Exploring Understanding and Usage of Two-Factor Authentication Account Recovery

Jeremiah D. Still and Lauren N. Tiller

Department of Psychology
Old Dominion Univerity
{jstill, ltill002}@odu.edu

Abstract. Users employ strategies that make passwords weaker than they appear. Companies have started requiring users to adopt two-factor authentication (2FA) to increase security, making regaining account access difficult. A potential solution is to provide users with an account recovery method used as a failsafe for 2FA in the event of a lost, broken, or stolen second factor. However, limited research evaluates users' employment of different types of 2FA account recovery methods. Our exploratory study surveyed 103 students. We found only 40% of the sample have more than one 2FA device enrolled per personal account. The majority opt to use 2FA devices that are executed using their phone, 81% use a mobile app, and 51% receive an SMS text message. Our findings suggest regaining account access could be challenging for users when their phone becomes unavailable. If companies do not adequately prepare for such occurrences, it will become costly and disruptive.

Keywords: Human Factors · Survey · Two-Factor Authentication

1 Introduction

When it comes to knowledge-based authentication, users bear the responsibility of creating strong passwords to ensure the security of their online accounts [1]. The security requirements for creating a strong password are cumbersome [2, 3, 4, 5]. To overcome these cognitive burdens, users often produce passwords that reflect common patterns or strategies that are easy to recall, which may reduce their account's resistance to cyber-attacks. To increase account security and compensate for insecure account protection provided by traditional alphanumeric passwords, some companies (e.g., Microsoft, Google, and Facebook) have started to offer or require their users adopt two-factor authentication [6].

Two-Factor (or Multi-Factor) Authentication (2FA) is a layered authentication process requiring the user to couple their password with another authentication method. In 2018, federal agencies that use dot-gov domains, such as the Department of Justice, began to prompt officials to add the two-factor security feature to increase the system's intruder attack resistance [7]. However, if a second-factor device fails, regaining account access can be problematic for the authorized user [8]. Essentially, when the authentication process requires more information to prove identity. As a result, regaining account access often becomes more difficult [8].

The password reset procedure for systems that only use a single-factor password is different from the 2FA account recovery processes. Renaud (2007), noted that systems using single-factor password authentication fulfill password reset requests by

either asking the user to answer personal questions, e-mailing the user their forgotten password, or e-mailing the user a secure link that obliges the user to create a new password [9]. The account recovery process for systems that implement 2FA is more complicated. Even though passwords may be involved, account recovery is not the same as a basic password reset [10]. Systems implementing 2FA require extra steps to ensure that an account is recovered to its rightful owner. Account recovery procedures are essentially bypassing the system's main security protocols, which necessitates systems to treat account recovery as an alternative authentication.

The purpose of an account recovery method is to maintain the high cyber-attack resistance while still allowing the authorized user account access. There is limited research that evaluates different types of 2FA account recovery methods. We aimed to further understand the end user's knowledge of and usage of 2FA authentication recovery.

1.1 User Studies Surrounding 2FA

Das et al. (2018) conducted research comparing user acceptance of various USB Yubico keys in a two-part study [11]. They focused on collecting usability and acceptability data. Despite the Yubico design improvements, they showed that participants continued to express their belief in password strength alone. Notably, they stated, "Even the best-designed hardware will not be used if the benefits are not apparent" [11, p. 15]. More closely aligned with our research within a university setting.

Colnago et al. (2018) explored the behaviors and opinions of 2FA adoption at Carnegie Mellon University (CMU)[12]. They found that users believed 2FA provided their account with more security, and it was reasonably easy to use. However, many found the requirement of 2FA annoying. Interestingly, their results indicated that users commonly reported problems such as forgetting their second factor, having it too far away, losing their phone, having a dead phone battery, having no data connection, and the hardware token desynchronizing. When these problems occurred, users reported consequences such as not being able to do homework and participate in class; not having access to e-mail or a computer system; not having access to a dorm or office.

1.2 2FA Account Recovery

An account recovery authentication option is an account feature that some systems with 2FA make available for users to set up before losing a second-factor device. Large tech companies use several 2FA recovery options. Loveless (2018) conducted an informal exploratory evaluation of authentication practices for several websites (e.g., Facebook, Amazon, Apple ID, GitHub, Reddit, Yahoo, Twitter, LinkedIn, Gmail, Kraken, Live, and Coinbase) [10]. It was revealed that organizations are employing several recovery options. That is, end-users can opt to receive a set of downloadable recovery codes, or they can set up a backup e-mail, phone number, or device. None of the evaluated companies provided users with all these options, but a fair degree of flexibility was common.

Organizations with 2FA (e.g., Reddit, GitHub, and Google) are currently offering precautionary account recovery options [13, 14]. Other websites such as Apple, Evernote, Twitter, and Coinbase inform account holders that in the event of a lost

second factor, it may take several business days to regain account access [15, 16]. LinkedIn users are required to complete a multi-part form and submit a copy of a government-issued ID when their second factor is unavailable [10]. Asking users to select the best account recovery option and understand their actions from a cybersecurity perspective requires expertise.

1.3 Cyber Hygiene: Training and Expertise

Asking users to make good security decisions relating to authentication often falls under the heading of cyber hygiene. Cain, Edwards, and Still (2018) conducted an extensive study to evaluate users' cyber hygiene knowledge of threats, concepts, and behaviors by examining cyber topics such as authentication, security software, social networking, web browsing, USB drive use, phishing scams, and Wi-Fi hotspot usage [17]. Their results indicated that people 45 years of age and older generally practice more secure cyber behaviors. Cyber hygiene knowledge did not differ by age. Another finding of their study suggested that users who were victims of past cyber-attacks reported behaviors and knowledge that did not differ from users who had not been subjected to a cyber-attack. Interestingly, the survey results showed that participants who indicated they had received past cybersecurity training had less knowledge and more risky behaviors than users who reported they had not received training. They found that 81% of their participants (n = 144) had received some form of cybersecurity training. Other research studies that evaluated the proportion of self-identified cybersecurity trained participants found much lower results [19% for college-age students, 18; 43% for adults, 19].

End users are asked to set up 2FA accounts. The registration process requires them to make decisions beyond the typical creation of a secure password. Now users are being asked to select a 2FA recovery method from a set of options. We aimed to reveal college users' 2FA account recovery choices. And we explored the impact self-reported cybersecurity training and experience with a previous attack had on general authentication knowledge.

2. Method

These data were extracted from a more extensive survey [20] examining other factors not presented in this article (e.g., Berlin Numeracy Test). We are going to focus on two question sections within the survey demographics and general knowledge of authentication.

2.1 Participants

A total of 113 undergraduate students (females = 78) were recruited through the SONA Experiment Management System and were compensated for participation. Participants had to answer two of the three attention check questions correctly and complete the security ranking questions to be included in the study. Data from 10 participants were omitted, resulting in 103 participants (females = 73). Ages ranged from 18 to 50 years ($M = 21.50$, $SD = 6.10$) and reported heavy daily computer usage ($M = 8.35$, $SD = 3.99$). The number of 2FA devices participants registered to any given account enrolled in 2FA ranged from 1 to 5 ($M = 1.58$, $SD = 0.92$).

2.2 Materials and Procedure

This research used a 42-question survey that took participants approximately 35 minutes to complete. Previous research has noted that self-report is a valid measure for the topics covered by our survey. According to Russell et al. (2017), when users do not behave securely, their recount of non-secure behaviors still results in honest reporting [21].

2.3 Knowledge of Authentication

To develop the construct for the general authentication knowledge, we chose seven questions (two general and five threats) from the Cain et al. (2018) article that related to authentication practices. And, one new question as created to target specific authentication understanding [17]. Participants were asked to respond to each question with Strongly Agree, Agree, Neither Agree nor Disagree, Disagree, and Strongly Disagree. Overall knowledge scores reflect a combination of the general- and threat- authentication knowledge scores (Cronbach α of .60; an acceptable level of reliability).

The knowledge of general authentication consisted of three questions about authentication security concepts. And, a new question to assess whether users understand the operational definition of authentication. These questions focused on capturing the participants' knowledge of common authentication terminology. The knowledge of threats questions focused on capturing the participants' knowledge regarding common threats, behaviors, or outcomes associated with secure authentication practices. An example of a threats statement is, “It is safe to share a password with others”.

3. Results

3.1 Demographics & Usage

Twenty percent of participants indicated they had previous exposure to some type of educational cybersecurity material (see Table 1). When the survey data were collected, our sample needed to have their accounts enrolled in 2FA. However, only 89% of participants indicated that they used 2FA to protect any personal accounts. Suggesting the conceptual meaning of 2FA is not apparent to some users. Eighty-one percent of participants indicated they use a smartphone or tablet app as their second factor, and 60% of participants only have one 2FA device enrolled per account (M = 1.58, SD = 0.92). For more reports on 2FA familiarity, see Table 1 and Figures 1 and 2.

Table 1. Frequency Table for Cybersecurity Familiarity

Variable	*n*	%
Received Cybersecurity Training		
Yes	11	10.7
No	92	89.3
Training Location		
Work	8	7.5
School	5	4.7
Online	2	1.9
Other – Military	2	1.9
N/A	89	84.0
Taken a Class with Cybersecurity Topics		
Yes	16	15.5
No	87	84.5
Cybersecurity Expert		
Yes	1	1.0
No	102	99.0
Target of a Cybersecurity Attack		
Yes	17	16.5
No	86	83.5

Note. $N = 103$.

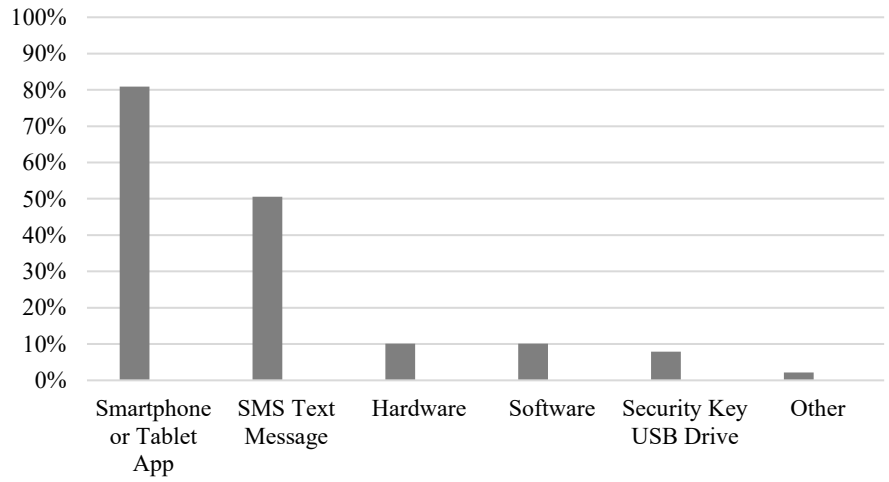

Fig. 1. 2FA Devices Used by Type. Note: The 89 participants who reported Yes to using 2FA were asked to indicate the type of 2FA devices they had used. Participants had the option to select more than one kind of 2FA device, which resulted in $N = 144$ responses. The percentage represents the proportion of participants out of the 89 participants who reported they use 2FA.

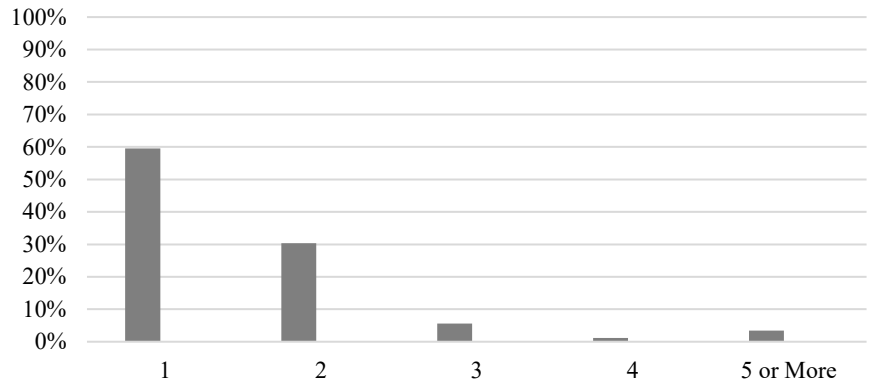

Fig. 2. The number of 2FA Devices Enrolled per Account. Note: The percentage represents the proportion of participants out of the 89 participants who reported they use 2FA.

3.2 Overall Authentication Knowledge: Cybersecurity Training and Experience with an Attack

The results revealed that participants answered more than half of the authentication knowledge questions correctly ($M = 6.91$, $SD = 1.70$). However, a low number of participants indicated that they had "… received training in cybersecurity…" ($N = 11$). To make group sizes more equal, the "yes" cybersecurity training group was expanded to include participants who indicated they are a cybersecurity expert or have taken classes that covered cybersecurity topics. Specifically, we added the participants that selected "yes" to the questions, "Have you taken classes covering the topic of cybersecurity in the past?" or "Do you consider yourself an expert in cybersecurity?" ($N = 21$).

An independent samples *t*-test was used to explore the relationship between overall authentication knowledge and cybersecurity training. Overall authentication knowledge scores for participants who had not received any form of cybersecurity training ($M = 6.83$, $SD = 1.71$, $N = 82$) were not significantly different from the scores of participants who had received cybersecurity training ($M = 7.24$, $SD = 1.67$, $N = 21$), $t(101) = -0.98$, $p = 0.165$, $d = -0.240$.

An independent samples *t*-test showed the authentication knowledge scores for participants who have not been a cyberattack victim ($M = 6.84$, $SD = 1.71$, $N = 86$) were not significantly different from participants who have been a cyberattack victim ($M = 7.29$, $SD = 1.65$, $N = 17$), $t(101) = -1.01$, $p = 0.315$, $d = -0.268$. However, we cautiously present this finding as the groups are far from equal (i.e., cyberattack victim, No: 86 versus Yes: 17).

4. Discussion

Systems implementing 2FA give users the option to enroll as many 2FA devices to their accounts as they desire. However, we found that 60% of participants indicated they typically have only one 2FA device enrolled per personal account ($M = 1.58$, $Md =$

1.00, *SD* = 0.92). This finding is aligned with Colnago et al. (2018) previous findings, which suggest users employ an average of 1.3 (*Md* = 1.00) 2FA devices [12]. Clearly, most users would not have another authentication option to gain account access if their primary 2FA device became unavailable. We found that 81% of participants used a mobile or tablet app as their 2FA device, and 51% indicated that they received an SMS text message. Only 10% of participants stated that they used either a hardware or a software device, and only 8% used a USB security key (see Figure 1). Colnago et al. (2018) found that as the frequency of experiencing 2FA problems increases, users' perceptions are negatively impacted, as well as the usability and security constructs [12]. Future training material should consider ways to convince users that it is necessary to enroll additional 2FA devices, other than just their phone.

Even though our results suggested that cybersecurity training or experience with an attack did not impact users' authentication knowledge, it is important to highlight that most of the sample indicated they had no prior experience with either. Further, exploration of previous training is limited because we did not inquire about the specific topics or the training's breadth.

Presumably, account recovery occurs intermittently; therefore, it is critical the 2FA option is easy to access and remember. Mobile phones are commonly employed as a recovery option, probably due to their easy access. A USB key is much less likely to be available. A knowledge-based authentication would need to be easy to retrieve from memory. A typical pattern across memorability studies suggests that graphical authentication schemes allow users to easily retrieve their passcode from memory (i.e., by employing both images and a recognition task; see 1; 22].

From a practitioner's perspective, users need to be strongly encouraged to enroll in at least two different 2FA devices (e.g., mobile app and USB key). We found an over-reliance on mobile phones. Therefore, we recommend that designers provide a narrative highlighting the danger associated with using the same device for both authentication and recovery. Similar to previous research suggesting that a company's communication should lead the user away from making risky security decisions [23].

Some companies warn employees that 2FA account recovery might take several business days [15, 16]. This awareness will encourage users to set up a 2FA recovery method. However, they may not be selecting an actual recovery option (i.e., their phones might be unavailable). If companies do not adequately prepare for such occurrences, it could be costly and disruptive as employees are prevented from accessing critical services needed to perform their duties.

5. References

1. Cain, A. A., & Still, J. D.: Usability comparison of over-the-shoulder attack resistant authentication schemes. J. of Usability Studies. *13*, 196--219 (2018)
2. Ashford W.: Millions of web users at risk from weak passwords [Web blog post]. http://www.computerweekly.com/Articles/2009/09/07/237569/Millions-of-web-users-at-risk-from-weak-passwords.htm (2009, September 7)
3. Barton, B. F., & Barton, M. S.: User-friendly password methods for computer-mediated information systems. J. Comp. & Sec. 3, 186--195 (1984)
4. Hoonakker, P., Bornoe, N., & Carayon, P.: Password authentication from a human factors perspective: Results of a survey among end-users. In: proceedings of the Human Factors and Ergonomics Society Annual Meeting*,* 53, 459--463 (2009)

5. Labuschagne, W. A., Veerasamy, N., Burke, I., & Eloff, M. M.: Design of cyber security awareness game utilizing a social media framework. In: proceedings of Information Security South Africa, 1--9 (2011)
6. Reese, K. R.: Evaluating the usability of two-factor authentication [Published Master's thesis]. All Theses and Dissertations Database, (UMI No. 6869) (2018)
7. Shaban, H.: The government is rolling out 2-factor authentication for federal agency dot-gov domains. The Washington Post. https://www.washingtonpost.com/technology/2018/10/08/government-is-rolling-out-factor-authentication-federal-agency-gov-domains/ (2018, October 8)
8. Tellini, N., & Vargas, F.: Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a digital assessment platform [Unpublished Bachelor's Thesis,]. KTH Royal Institute of Technology (2017)
9. Renaud, K.: A process for supporting risk-aware web authentication mechanism choice. J. of Reliability Eng. & Sys. Safety 92, 1204--1217 (2007)
10. Loveless, M.: How popular web services handle account recovery. Duo Security. https://duo.com/decipher/reality-of-online-account-recovery (2018, March 6)
11. Das, S., Dingman, A., & Camp, L. J.: 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, (2018)
12. Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N.: "It's not actually that horrible": Exploring adoption of two-factor authentication at a university. In: CHI Conference on Human Factors in Computing Systems, 1--11 (2018)
13. Prins, C. W.: 2-Factor authentication recovery codes [Web blog post]. 4me. https://www.4me.com/blog/two-factor-authentication/two-factor-authentication-recovery-codes/ (2018, April 15)
14. Wallen, J.: How to retrieve your Google 2FA backup codes (and make more) [Web blog post]. TechRepublic. https://www.techrepublic.com/article/how-to-retrieve-your-google-2fa-backup-codes-and-make-more/ (2018, August 7)
15. Afonin, O.: The ugly side of two-factor authentication [Web blog post]. https://blog.elcomsoft.com/2016/12/the-ugly-side-of-two-factor-authentication/ (2016, December 20)
16. Ravenscraft, E.: What happens if I use two-factor authentication and lose my phone? [Web blog post]. lifehacker. https://lifehacker.com/what-do-i-do-if-i-use-two-factor-authentication-and-los-1668727532 (2014, December 09)
17. Cain, A. A., Edwards, M. E., & Still, J. D.: An exploratory study of cyber hygiene behaviors and knowledge. J. Info. Sec. and App. 42, 36--45 (2018)
18. Aytes, K., & Conolly, T.: A research model for investigating human behavior related to computer security. In: proceedings of Americans Conference on Information Systems. *9*, 2027—2031 (2003)
19. National Cyber Security Alliance.: NCSA / Norton by Symantec Online Safety Study. http://www.staysafeonline.org/download/datasets/2064/FINAL+NCSA+Full+Online+Safety+Study+2010%5B1%5D.pdf (2010)
20. Tiller, L. N.: Account recovery methods for two-factor authentication (2FA): An exploratory study. [Unpublished Master's Thesis]. Old Dominion University (2020)
21. Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G.: Self-reported secure and insecure cyber behaviour: Factor structure and associations with personality factors. J. of Cyber Sec. Tech. 1, 163--174 (2017)
22. Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme. In: proceedings of the Working Conference on Advanced Visual Interfaces, 177--184. (2006)
23. Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K.: Trustworthy and effective communication of cybersecurity risks: A review. In: proceedings of the 1st Workshop on STAST, 60--68 (2011)