"I cannot do anything": User's Behavior and Protection Strategy upon Losing, or Identifying Unauthorized Access to Online Account

Mahdi Nasrullah Al-Ameen
Utah State University
mahdi.al-ameen@usu.edu

Huzeyfe Kocabas
Utah State University
huzeyfe.kocabas@aggiemail.usu.edu

Abstract

A wide-range of personal and sensitive information are stored in user's online accounts. Losing access, or an unauthorized access to one of those accounts could put them into the risks of privacy breach, cause financial loss, and compromise their accessibility to important information and documents. A large body of prior work focused on developing new schemes and strategies to protect user's online security. However, there is a dearth in existing literature to understand users' strategies and contingency plans to protect their online accounts once they lose access, or identify an unauthorized access to one of their accounts. We addressed this gap in our work, where we conducted semi-structured interview with 22 participants. Our findings reveal the unawareness, misconceptions, and privacy and accessibility concerns of users, which refrain them from taking security-preserving steps to protect their online accounts. We also identified users' prevention strategies that could put their online security into further risks.

1 Introduction and Background

The authentication secrets of 620 million user accounts are stolen by adversaries from 16 different websites [19], where many users are unsure of how they could recover access to their accounts [15]. Users are found to understand the risks of data breaches [9], however, their security behavior is influenced by costs associated with protective measures, where they have a general tendency towards delaying action until harm has occurred [21]. The study of Marques et al. [13] investigated users' perceptions of unauthorized physical access to smartphones, where they analyzed the relation between social trust, personal relationship, and security vulnerabilities.

To prevent unauthorized access to users' accounts, the prior studies focused on studying users' password management strategies [11, 14, 17], improving the security and usability of authentication schemes [1, 2, 4], developing automated techniques to detect unauthorized access to an account [10], and designing educational tools and warning system to prevent social engineering attacks [3, 12, 16]. However, a little study is conducted to date, to understand users' behavior once they lose access or identify an unauthorized access to their online account. To address this gap, we focused on the following research questions in our work: i) How do users respond to a situation when they lose access, or identify an unauthorized access to their online account? ii) What are the strategies and contingency plans of users to protect their online accounts in the future?

The study of Haque et al. [7] divided online accounts into four categories (e.g., financial, identity, content, and sketchy), where they emphasized on the protection of financial, and identity accounts (e.g., email, social networking). Thus, our study focused on user's protection behavior for financial and identity accounts, considering the sensitivity of user information stored, or shared through these accounts.

2 Methodology

We conducted semi-structured interview (audio-recorded) with 22 participants, who are from diverse disciplines, including mathematics, learning science, architecture, and engineering (see Table 1 in Appendix for demographic information of our participants). We recruited participants through posting flyers on public places, and sharing the study information through online social media. Our study was approved by the Institutional Review Board (IRB) at our university.

In this study, each participant was interviewed individually in a lab setting. We asked them about their past experience of losing access to their financial and identity accounts, identifying an unauthorized access to any of these accounts, and what

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Boston, MA, USA.

protection steps they had taken in such instances. Participants were also asked about their strategies and contingency plan to protect their financial and identity accounts in the future. At the end, they completed a paper-based survey on demographic questionnaire. On average, each session took between 20 and 30 minutes. We compensated each participant with a $10 amazon.com gift card.

At the end of data collection, we transcribed the audio recordings, and performed thematic analysis on our transcription [5]. Two researchers independently coded the interviews, and analyzed the collected data by looking at common themes that emerged in our interviews.

3 Results

Seventeen out of 22 participants reported to lose access, or identify an unauthorized access to their financial, or identity account, where we unpacked their strategies to regain access and protect their accounts. For other five participants, we reported their contingency plan in case of losing access or identifying an unauthorized access in the future (see §3.3.3).

3.1 Losing Access to Online Account

About half of our participants reported losing access to at least one of their financial, or identity (e.g., email, or social networking) accounts, where they could not recover the access. Below, we report our findings revealing why participants lost access to their accounts.

Geographic Relocation. Many service providers block suspicious login attempts from unusual location to protect their users' online accounts from unauthorized access. In such cases, a user might be asked to prove her identity by entering a one-time-code delivered to her phone number, registered with the system [6]. We found that such security measures could pose accessibility challenges to users, causing them to lose access to their online accounts. For instance, one of our participants (P17) who moved to the USA from a country in Asia, could no longer authenticate to her social networking account after geographic relocation. Her login attempt from the USA was considered suspicious by the system, where she could not prove her identity through her phone number in the USA as it was not registered with her account. P15 mentioned that he was blocked from accessing his email account: *"There was one email account that I lost completely because I had not connected my phone number with it, and I tried using it from a different country using a wrong password and it blocked me out."* He then contacted the customer service to recover his account: *"I tried calling them. For some reasons that did not work and you know what happened after that [could no longer access this account].* Due to the risks of information leakage, he reported concern about registering his phone number with an online account.

Lack or Failure of Secondary Authentication. P01 commented, *"I lost like many times, I mean my email accounts"*. Including P01, several participants lost access to their financial or identity accounts as they could not recover the access upon forgetting their primary authentication code, e.g., password. Among them, some participants failed to recover their access as they forgot their secondary authentication code. For instance, P19 could not recall the answer to her security question for secondary authentication: *"There were some other special questions that asked like, what was your third grade teacher or some special question, and I just didn't remember them. So I had to create another email [account]."* P15 reported losing access to his online bank account as he could not recall his email ID connected to that account for secondary authentication. Several participants lost access to their account as they had not set a secondary authentication code during account creation, where P03 commented, *"I think that if I designed some security question at the beginning of creating account, now I would not lose that access and recover my account."*

Adversary's Action. Among those participants who lost access to online accounts, several of them reported that their account was hacked followed by changing the authentication code by adversaries. Participants are not sure whether they were the victim of a targeted attack by someone they know, or their passwords were leaked to unknown attackers. P04, who lost access to his social networking account, perceives that the leakage of his password could be prevented if the service provider would have taken appropriate measures to protect users' credentials.

3.2 Unauthorized Access to Online Account

About one-third of our participants reported that they had identified an unauthorized access to at least one of their financial or identity accounts, where they did not lose access to that account. Among them, a few participants identified unauthorized access to their social networking account through checking the activity log. The other participants reported, they got aware of unauthorized access through email notification from the service provider. For instance, P01 mentioned an email delivered to him, which provided him with the location information of an adversary logging into his social networking account. This participant perceives that the service providers of different online accounts work together to protect their users' online security, which assures him that he does not need to worry about unauthorized access to his online accounts.

P02 reported an incident where he received an email asking him to change his password for a bank account, because *"someone else was using my information, hacked the account or something."* The similar incidents were reported by a few other participants, where they received an email asking to change their authentication secret; P12 mentioned, *"Once I*

got an email from Gmail that someone is trying to access my account and gave me a link [to change password]...I went to the link and changed my password."

3.3 Prevention Strategy & Contingency Plan

Most of our participants reported that they had lost access, or identified an unauthorized access (but did not lose access) to one of their financial or identity accounts. P01 and P15 encountered both instances. In this section, we report our findings on the steps taken by our participants upon losing access, or identifying an unauthorized access to their account (Figure 1 in Appendix illustrates the prevention strategy and contingency plan of our participants).

3.3.1 Who Lost Access to Online Account

P15 lost access to his email account as he forgot his password and could not leverage secondary authentication due to geographic relocation (e.g., moving to a new country). To prevent such incident from happening in the future, he now stores his authentication secrets to address the memorability issue: *"I try to save my password somewhere whether it is in browser or in a text file."* Most of our participants who lost access to their online accounts because of not setting a secondary authentication method, now store their primary authentication code, e.g., password in a digital (e.g., text file, email) or physical medium (e.g., notebook). P01 said, *"I just take the note like, you know, to my notebook. And I just use that one to reach my account, just to remember my password...And the steps I took like are working very well for now."*

Participants who store their password in a physical medium reported confidence in securing that from unwanted entities. For instance, P09 commented, *"I am more aware [now] and so like I write them [passwords] down. But no one will see it but myself."* Participants who could not recover their accounts due to forgetting secondary authentication code (e.g., answer to a security question), consider it as a safer option to write down the answers to their security questions for secondary authentication, instead of storing their primary authentication code (e.g., password). Our participants store their password, or answer to a security question in plaintext.

Among those participants whose online accounts were compromised by the adversary, P04 mentioned creating a stronger password for his new account to prevent such incident from happening in the future: *"I chose a longer password."* The other participants did not report taking any security-preserving steps to protect their online accounts from an unauthorized access. Some of them feel helpless in face of adversary's action, and are unsure of how they could protect their online security. For example, when we asked about their steps, taken to prevent unauthorized access to their accounts in the future, P02 said, *"I cannot do anything."* In this context, a few participants reported a contingency plan that they would meet the customer service personnel in person, if their online accounts are further compromised by an adversary.

3.3.2 Who Identified Unauthorized Access

Among the participants who identified unauthorized access to their online account, most of them did not take any preventive steps. We found that participants place trust on the service provider to protect their online security. For instances, P01 and P15 believe that the service providers take required steps whenever an adversary attempts to compromise their account, and notify them through email when such unauthorized attempts to access their account fail due to organization's security protection in place. Here, some participants do not have a clear idea about what steps they should take once an unauthorized access is identified, where P18 said, *"I don't know what to do...what i am going to do. I don't know."* A few participants reported to change their password of email and social networking account using the link provided in the email that had informed them about an unauthorized access to their account. In this context, P13 did not change her password for the account where an unauthorized access was identified, rather she set up security questions and added a recovery email ID for secondary authentication, so that she could recover her access to that account if the primary authentication code is changed by the adversary. She preferred not to add her mobile phone number for two-factor authentication as she was concerned that she might not be able to access her account when she would be out of her phone's network coverage.

Once P21 identified an unauthorized access to his social networking account through checking the activity log, he considered that deleting that account would be the best line of defense to protect his personal information. Then, he took a series of steps to prevent unauthorized access in the future. He created a new social networking account, and divided his online accounts into two categories: 'important' and 'non-important'. For his 'important' accounts, he created new passwords that are different from each other, as this participant was afraid that the adversary accessing his social networking account might be able to guess his password for other accounts. He then activated two-factor authentication for his 'important' accounts by adding his phone number.

3.3.3 Others

Among those participants who did not lose access or identify any unauthorized access to their online accounts, a few of them were confident that they would not encounter any such incidents in the future, where P06 commented, *"They [adversaries] cannot get my password."* We identified uncertainty among participants when we asked them about their contingency plan in case they lose access to an online account. Several of them mentioned, they would contact the tech support of the service provider, however, were not sure how to reach out to them. Here, P22 mentioned that he would contact the upper management in Google if his access to email

account is compromised.

If an unauthorized access to the online account is identified, P07 mentioned that he would change the password of that account. However, he also reported uncertainty if this step would be sufficient to protect his account from the adversary. In this context, P10 and P11 believe that the only way to protect an account is to delete it upon identifying an unauthorized access. P10 would also reach out to the law enforcement agency to identify the adversary in order to protect his online accounts; he added, *"[It is] always difficult to track who is trying to hack your account. But I think this day with technology, I've heard police is able to track or know who is sending what from where."*

P22 reported using an antivirus software in his computer, where he perceives that the antivirus application would protect his computer and online accounts from adversaries. A few participants keep local backup of their personal documents and photos that are shared or stored online, so that they do not lose access to those files in case their email or social networking accounts are compromised.

4 Discussion

4.1 Prevention Strategies, Risks, & Concerns

Our findings indicate that the prevention strategies taken by users upon losing access to an online account could increase their exposure to cyber attacks, and in turn, weaken their security protection. Forgetting passwords, coupled with geographic relocation or the failure/lack of secondary authentication caused our participants losing access to their online account. As a prevention strategy, they started to write down their password (in plaintext) on paper, or store that in a digital medium, e.g., textfile or email. Participants who could not leverage secondary authentication to recover their account due to forgetting answers to security questions, now write down those answers to address the memorability issue. However, writing down or storing password in an unprotected medium could lead to password leakage [20], increasing the risks of unauthorized access to their online accounts. The future research should further investigate how users protect the medium that they use to write down their passwords.

Our participants mentioned the email notification that asked to change their password for an online account. It was out of the scope of this study to verify the legitimacy of the reported emails, however, we note that the dependency of participants on email notifications to identify an unauthorized access could be exploited by adversaries to conduct phishing attacks [3]. The future research should explore the relation between users' strategies to protect their online accounts and underlying susceptibility to social engineering attacks, e.g., phishing.

Our results show that the uncertainty about accessibility could refrain users from taking security-preserving steps to protect their online accounts. While one-time password based two-factor authentication using mobile phones contribute to enhance online security [6], participants reported concern that they might loose access to their online account if they are out of their cellphone's network coverage, e.g., due to geographic relocation. Also, participants worried about privacy leakage in sharing their mobile phone number with the service providers.

4.2 Security (Mis)conceptions

In this section, we discuss about the misconceptions of participants, which give them a false sense of security in protecting their online accounts. We emphasize that future research should focus on identifying appropriate measures to alleviate user's misconceptions, so that they could make an informed security decision.

Writing down a secondary authentication code in an unprotected medium could be as vulnerable as writing down a primary authentication secret (e.g., password); if adversaries gain access to the answer of a security question, they could exploit the secondary authentication method to compromise a user's account [8, 20]. However, the participants who write down their secondary authentication code (e.g., answer to a security question), perceive it as a more secure approach than writing down their password.

Some service providers (e.g., Google [1]) inform their customers through email about login from a new device or location, to help them with identifying unauthorized access and taking appropriate actions. However, the purpose of such email notifications is misunderstood by several participants. As they perceive, receiving such email indicates that adequate security measures are taken by the service provider, requiring no further action at user's end. Our findings indicate the need of redesigning email-based security alerts, to help users with better understanding of security risks and protective measures.

Participants place over-reliance on security software as they lack understanding of how that system works. Antivirus application, in general, is designed to protect a computer from malicious software [18], where a few participants perceive that the antivirus application also protects their online accounts from the adversaries. Such reliance provides them with a false sense of security, which in turn, refrains them from taking security measures to protect their online account.

4.3 Limitations

Our sample size is relatively small, where we followed the widely-used method for qualitative research [5], focusing in depth on a small number of participants and continuing the interviews until no new themes emerged (saturation). Most of our participants were male, young, and students at the university. Thus, our findings may not be generalizable to the entire population. In our future work, we would conduct a large-scale survey with the participants from diverse demographics and literacy levels to attain quantitative and more generalizable results.

[1] https://support.google.com/accounts/answer/2590353?hl=en

References

[1] Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright, and Shannon Scielzo. The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In *Symposium On Usable Privacy and Security*, pages 185–196, 2015.

[2] Mahdi Nasrullah Al-Ameen and Matthew Wright. Exploring the potential of Geopass: A geographic location-password scheme. *Interacting with Computers*, 29(4):605–627, 2017.

[3] Mohamed Alsharnouby, Furkan Alaca, and Sonia Chiasson. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82:69–82, 2015.

[4] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44(4):1–41, 2012.

[5] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[6] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, and Muhammad Khurram Khan. Otp-based two-factor authentication using mobile phones. In *2011 Eighth International Conference on Information Technology: New Generations*, pages 327–331. IEEE, 2011.

[7] S M Taiabul Haque, Matthew Wright, and Shannon Scielzo. A study of user password strategy for multiple accounts. In *ACM conference on Data and application security and privacy*, pages 173–176, 2013.

[8] Mike Just and David Aspinall. Personal choice and challenge questions: a security and usability assessment. In *Symposium on Usable Privacy and Security*, pages 1–11, 2009.

[9] Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. Data breaches: user comprehension, expectations, and concerns with handling exposed data. In *Symposium on Usable Privacy and Security*, pages 217–234, 2018.

[10] Milton King, Dima Alhadidi, and Paul Cook. Text-based detection of unauthorized users of social media accounts. In *Canadian Conference on Artificial Intelligence*, pages 292–297. Springer, 2018.

[11] Vijay Kothari, Ross Koppel, Jim Blythe, and Sean Smith. Password logbooks and what their amazon reviews reveal about their users' motivations, beliefs, and behaviors. In *European Workshop on Usable Security*, 2017.

[12] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. How effective is anti-phishing training for children? In *Symposium on Usable Privacy and Security*, pages 229–239, 2017.

[13] Diogo Marques, Tiago Guerreiro, Luís Carriço, Ivan Beschastnikh, and Konstantin Beznosov. Vulnerability & blame: Making sense of unauthorized access to smartphones. In *2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[14] Peter Mayer and Melanie Volkamer. Addressing misconceptions about password security effectively. In *Workshop on Socio-Technical Aspects in Security and Trust*, pages 16–27, 2018.

[15] Ron Miller. That time i got locked out of my google account for a month, December 2017. https://techcrunch.com/2017/12/22/that-time-i-got-locked-out-of-my-google-account-for-a-month/.

[16] Sovantharith Seng, Mahdi Nasrullah Al-Ameen, and Matthew Wright. Understanding users' decision of clicking on posts in facebook with implications for phishing. In *Workshop on Technology and Consumer Protection (ConPro)*, 2018.

[17] Elizabeth Stobert and Robert Biddle. The password life cycle. *ACM Transactions on Privacy and Security*, 21(3):1–32, 2018.

[18] Orathai Sukwong, Hyong Kim, and James Hoe. Commercial antivirus software effectiveness: an empirical study. *Computer*, (3):63–70, 2010.

[19] Chris Williams. 620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts, February 2019. https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/.

[20] Leah Zhang-Kennedy, Sonia Chiasson, and Paul van Oorschot. Revisiting password rules: facilitating human management of passwords. In *APWG symposium on electronic crime research (eCrime)*, pages 1–10, 2016.

[21] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. "I've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In *Symposium on Usable Privacy and Security*, pages 197–216, 2018.

Appendix

See next page.

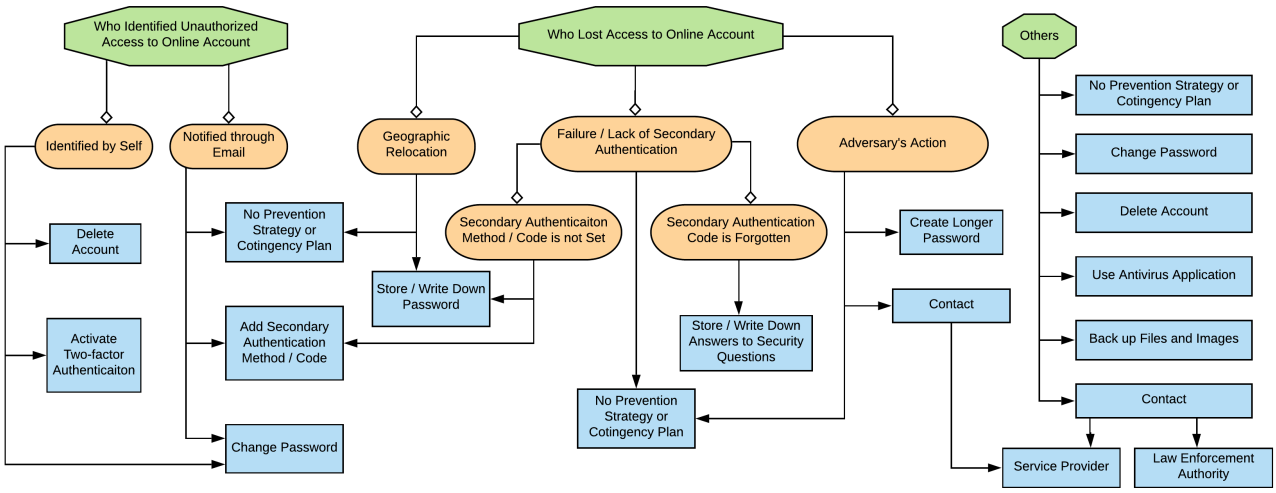

Figure 1: Prevention Strategies and Contingency Plans of Participants to Protect Their Online Accounts

Gender	**Participants**
Male	P1 - P4, P7, P8, P10 - P12, P14 - P16, P18, P20 - P22
Female	P5, P6, P9, P13, P17, P19
Age-range	
18-24	P5, P6, P19, P21, P22
25-29	P2, P7 - P15, P18, P20
30-34	P1, P3, P16, P17
35-39	-
40 and above	P4
Literacy Level	
High School	P19, P21, P22
Undergraduate*	P5, P6, P9, P13, P14, P18, P20
Graduate*	P1 - P4, P7, P8, P10 - P12, P15 - P17
Primary Occupation	
Student	P1 - P3, P6 - P8, P10 - P14, P18, P19, P22
Employee at Educational Institution	P4, P15 - P17, P21
Employee at Non-profit Organization	P20
Employee at Business Industry	P5
Other	P9

Table 1: The Highlight of Participants' Demographic Traits [*Either completed or currently studying at the noted education level]