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections.
The Version of Record is available online at: http://dx.doi.org/10.1007/978-3-032-00639-4_10.

avoid account takeover attacks, they can also reduce usability for the end-user and even lead to account lockout, i.e., the legitimate user losing access to their account [26].

Another observation is that many online services not only request identity proofs during the login procedure. Also, when performing certain operations, e.g., changing security settings or requesting their data, users must often provide additional evidence of their identity, even if they are already logged in to the service. While users might feel annoyed by such recurring requests, it can increase the security and mitigate, for example, session stealing attacks. Similar behavior is known from continuous authentication systems [4].

While service login procedures and their different characteristics (i.e., simple password, multi-factor, and risk-based) are widely studied, research on online services' authentication outside the login procedure is sparse. Therefore, this paper presents a study on the holistic authentication behavior (i.e., during login and specific usage contexts) of ten selected online services. The main contributions are as follows:

- We analyze how authentication features vary across usage scenarios and services.
- We identify inconsistencies in how 2FA affects trust in logged-in users.
- We discuss the security implications of the observed authentication features.

The remainder of this paper is organized as follows: We first highlight the importance of this study by summarizing related work in Section 2. In Section 3, we outline the methodology before presenting the experiment results in Section 4. Finally, we discuss the experiment and results and conclude our paper in Sections 5 and 6, respectively.

2 Related Work

Different authentication aspects of online services have been studied extensively. For instance, Klivan et al. [18] and Amft et al. [3] both investigated the security and user experience for MFA recovery procedures. The authors show that many websites deploy insecure MFA recovery procedures, where MFA can be disabled when having access to the accounts' associated email addresses. Moreover, Büttner and Gruschka [11] evaluated the security and lockout risks of MFA and recovery settings for Google and Apple users. Tiefenau et al. [30] conducted interviews and a survey to understand the user perception of 2FA recovery. The authors show that users often rely on website support to regain access.

Furthermore, several studies have investigated RBA. Since online services tend not to publish their RBA configuration, reverse engineering is one way to identify involved features, like fingerprints and IP geolocation. Freeman et al. [14], Makowski and Pöhn [22], and Wiefling et al. [33] tried to shed light on the characteristics of RBA and its configuration by blackbox testing, among others. Büttner et al. [10] show that RBA may also play a role in account recovery. Based on the results, the authors create a first maturity model for RBA recovery

challenges. Pöhn et al. [26] proposed a framework to analyze authentication risks in single accounts and account networks. However, the authors did not analyze the interplay between the different factors.

When it comes to specific usage scenarios, past research has so far only focused on one specific scenario each. Boniface et al. [7], for example, analyzed the verification of the subject of data subject access rights. The authors observed some unsafe or doubtful procedures, including the copy of a national identity card transmitted over an insecure channel. Di Martino et al. [12] conducted a longitudinal study to examine whether or not services improved their policies for identifying data subjects during a subject access request (SAR). Their results showed an increase in vulnerable organizations from 27% to 30% over a two-year span, along with indicating the inconsistencies in how organizations handle the identification process of a SAR.

In a thesis written by Broen [8], experiments were conducted on the mechanisms used by services to authenticate the user when exercising one's right to access data according to Art. 15 of the European General Data Protection Regulation (GDPR) [29]. The thesis found that the authentication methods differed for the selected services, along with some requiring additional verification of the data subject to be able to exercise their rights.

The related work shows that most research focuses on authentication methods for login procedures and account recovery. However, there is a lack of studies on authentication requests outside these two scenarios. This paper studies online services' overall authentication behavior. It will focus on the distinction between different services and scenarios and the influence of MFA.

3 Methodology

Online users may encounter various scenarios where an online service requires different levels of confidence about their authenticity. Such scenarios can include, for example, modifying sensitive account settings, accessing personal information, or recovering an account. Thus, we are interested in understanding how online services actually implement authentication for such scenarios. In this regard, we aim to answer the following research questions:

- **RQ1** How do authentication methods differ across different usage scenarios?
- **RQ2** How do authentication methods differ across various online services?
- **RQ3** How does 2FA influence the authentication methods beyond the login?

To address these questions, we conducted an exploratory study [13] in which we systematically tested different online services. For this, we first selected a set of online services as our test sample. Next, we executed specific usage scenarios and documented the authentication methods required to verify the user, respectively. Finally, we analyzed the results focusing on the above-mentioned research questions.

Table 1. Overview of selected services for the study

Service	URL
Amazon	`https://amazon.com`
ChatGPT	`https://chatgpt.com`
Facebook	`https://facebook.com`
GitHub	`https://github.com`
Google	`https://google.com`
LinkedIn	`https://linkedin.com`
Microsoft Outlook	`https://live.com`
Pinterest	`https://pinterest.com`
Spotify	`https://spotify.com`
X (formerly Twitter)	`https://x.com`

3.1 Selecting Services

Given the need to conduct the experiments manually, we had to select a smaller sample of online services for our experiments. We first narrowed down the choice of services to the most popular ones by cross-referencing the top 1000 popular services of three widely used website rankings. This includes the Tranco Top Sites [20], Majestic Million[3], and Chrome (CrUX) Top Million Websites[4], which have proven to be appropriate sources for selecting relevant services [27].

The list was further reduced by excluding services requiring payment information, adult content, or those without English language support. Moreover, we removed services where an online account is not a key consumer feature or is mainly used by administrators or content creators. From the resulting list, we selected the ten services shown in Table 1.

3.2 Scenarios

For our study, we considered different account usage scenarios in which we assumed the user's authenticity to be relevant. We therefore decided to test the following six specific scenarios, labeled S1 through S6. The scenarios are described below in more detail.

S1: Login The login is the most common scenario in which a user must authenticate. It is typically the first point of interaction with an online account. Hence, a successful login is crucial for performing any further operations related to this account.

S2: Modify Email Address For most online services, the email address is essential to verify a user's identity. We therefore investigated whether modifying

[3] https://majestic.com/reports/majestic-million (Last accessed: 2025-02-11)
[4] https://github.com/zakird/crux-top-lists (Last accessed: 2025-02-11)

the email address yields any different or additional authentication compared to the regular login. Depending on the service, we either added secondary email addresses or, if this was not possible, modified the primary email address. In both cases, the service eventually accepts a different email address to verify a user than the email initially registered.

S3: Toggle 2FA Setting Online services nowadays usually offer 2FA for additional protection of online accounts. In addition to using a password, a user can set up one or several additional authentication factors. This typically includes a one-time password (OTP) app, phone number, or a security key. Within our experiments, we tested this scenario by first setting up an OTP app as 2FA method and later disabling 2FA. In one instance, we had to set up a phone number as a second factor because short message service (SMS) OTP was the only 2FA method offered.

S4: Change Name We further considered modifying personal information as an interesting use case. It is not directly connected to user authentication and, thereby, presumably the least critical compared to the other scenarios. It is still possible that changing personal information in a user account is treated differently by online services. We tested this by modifying the full name (i.e., not the username) in the user's profile where possible.

S5: Right of Access Request Another action that may be performed to gain access to an online account or some of its data is a *Right of Access* request. Online services must enable citizens of countries that are subject to EU law (and thus to the GDPR [29]) to exercise their data subject rights. Since this is often implemented as a specific function, it can present a different way of accessing an account owner's information. In practice, this typically involves two distinct phases [25]. First, a user requests the service to create a data archive with some or all of the user's data. Then, after a certain time period, the user is notified when the data is available for download. Since both phases are somewhat isolated, we split this scenario into the following two sub-scenarios: S5.1 Data Request and S5.2 Data Access.

Note that the Right of Access can often also be exercised through other channels, e.g., sending a request via email. However, we decided to focus on data requests directly through the account and refer the reader to previous works investigating other methods for requesting data [7,12].

S6: Password Reset The last scenario we included was resetting the password. When users lose their login credentials, they can usually regain access to their account through fallback authentication methods. Consequently, methods for a password reset differ from those for regular login. The challenge here is to ensure a legitimate user can regain access while preventing attackers from exploiting this to bypass authentication.

3.3 Study Procedure

We initially set up a test account for each service with a minimal configuration, i.e., with an email address and a password. Since we were also interested in testing whether 2FA has any effect on the scenarios (see RQ3), we compared authentication for each scenario with two different authentication settings. In one setting, the account was configured only with a password; in the other, 2FA was enabled. In the latter case, we used an OTP app where possible, as this did not require us to disclose unnecessary personal information. Thus, the scenarios were conducted twice with different 2FA configurations. For comparability reasons, we utilized the same browser, in our case Firefox, in a private browser mode for each scenario.

We made some exceptions concerning the scenarios and 2FA configuration due to certain limitations of some services. On ChatGPT, we had to omit scenarios S2 and S4 because there was no way to add or change an email address, and no personal information was stored in the user's profile. GitHub started enforcing 2FA in 2023 [24], and it was thus not possible to turn off 2FA once enabled. Moreover, Spotify did not offer 2FA for consumer accounts at the time of the study [28]. We consequently tested this service only with a password-based configuration. Finally, Pinterest only offered SMS OTP as a 2FA method. Therefore, we used SMS OTP instead of an OTP app.

4 Experiment Results

The experiments described in the previous section were carried out during March and April 2025. Table 2 provides a complete summary of what authentication methods were observed with respect to the different services and scenarios. In the remainder of this section, we point out important findings with regard to our research questions. We also describe some observations we made beyond this.

4.1 Comparison of Scenarios (RQ1)

The experiments show that our tested scenarios required different authentication methods. In particular, they were often inconsistent across different services.

Modifying the email address appears to be considered a rather sensitive scenario. This was indicated by requesting additional authentication steps upon the initial login. Many services required a logged-in user to re-enter the password or verify a previously registered email address before a new one can be set up.

Similarly, the 2FA setting often triggered an elevated authentication procedure. On half of the selected services, changing the 2FA configuration required entering the password again, verifying the email address, or both, before setting up the 2FA method.

In nearly all cases, the scenario of changing the user's name did not involve any additional authentication methods when the user was already logged in. Only X required re-entering the additional password.

Table 2. Overview of authentication methods required for each service and scenario. For each service, the first row shows the results for a password-only configuration and the second row for the 2FA configuration. Note that Spotify could only be tested with a password.

Service	S1	S2	S3	S4	S5.1	S5.2	S6
Amazon	P	L,EO_{new},P	L,A	L	L,EL	L,EO	EO
	P,A	=	L,EO	=	=	=	=
ChatGPT	P	-	L,A	-	L	EL,L	EO
	P,A	-	L	-	=	=	=
Facebook	P	L,EO_{old},EO_{new}	L,EO,A	L	L	L	EO
	P,A	=	L,EO	=	=	=	EO,A
GitHub	P	L,EL_{new}	L,A	L	L	L,EL	EL
	P,A	=	-	=	=	=	EL,A
Google	P	L,EO_{new}	L,A	L	L	L	EO
	P,A	L,A,EO_{new}	=	=	=	=	EO,A
LinkedIn	P	L,EO_{old},EO_{new}	L,EO,P,A	L	L	L	EO
	P,A	=	L,EO,P	=	=	=	EO,A
Microsoft	P	L,EO_{old},EO_{new}	L,EO,A	L	L,EO	L,EO	EO
	P,A	L,EO_{new}	L	=	L	L	EO,A
Pinterest	P	L,EO_{new}	L,P,S	L	L	EL,EO	EL
	P,S	=	L,P	=	=	=	=
Spotify	P|EO	L,P,EL_{new}	-	L	L,EL	EL,L	EL
X	P	L,P,P,EO_{new}	L,P,A	L,P	L,EO	L,EO	EO
	P,A	=	L,P	=	L,P,EO	L,P,EO	EO,A

P: Password; EL: Email Link; EO: Email OTP; A: App OTP; S: SMS OTP; L: Login; *a*,*b*: *a* and *b*; *a*|*b*: *a* or *b*; =: Same as above; -: Not applicable

Regarding the Right of Access scenario, we found that only four services requested additional user verification to request the data. However, six of the services required signing in and verifying the email. A special case was Pinterest, where the data request was sent through the account settings. Yet, the data was ultimately provided by a third-party service[5] that verified the email without requiring the user to be logged in to their Pinterest account.

Resetting the password did not inherently require a login and is therefore different from the other scenarios. It is an ongoing problem to design account recovery in a way that helps users when losing an authentication factor while not creating a backdoor [21]. All services in our test sample allowed resetting the password by verifying the email address. When a 2FA method was configured, many of the services required verifying both the email address and the 2FA

[5] https://pinterest.sendsafely.com (Last accessed: 2025-05-04)

Table 3. Summary of features and patterns observed on the tested services.

Service	Re-Enter Password	Verify Old Email	Email OTP	Email Link	Enter Email	2FA Backup Code
Amazon	○	○	●	●	○	○
ChatGPT	○	○	●	●	○	●
Facebook	○	●	●	○	○	●
GitHub	○	○	○	●	○	●
Google	○	○	●	○	○	●
LinkedIn	●	●	●	○	○	○
Microsoft	○	●	●	○	●	●
Pinterest	○	○	●	●	○	●
Spotify	●	○	●	●	○	-
X	●	○	●	○	○	●

●: Feature present; ○: Feature not present

method (or backup code when available). However, three services still did not require 2FA even when enabled in the account settings.

To summarize our findings for RQ1, the configuration of email addresses and 2FA settings always required additional steps and were thus the most protected among our test scenarios. In contrast, changing personal information has turned out to be the least critical scenario, as it mostly required nothing more than the initial login. The Right of Access request on several services required additional steps, especially when accessing the data. Resetting the password always relied on verifying the email address, and in most cases, the 2FA method, when enabled.

4.2 Comparison of Services (RQ2)

We further compared the services' approaches to verifying the user in the tested scenarios. In particular, some behavioral patterns were observed on several services, which are shown in Table 3 and further described in the following.

A pattern found on several services was that the password had to be re-entered when accessing and modifying specific account settings. This was observed on LinkedIn, Spotify, and X. The latter used it extensively, as it repeatedly requested the password in all scenarios except for the password reset. Remarkably, when changing the email address on X, one had to enter the password three times in total.

Specifically, when modifying the email address, all services verified the newly configured email address. However, only a few services, including Facebook, LinkedIn, and Microsoft, verified the previously set-up email address before allowing the configuration of a new or additional one.

Table 4. This table shows in which scenarios the authentication procedure differed depending on whether 2FA was enabled. (S1 is omitted as it is trivial, and Spotify is not listed since it did not offer 2FA.)

Service	S2	S3	S4	S5.1	S5.2	S6
Amazon	○	●	○	○	○	○
ChatGPT	-	●	-	○	○	○
Facebook	○	●	○	○	○	●
GitHub	○	-	○	○	○	●
Google	●	○	○	○	○	●
LinkedIn	○	●	○	○	○	●
Microsoft	●	●	○	●	●	●
Pinterest	○	●	○	○	○	○
X	○	●	○	●	●	●

●: Difference; ○: No difference; -: Not applicable

In our experiments, we mainly documented the default authentication method offered, since the alternative—typically verifying an email address—is normally the same as a password reset. However, unlike other services, Spotify requested an email OTP as the default authentication method instead of a password. In this regard, another interesting observation was that some services, including Amazon, ChatGPT, Pinterest, and Spotify, use both email links and OTPs depending on the scenario.

Beyond this, Microsoft stood out by prompting the user to enter the email address before sending an email OTP. Microsoft thereby challenges the user by requiring knowledge of an email address configured for email verification. Using this consistently was not observed on any of the other services.

Finally, as this is highly relevant for recovering accounts with 2FA support, we further noted whether the online services offered a 2FA backup code. Two services, Amazon and LinkedIn, did not offer such a backup code.

4.3 Influence of 2FA (RQ3)

The standard behavior of an account with 2FA enabled is that the regular login requires a password and the second authentication factor, i.e., the app OTP or SMS OTP. Furthermore, the user could use a backup code if the second authentication factor was unavailable, provided the online service offers this. However, as shown in Table 4, we observed that having 2FA enabled or disabled still influenced whether some services request additional verification methods or what recovery methods they require.

Microsoft behaved uniquely in comparison to the other services. We found that it treats a user signed in with 2FA with higher confidence. This is shown by

the fact that it relaxed the requirement for additional email verification in all scenarios, where otherwise an email OTP was requested. In contrast, three services showed a somewhat opposite behavior in that they required more authentication steps in at least one scenario when logged with 2FA. Amazon required an additional email OTP when disabling the 2FA method. Google requested the app OTP again when modifying the email address and disabling 2FA. On X, this occurred in the Right of Access scenario, which required re-entering a password only when 2FA was enabled.

Aside from the above-mentioned cases of Amazon and Google, the only difference when toggling the 2FA method was that it could be disabled without verifying the second factor.

The Right of Access request was not affected by 2FA in almost all cases, except for X, as mentioned above. However, it is important to note that accessing the data from Pinterest does not even require the 2FA at all, as it is handled by a third-party service that only verifies the email address.

When it comes to the password reset, the 2FA setting did affect six of nine services because the 2FA method was required in addition to verifying the email address. In turn, this means that three services, including Amazon, ChatGPT, and Pinterest, allow a password reset without having the 2FA factor. Importantly, a password reset does not imply regaining access to an account. Even when the password could be reset without the second factor, it would not allow bypassing 2FA during the subsequent login.

4.4 Additional Findings

We also want to point out some additional findings that were not the main focus but are still relevant regarding account security and suggest directions for potential future research.

We noticed that some services limited the frequency of changing information. X and Facebook, for instance, temporarily restricted the possibility of modifying email addresses or authentication methods for a certain time period. X also blocked access to the Right of Access data in some instances. However, it was unclear what caused X to do so.

Another measure often implemented by online services is a CAPTCHA [1]. We did not include this in our main results, as it does not verify a user, which was our main scope. However, it is still a security measure used to block automated attacks. Within our experiments, it only occurred in two concrete cases. Microsoft requested it when changing the user's full name, and GitHub requested a CAPTCHA during account recovery. It was therefore rather surprising that we could not observe CAPTCHAs consistently on more services and scenarios.

Although analyzing risk-based features was not the primary focus of our study, we highlight several relevant observations in this context. Many of the online services applied RBA primarily during the regular login. We further confirmed the occurrence of a risk-based behavior on Amazon during account recovery, which was already suggested by Büttner et al. [10]. However, while they

only observed a CAPTCHA as an additional authentication step, we found that Amazon would add a security question.

5 Discussion

5.1 Security Impact

Online services nowadays use strong measures to protect their users. We have particularly looked into scenarios where a user needs to log in before taking any further actions, making it challenging for an attacker to access the account settings in the first place. However, when an account is only protected by a password, the difficulty to bypass the login can be rather low due to the risk of credential stuffing and phishing [16,23]. While 2FA can prevent this, more sophisticated attacks like session stealing [9] or cross-site request forgery [5] may still pose a risk. This, therefore, demands stronger measures, such as additional authentication steps.

Overall, we observed that the services we tested offered elevated authentication mechanisms. A remarkable observation was that Microsoft requested fewer authentication steps when a user was signed in using 2FA. Given the risks mentioned above, and also considering that changing email or 2FA settings affects authentication significantly, it could be argued that requesting additional methods independently of the initial login would be better for the protection of the user. However, the opposite approach of requesting more methods, as done by Google and X, may be disadvantageous in terms of usability.

Also, we noticed some of the additional authentication steps used by the tested services are further debatable concerning the user's security. In particular, it is questionable how re-entering a password or entering an email address before verifying the respective email can truly improve security. Moreover, the usage of two email verification variants, email OTP or link, has been observed. In some instances, both were used by the same service. Both have their advantages and disadvantages. Email OTP is, for example, vulnerable to phishing, but also has a short lifetime, while an email link is not vulnerable to phishing, but has a longer lifetime. Generally, using email authentication is a controversial topic since email accounts are often the main weakness in user account settings [19,21,17].

Likewise, the dedicated use of CAPTCHAs is rather questionable. Particularly in the case of Microsoft, it is not clear why it is critical to prevent automated attacks when changing a user's name compared to other scenarios.

On the positive side, we noticed that a password reset could not be exploited to bypass 2FA. The second factor was required during the password reset or subsequent login. In any case, one could not avoid 2FA. Most services, except for Amazon and LinkedIn, also offered a 2FA backup code. Yet, this does not guarantee that a user has stored it or noted it down. This therefore creates a significant usability compromise, as also noted by similar research on this [3].

5.2 Ethics

Online services may prohibit users from employing pseudonymized or test accounts for research. Respective rights may overrule such terms, depending on the country and decisions [32]. In this regard, the American Psychological Association and the German equivalent declare that no studies based on deception are to be carried out unless deception techniques are justified by, e.g., a significant gain in scientific knowledge, and no alternative procedure is possible [2,6]. In our case, we used only our own accounts and avoided any interactions with non-study users. Thereby, we largely eliminated the risk of deceit. Additionally, we did not create significant web traffic or server load that would affect other users, nor did we exploit specific vulnerabilities. This procedure can be seen as justifiable, as new knowledge is gained.

5.3 Limitations

We conducted an exploratory study to test how consistent authentication methods occur on different services and scenarios. However, due to the limited number of services and scenarios, this is a pure qualitative study, and results cannot be generalized. Yet, the services we tested are among the most popular and provide a reasonable first sample. The results thus motivate more research on the security of authentication in specific scenarios. While we tested the difference between a password and 2FA, we excluded testing Single Sign-On (SSO), since its authentication behavior depends on the SSO provider. The use of passkeys was also not considered, mainly because they would have introduced a significantly higher variability and complexity to the experiments.

Furthermore, we did not test RBA extensively. Our goal was to examine which authentication methods and patterns are applied consistently across scenarios, in contrast to risk-based authentication mechanisms, which vary depending on contextual factors. However, RBA can have considerable side effects on authentication methods in these scenarios. Lastly, we did not investigate any time effects, i.e., whether a user has to re-authenticate after a certain timeout.

6 Conclusion and Outlook

This paper has studied the authentication behavior of selected online services. In addition to the regular login procedure, authentication was observed for service functions like changing email addresses or multi-factor configuration. The results show strongly divergent behavior across different scenarios and services. In particular, we observed specific patterns, such as repeatedly requesting a password or verifying the email address. Furthermore, the extent to which 2FA affects the different behaviors also varied considerably between scenarios and services. An interesting observation was that services handled 2FA-configured accounts in contrasting ways, either by treating them with higher confidence or by enforcing a more stringent login process. This indicates that there is no consensus about the ideal approach to handling these scenarios.

Future work should analyze the different patterns and approaches that were found within this study regarding their security. In particular, it should also be investigated how users perceive this. Finally, a study on a larger scale, i.e., with more services and scenarios, should be conducted to discover further authentication patterns. However, this requires more resources or approaches with higher scalability.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. von Ahn, L., Blum, M., Hopper, N.J., Langford, J.: Captcha: Using hard ai problems for security. In: Biham, E. (ed.) Advances in Cryptology — EUROCRYPT 2003. pp. 294–311. Springer Berlin Heidelberg, Berlin, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_18
2. American Psychological Association: Ethical principles of psychologists and code of conduct. https://www.apa.org/ethics/code (2017)
3. Amft, S., Höltervennhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., Fahl, S.: Lost and not found: An investigation of recovery methods for multi-factor authentication. CoRR (1 2023). https://doi.org/10.60882/cispa.25186640.v1
4. Baig, A.F., Eskeland, S.: Security, Privacy, and Usability in Continuous Authentication: A Survey. Sensors **21**(17) (2021). https://doi.org/10.3390/s21175967, https://www.mdpi.com/1424-8220/21/17/5967
5. Barth, A., Jackson, C., Mitchell, J.C.: Robust defenses for cross-site request forgery. In: Proceedings of the 15th ACM Conference on Computer and Communications Security. p. 75–88. CCS '08, Association for Computing Machinery, New York, NY, USA (2008). https://doi.org/10.1145/1455770.1455782
6. Berufsverband Deutscher Psychologinnen und Psychologen e.V., Deutsche Gesellschaft für Psychologie e.V.: Berufsethische Richtlinien des Berufsverbandes Deutscher Psychologinnen und Psychologen e.V. und der Deutschen Gesellschaft für Psychologie e.V. https://www.bdp-verband.de/fileadmin/user_upload/BDP/website/dokumente/PDF/Profession/Berufsethik/BER-Foederation-20230426-Web-1.pdf (2022)
7. Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., Santos, C.: Security analysis of subject access request procedures. In: Naldi, M., Italiano, G.F., Rannenberg, K., Medina, M., Bourka, A. (eds.) Privacy Technologies and Policy. pp. 182–209. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-21752-5_12
8. Broen, S.S.: Observational Study of the Right of Access and Erasure-From the Perspective of the Data Subject and the Data Controller. Master's thesis, University of Oslo (2024), Available at https://www.duo.uio.no/handle/10852/116541
9. Burgers, W., Verdult, R., van Eekelen, M.: Prevent session hijacking by binding the session to the cryptographic network credentials. In: Riis Nielson, H., Gollmann, D. (eds.) Secure IT Systems. pp. 33–50. Springer Berlin Heidelberg, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41488-6_3
10. Büttner, A., Pedersen, A.T., Wiefling, S., Gruschka, N., Lo Iacono, L.: Is It Really You Who Forgot the Password? When Account Recovery Meets Risk-Based

Authentication. In: Wang, G., Wang, H., Min, G., Georgalas, N., Meng, W. (eds.) Ubiquitous Security. pp. 401–419. Springer Nature Singapore, Singapore (2024). https://doi.org/10.1007/978-981-97-1274-8_26
11. Büttner, A., Gruschka, N.: Evaluating the Influence of Multi-Factor Authentication and Recovery Settings on the Security and Accessibility of User Accounts. In: Proceedings of the 10th International Conference on Information Systems Security and Privacy - ICISSP. pp. 691–700. INSTICC, SciTePress (2024). https://doi.org/10.5220/0012319000003648
12. Di Martino, M., Meers, I., Quax, P., Andries, K., Lamotte, W.: Revisiting identification issues in gdpr 'right of access' policies: a technical and longitudinal analysis. Proceedings on Privacy Enhancing Technologies (2022). https://doi.org/10.2478/popets-2022-0037
13. Edgar, T.W., Manz, D.O.: Research Methods for Cyber Security. Syngress Publishing, 1st edn. (2017)
14. Freeman, D.M., Jain, S., Dürmuth, M., Biggio, B., Giacinto, G.: Who Are you? A Statistical Approach to Measuring User Authenticity. In: Proceedings of the USENIX Network and Distributed System Security (NDSS) Symposium. San Francisco, CA (Jan 2016). https://doi.org/10.14722/ndss.2016.23240
15. Gavazzi, A., Williams, R., Kirda, E., Lu, L., King, A., Davis, A., Leek, T.: A Study of Multi-Factor and Risk-Based Authentication Availability. In: 32nd USENIX Security Symposium (USENIX Security 23). pp. 2043–2060. USENIX Association, Anaheim, CA (Aug 2023), https://www.usenix.org/conference/usenixsecurity23/presentation/gavazzi
16. IBM Security: X-Force 2025 Threat Intelligence Index. Tech. rep., IBM (2025)
17. Joukov, A., Joukov, N.: Six-year study of emails sent to unverified addresses. In: Furnell, S., Clarke, N. (eds.) Human Aspects of Information Security and Assurance. pp. 337–345. Springer Nature Switzerland, Cham (2023). https://doi.org/10.1007/978-3-031-38530-8_27
18. Klivan, S., Höltervennhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., Fahl, S.: "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. In: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. p. 3138–3152. CCS '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3576915.3623180, https://doi.org/10.1145/3576915.3623180
19. Kraus, L., Svidronová, M., Stobert, E.: How do users chain email accounts together? In: Jøsang, A., Futcher, L., Hagen, J. (eds.) ICT Systems Security and Privacy Protection. pp. 416–429. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-78120-0_27
20. Le Pochat, V., Van Goethem, T., Tajalizadehkhoob, S., Korczyński, M., Joosen, W.: Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In: Proceedings of the 26th Annual Network and Distributed System Security Symposium. NDSS 2019 (Feb 2019). https://doi.org/10.14722/ndss.2019.23386
21. Li, Y., Chen, Z., Wang, H., Sun, K., Jajodia, S.: Understanding account recovery in the wild and its security implications. IEEE Transactions on Dependable and Secure Computing **19**(1), 620–634 (2022). https://doi.org/10.1109/TDSC.2020.2975789
22. Makowski, J.P., Pöhn, D.: Evaluation of Real-World Risk-Based Authentication at Online Services Revisited: Complexity Wins. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES '23, Association

for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3600160.3605024
23. Naprys, E.: Password crisis deepens in 2025: lazy, reused, and stolen. https://cybernews.com/security/password-leak-study-unveils-2025-trends-reused-and-lazy/ (2025)
24. Paine, L., Singhal, H.: Raising the bar for software security: GitHub 2FA begins March 13. https://github.blog/news-insights/product-news/raising-the-bar-for-software-security-github-2fa-begins-march-13/ (2023)
25. Pöhn, D., Gruschka, N.: Qualitative in-depth analysis of gdpr data subject access requests and responses from major online services. In: Proceedings of the 11th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP. pp. 149–156. INSTICC, SciTePress (2025). https://doi.org/10.5220/0013093000003899
26. Pöhn, D., Gruschka, N., Ziegler, L., Büttner, A.: A framework for analyzing authentication risks in account networks. Computers & Security **135**, 103515 (2023). https://doi.org/https://doi.org/10.1016/j.cose.2023.103515
27. Ruth, K., Kumar, D., Wang, B., Valenta, L., Durumeric, Z.: Toppling top lists: evaluating the accuracy of popular website lists. In: Proceedings of the 22nd ACM Internet Measurement Conference. p. 374–387. IMC '22, Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3517745.3561444
28. Spotify AB: Protect your Spotify account. https://support.spotify.com/uk/article/protect-your-account/ (2025)
29. The European Parliament and the Council of the European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016)
30. Tiefenau, E., Grohs, J.A., Häring, M., Smith, M., Tiefenau, C.: "They are responsible for ensuring that I can continue to use the service." Investigating Users' Expectations Towards 2FA Recovery in Germany. In: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. CHI '25, Association for Computing Machinery, New York, NY, USA (2025). https://doi.org/10.1145/3706598.3714245, https://doi.org/10.1145/3706598.3714245
31. Wang, X., Yan, Z., Zhang, R., Zhang, P.: Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications **188**, 103080 (2021). https://doi.org/https://doi.org/10.1016/j.jnca.2021.103080, https://www.sciencedirect.com/science/article/pii/S1084804521001028
32. Wauters, E., Lievens, E., Valcke, P.: Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites. International Journal of Law and Information Technology **22**(3), 254–294 (03 2014). https://doi.org/10.1093/ijlit/eau002
33. Wiefling, S., Lo Iacono, L., Dürmuth, M.: Is this really you? An empirical study on risk-based authentication applied in the wild. In: ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings 34. pp. 134–148. Springer (2019). https://doi.org/10.1007/978-3-030-22312-0_10