7-3-2021

Understanding User's Behavior and Protection Strategy upon Losing, or Identifying Unauthorized Access to Online Account

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

Swapnil Nandy
Jadavpur University, swapnilnandy2@gmail.com

Tanjina Tamanna
University of Dhaka, turnatatatu666@gmail.com

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

Recommended Citation

Kocabas H., Nandy S., Tamanna T., Al-Ameen M.N. (2021) Understanding User's Behavior and Protection Strategy upon Losing, or Identifying Unauthorized Access to Online Account. In: Moallem A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2021. Lecture Notes in Computer Science, vol 12788. Springer, Cham. https://doi.org/10.1007/978-3-030-77392-2_20

Understanding User's Behavior and Protection Strategy upon Losing, or Identifying Unauthorized Access to Online Account

Huzeyfe Kocabas[1], Swapnil Nandy[2], Tanjina Tamanna[3], and Mahdi Nasrullah Al-Ameen[1]

[1] Utah State University, USA
[2] Jadavpur University, India
[3] University of Dhaka, Bangladesh

huzeyfe.kocabas@aggiemail.usu.edu, swapnilnandy2@gmail.com, turnatatatu666@gmail.com, mahdi.al-ameen@usu.edu

Abstract. A wide-range of personal and sensitive information are stored in users' 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 users' 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 59 participants from three different countries: Bangladesh, Turkey, and USA. 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.

Keywords: User Behavior · Qualitative Study · Protection Strategy · Contingency Plan · Online Accounts · Cross-cultural Study

1 Introduction

The authentication secrets of 620 million user accounts are stolen by adversaries from 16 different websites [39], where many users are unsure of how they could recover access to their accounts [26]. Users are found to understand the risks of data breaches [20], however, their security behavior is influenced by costs

The article is published in HCII 2021. This is the author's copy of the accepted version. The final authenticated version is available online at https://doi.org/10.1007/978-3-030-77392-2_20

associated with protective measures, where they have a general tendency towards delaying action until harm has occurred [41]. The study of Marques et al. [24] 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 [34,25,22], improving the security and usability of authentication schemes [5,8,3], developing automated techniques to detect unauthorized access to an account [21], and designing educational tools and warning system to prevent social engineering attacks [6,23,33]. 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? iii) How do users' strategies and contingency plans to protect their online accounts vary across geographic regions?

The study of Haque et al. [17] 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. Security and Privacy, being contextual, demand a situated understanding of user's perceptions and behavior in order to explore the design and policy practices [27,28,13]. Thus, it is important to investigate the security perceptions and behavior of users beyond Western contexts. In our study, we conducted semi-structured interview with 59 participants from three different countries, including Bangladesh (a developing country located in South Asia), Turkey (a developing country straddling Eastern Europe and Western Asia), and USA (a developed country in North America).

Contributions. Our findings reveal the unawareness and uncertainty of participants in taking appropriate steps once they lose access or identify an unauthorized access to their online account. In this context, we unpack the misconceptions of participants, which refrain them from taking security-preserving actions, or lead them to adopt prevention strategy that could put their online security into further risks. Our results shed light on the relation between users' security behavior to protect their online accounts, privacy concern with sharing personal information for secondary authentication (used to recover access to an account, like when password is forgotten [38]), and their perceptions of accessibility related to two-factor authentication. Taken together, our study contributes to advance the understanding of Security and HCI community on users' security vulnerabilities and usability challenges in protecting their online accounts.

2 Related Work

In this section, we first report the findings from prior studies on user's security perceptions and behavior, followed by a discussion on notable usable security and privacy studies conducted outside the Western regions.

The study of Ion et. al. [18] compared the online security practices of expert and non-expert users, where they found differences in their security behavior. For instances, expert users generally install updates, use password manager, and leverage two-factor authentication, where the non-expert users prefer to use antivirus application, change their passwords, and visit only the known websites [18]. Karunakaran et. al. [20] investigated users' expectations of how companies should respond to data breaches. The authors [20] found that users understand the risk of data leakage, and have certain expectations from the organizations in case of a data breach, which include sending users an immediate notification, enabling two-factor authentication, and resetting their passwords.

The study of Zou et. al. [41] focused on Equifax data breach, where the findings revealed users' perceived risks of data leakage. The authors [41] identified the factors that could influence users towards not taking a protective measure, which include but not limited to the optimism bias, procrastination until harms occur, and the costs of taking a security-preserving action. In a separate study [30], Ruoti et. al. found that users' security behavior depend upon their understanding of a threat, evaluation of risks, and the estimation of impact, where they select coping strategies based on their evaluation of the trade-offs between potential harms and the costs to take protective measures.

Although local values often contrast with the liberal notions of privacy and security embedded in current computing systems [4,1,11], the digital privacy and security research beyond Western contexts is still at its very early stage [12,37]. In a recent study [29], the author recruited participants from both within and outside of Western countries. The findings from this study [29] show that the user's behavioral response to a suspicious login attempt to their Facebook account depends upon their awareness, and mental model of the incident, where cultural background and past experiences could also influence their security decision.

Although online threats are global, perceptions of threat are very localized [4,16,36,11]. The study of Al-Ameen et al. [4] explored how users balance their needs, conveniences, and privacy in the context of data collection and sharing by smartphone apps, and unveiled how privacy leakage incidents affect app usage behavior in the Global South. The study of Haque et al. [16] shed light on how situated morality influence the privacy behavior of people in the digital service centers at Bangladesh. In a study conducted in urban Ghana [11], the participants reported confidence of being able to defend against cyberattacks despite passwords often being their only line of defense.

Digital devices, such as mobile phones that are designed for developing regions often fail to satisfy their local needs. In a study conducted with low-literate Berber women in Morocco [14], the authors identified that the lack of functional literacy presented significant barriers to using mobile phones. The

studies conducted by Ahmed et al. [2] and Sambasivan et al. [32] demonstrate that the mobile phones often do not have one-to-one mapping with a user in the resource-constrained settings of developing countries, where a recent study with the women in Global South [31] examined the privacy negotiation of female users from their family members while using a mobile phone.

Our Study. The findings from these studies indicate that 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.

3 Methodology

We conducted semi-structured interview with 59 participants. We recruited participants through sharing the study information via email and online social media, posting flyers on public places, snowball sampling, and leveraging authors' personal connections. We interviewed the participant over telephone, via Skype, or in person. Our study was approved by the Institutional Review Board (IRB) at our university.

3.1 Procedure

The interviews were conducted in the country's official language. That is, the interviews with the participants living in the USA, Bangladesh, and Turkey were conducted in English, Bengali, and Turkish, respectively. During the interview, we asked them a set of questions on online accounts, in particular, financial and identity accounts (e.g., email, social networking). Participants were asked about their past experience of losing access to their financial and identity accounts, identifying an unauthorized access to any of these accounts, and what protection steps they had taken in such instances. At the end, participants responded to a set of demographic questionnaire. The interviews were audio recorded. On average, each session took between 20 and 30 minutes.

3.2 Analysis

We transcribed the audio recordings. For the interviews with the participants from Bangladesh and Turkey, the researchers who are the native speaker of Bengali and Turkish translated the transcriptions into English. We then performed thematic analysis on our transcriptions [9,10]. Two researchers independently read through the transcripts of half of the interviews, developed codes, compared them, and then iterated again with more interviews until we had developed a consistent codebook. Once the codebook was finalized, two researchers divided up the remaining interviews and coded them. After all interviews had been coded, both researchers spot-checked the other's coded transcripts and did not find any inconsistencies. Finally, we organized and taxonomized our codes into higher-level categories.

Table 1. The Highlight of Participants' Demographic Traits [*Either completed or currently studying at the noted education level] **Note:** *UP*: Participants living in the USA; *BP*: Participants living in Bangladesh; *TP*: Participants living in Turkey

Gender	**Participants**
Male	BP1-BP3, BP6-BP9, BP11, BP15, BP17-BP29, UP1-UP4, UP7, UP8, UP10-UP12, UP14-UP16, UP18, UP20-UP22, TP1, TP3, TP4, TP6, TP8
Female	BP4, BP5, BP10, BP12-BP14, BP16, UP5, UP6, UP9, UP13, UP17, UP19, TP2, TP5, TP7
Age-range	
18-24	BP4, BP7, BP8, UP5, UP6, UP19, UP21, UP22
25-29	BP2, BP3, BP5, BP6, BP9, BP19, BP20, BP25, UP2, UP7-UP15, UP18, UP20, TP1-TP3
30-34	BP1, BP17, BP18, BP21, BP24, BP28, UP1, UP3, UP16, UP17
35-39	BP23, TP6
40-44	BP16, BP22, BP26, BP27, BP29, UP4
45-49	BP14, TP4, TP7
50-54	BP15, TP5, TP8
55+	BP10, BP11, BP12, BP13
Literacy Level*	
Fifth Grade	BP19, BP27, BP29, TP6, TP7
Between Eighth and Tenth Grade	BP17, BP20, BP22, BP24, BP25, BP26, BP28, TP4
Twelfth Grade	BP12, BP18, BP21, BP23, UP19, UP21, UP22, TP2, TP5, TP8
Undergraduate and above	BP1-BP11, BP13-BP16, UP1-UP18, UP20, TP1, TP3
Profession	
Student	BP4, BP5, BP7, BP9, UP1-UP3, UP6-UP14, UP18, UP19, UP22
Employee at Industry	BP1-BP3, BP6, BP8, BP11, BP17-BP19, BP21-BP29, UP5, TP3, TP4, TP6
Employee at Educational or Non-profit Org.	BP10, BP15, UP4, UP15-UP17, UP20, UP21, TP1
Car Driver	BP20
Housewife	BP12-BP14, TP2, TP5, TP7
Physician	BP16
Retired	TP8

3.3 Participants

Table 1 presents the demographic information of our 59 participants, where 16 of them are women, and 43 are men. Almost all of our participants were in the age range of 18 to 55, where four participants were above 55 years old. The literacy level of 39% of our participants was between fifth and twelfth grade, where others were either undergraduate students or had already earned the de-

gree. Thirty-two percent of our participants were students, where others were from diverse professions, including physician, car driver, housewife, and the employee at industry, educational institution, or non-profit organization. Among our participants, twenty two of them live in the USA, eight participants live in Turkey, and 29 participants live in Bangladesh. In this paper, the participants living in the USA, Bangladesh, and Turkey are denoted by *UP*, *BP*, and *TP*, respectively.

4 Results

Twenty-six (USA: 17, Bangladesh and Turkey: 9) out of 59 participants reported losing access, or identifying unauthorized access to their financial, or identity account, where we unpacked their strategies to regain access and protect their accounts. For other participants, we reported their contingency plan in case of losing access or identifying an unauthorized access in the future (see §4.3).

4.1 Losing Access to Online Account

Nineteen participants (USA: 12, Bangladesh and Turkey: 7) reported losing access to at least one of their financial, or identity (e.g., email, or social networking) accounts, where most of them could not recover the access. Below, we report our findings revealing why participants lost access to their accounts.

Lack or Failure of Secondary Authentication. Among the participants who lost access to their financial or identity accounts, about half of them including from all three countries reported that 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, UP19 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]."* UP15 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 UP3 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."*

BP20 could not recover access to one of his online accounts upon forgetting the primary authentication code where he also forgot the password of his email account that was registered for secondary authentication. UP1 commented, *"I lost like many times, I mean my email accounts"*. Including UP1, a few participants lost access to their online accounts multiple times due to forgetting their authentication codes. TP8 has reported, several online accounts require him to change his password once every three months, which makes it difficult for him to remember the new password.

Geographic Relocation. Several U.S. participants reported geographic relocation as the reason behind losing access to their online accounts. Many service providers block suspicious login attempts from an 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 [15]. 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 (UP17) 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.

UP15 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 reason 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.

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. BP5 reported an incident of losing access to multiple online accounts, where a social networking account, hacked by the adversary was linked to other accounts through a single sign-on feature. Most 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. UP4, 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.

BP10 reported an incident of robbery, where the attacker forcefully gained access to victim's bank account from his smartphone. In another instance, the attacker demanded ransom from BP20 over phone threatening our participant to ruin his reputation through posting inappropriate contents on the hacked social networking account.

4.2 Unauthorized Access to Online Account

Thirteen participants (USA: 7, Bangladesh and Turkey: 6) reported that they had identified 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, where most of others reported, they got aware of unauthorized access through email notification from the service provider. For

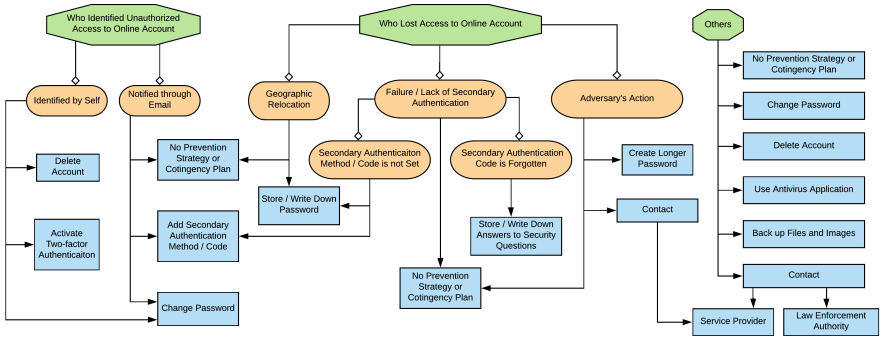

Fig. 1. Prevention Strategies and Contingency Plan of Our Participants

instance, UP1 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.

UP2 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 BP5 and UP18, where they received an email asking to change their authentication secret for a social networking account. UP12 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."*

TP8 reported that his bank account was accessed from a foreign country, incurring him financial loss. He suspects, he was a victim of phishing attack, where his bank account was accessed after he had provided his account information in a website that tricked him to believe that he had won a lottery.

4.3 Prevention Strategy & Contingency Plan

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

Who Lost Access to Online Account. UP15 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). UP1 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, UP9 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, UP4 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, including from all three countries 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, UP2 said, *"I cannot do anything."* Similarly, TP8 perceives that it is not possible to recover an online account if it is compromised by an adversary, in which case, the victim would need to create a new account. In this context, a few U.S. 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.

Who Identified Unauthorized Access. Among the participants from all three countries 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, a few participants 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.

Some participants do not have a clear idea about what steps they should take once an unauthorized access is identified, where UP18 said, *"I don't know what to do...what i am going to do. I don't know."* TP8 experienced unauthorized access to his bank account. Including him, a few other participants mentioned

the importance of being more careful about security issues, however, they were unsure of the strategy or plan that could protect their online accounts from unauthorized access in the future.

A few participants from Bangladesh and USA 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, UP13 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 UP21 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.

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 UP6 commented, *"They [adversaries] cannot get my password."* We identified uncertainty among participants from all three countries when we asked them about their contingency plan in case they lose access to an online account. Several U.S. participants mentioned, they would contact the tech support of the service provider, however, were not sure how to reach out to them. Here, UP22 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, several participants mentioned that they would change the password of that account. However, UP7 and TP6 also reported uncertainty if this step would be sufficient to protect their account from the adversary. In this context, UP10 and UP11 believe that the only way to protect an account is to delete it upon identifying an unauthorized access. UP10 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."* Similarly, several participants from Bangladesh and Turkey who did not lose access, or identify an unauthorized access to their online account,

mentioned that they would ask help from the law enforcement authority if they identify an unauthorized access to their online account in the future.

UP22 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.

5 Discussion

5.1 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 [40], 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 [6]. 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 [15], 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.

5.2 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 [19,40]. 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 [4]) 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 [35], 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.

5.3 Similarities and Differences across Geographic Locations

Our findings show that more U.S. participants, in comparison to the participants in Bangladesh and Turkey reported losing access or identifying unauthorized access to their financial, or identity account. Participants' responses on how they had identified an unauthorized access were similar across all three countries. While the lack or failure of secondary authentication, and adversary's action are reported by the participants from all three countries why they had lost access to their online accounts, only U.S. participants mentioned geographic relocation as the reason behind losing access to their account. It is possible, although we cannot confirm from our study, that the participants from Bangladesh and Turkey did not travel outside their country, and thus, did not experience losing access to an online account due to geographic relocation.

Overall, we found similarities in protection strategies across the participants from USA, Bangladesh, and Turkey. However, none of our participants from Bangladesh and Turkey reported activating two-factor authentication when an unauthorized access to their online account was identified, or contacting service provider in case of losing access to their account. We believe, further investigations are required in the contexts of developing countries, including Bangladesh

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

and Turkey to understand the availability and usability of two-factor authentication, and the scopes and challenges involved in getting help from the service provider when a user loses access to her online account.

6 Limitations and Conclusion

We interviewed 59 participants in our study, where we followed the widely-used methods for qualitative research [7,10,9], focusing in depth on a small number of participants and continuing the interviews until no new themes emerged (saturation). We acknowledge the limitations of such study that a different set of samples might yield varying results. Thus, we do not draw any quantitative, generalizable conclusion from this study. In addition, self-reported data might have limitations, like recall and observer bias.

Despite these limitations, our study unpacks the strategies of users to protect their online account, where we identified the unawareness, misconceptions, and accessibility and privacy concerns of users that refrain them from taking security-preserving steps. In our future work, we would conduct a large-scale survey with the participants from diverse age-groups and literacy levels to attain quantitative and more generalizable results.

References

1. Ahmed, S.I., Guha, S., Rifat, M.R., Shezan, F.H., Dell, N.: Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In: Proceedings of the Eighth International Conference on Information and Communication Technologies and Development. pp. 11:1–11:10. ICTD '16, ACM, New York, NY, USA (2016). https://doi.org/10.1145/2909609.2909661
2. Ahmed, S.I., Haque, M.R., Chen, J., Dell, N.: Digital privacy challenges with shared mobile phone use in bangladesh. Proc. ACM Hum.-Comput. Interact. **1**(CSCW), 17:1–17:20 (Dec 2017). https://doi.org/10.1145/3134652
3. Al-Ameen, M.N., Fatema, K., Wright, M., Scielzo, S.: The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 185–196 (2015)
4. Al-Ameen, M.N., Tamanna, T., Nandy, S., Ahsan, M.A.M., Chandra, P., Ahmed, S.I.: We don't give a second thought before providing our information: Understanding users' perceptions of information collection by apps in urban bangladesh. In: Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS'20). p. 32–43. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3378393.3402244
5. Al-Ameen, M.N., Wright, M.: Exploring the potential of Geopass: A geographic location-password scheme. Interacting with Computers **29**(4), 605–627 (2017)
6. Alsharnouby, M., Alaca, F., Chiasson, S.: Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies **82**, 69–82 (2015)
7. Baxter, K., Courage, C., Caine, K.: Understanding Your Users: A Practical Guide to User Research Methods. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2 edn. (2015)

8. Biddle, R., Chiasson, S., Van Oorschot, P.C.: Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR) **44**(4), 1–41 (2012)
9. Boyatzis, R.E.: Transforming qualitative information: Thematic analysis and code development. sage, Thousand Oaks, CA, USA (1998)
10. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology **3**(2), 77–101 (2006)
11. Chen, J., Paik, M., McCabe, K.: Exploring internet security perceptions and practices in urban ghana. In: Proceedings of the Tenth USENIX Conference on Usable Privacy and Security. p. 129–142. SOUPS '14, USENIX Association, USA (2014)
12. Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F., Kohno, T.: Computer security for data collection technologies. Development engineering **3**, 1–11 (2018)
13. Crabtree, A., Tolmie, P., Knight, W.: Repacking 'privacy' for a networked world. Comput. Supported Coop. Work **26**(4-6), 453–488 (Dec 2017). https://doi.org/10.1007/s10606-017-9276-y
14. Dodson, L.L., Sterling, S.R., Bennett, J.K.: Minding the gaps: Cultural, technical and gender-based barriers to mobile use in oral-language berber communities in morocco. In: Proceedings of the Sixth International Conference on Information and Communication Technologies and Development: Full Papers - Volume 1. p. 79–88. ICTD '13, Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2516604.2516626
15. Eldefrawy, M.H., Alghathbar, K., Khan, M.K.: Otp-based two-factor authentication using mobile phones. In: Proceedings of the 2011 Eighth International Conference on Information Technology: New Generations. p. 327–331. ITNG '11, IEEE Computer Society, USA (2011), https://doi.org/10.1109/ITNG.2011.64
16. Haque, S.M.T., Haque, M.R., Nandy, S., Chandra, P., Al-Ameen, M.N., Guha, S., Ahmed, S.I.: Privacy vulnerabilities in public digital service centers in dhaka, bangladesh. In: Proceedings of the 2020 International Conference on Information and Communication Technologies and Development. ICTD2020, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3392561.3394642
17. Haque, S.T., Wright, M., Scielzo, S.: A study of user password strategy for multiple accounts. In: Proceedings of the Third ACM Conference on Data and Application Security and Privacy. p. 173–176. CODASPY '13, Association for Computing Machinery, New York, NY, USA (2013), https://doi.org/10.1145/2435349.2435373
18. Ion, I., Reeder, R., Consolvo, S.: "...no one can hack my mind": Comparing expert and non-expert security practices. In: Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security. p. 327–346. SOUPS '15, USENIX Association, USA (2015)
19. Just, M., Aspinall, D.: Personal choice and challenge questions: a security and usability assessment. In: Proceedings of the 5th Symposium on Usable Privacy and Security. pp. 1–11 (2009)
20. Karunakaran, S., Thomas, K., Bursztein, E., Comanescu, O.: Data breaches: user comprehension, expectations, and concerns with handling exposed data. In: Symposium on Usable Privacy and Security. pp. 217–234 (2018)
21. King, M., Alhadidi, D., Cook, P.: Text-based detection of unauthorized users of social media accounts. In: Canadian Conference on Artificial Intelligence. pp. 292–297. Springer (2018)
22. Kothari, V., Koppel, R., Blythe, J., Smith, S.: Password logbooks and what their amazon reviews reveal about their users' motivations, beliefs, and behaviors. In: European Workshop on Usable Security (2017)

23. Lastdrager, E., Gallardo, I.C., Hartel, P., Junger, M.: How effective is anti-phishing training for children? In: Symposium on Usable Privacy and Security. pp. 229–239 (2017)
24. Marques, D., Guerreiro, T., Carriço, L., Beschastnikh, I., Beznosov, K.: Vulnerability & blame: Making sense of unauthorized access to smartphones. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–13 (2019)
25. Mayer, P., Volkamer, M.: Addressing misconceptions about password security effectively. In: Workshop on Socio-Technical Aspects in Security and Trust. pp. 16–27 (2018)
26. Miller, R.: That time i got locked out of my google account for a month (December 22, 2017), https://techcrunch.com/2017/12/22/that-time-i-got-locked-out-of-my-google-account-for-a-month/
27. Nissenbaum, H.: Privacy as contextual integrity. Wash L. Rev **79**, 119 (2004)
28. Patrick, A., Kenny, S.: From privacy legislation to interface design: Implementing information privacy in human-computer interactions. In: Privacy Enhancing Technologies. pp. 107–124. Springer, Springer Berlin Heidelberg, Berlin, Heidelberg (2003)
29. Redmiles, E.M.: "should i worry?" a cross-cultural examination of account security incident response. In: 2019 IEEE Symposium on Security and Privacy (SP). pp. 920–934. IEEE (2019)
30. Ruoti, S., Monson, T., Wu, J., Zappala, D., Seamons, K.: Weighing context and trade-offs: How suburban adults selected their online security posture. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). pp. 211–228 (2017)
31. Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L.S., Matthews, T., Consolvo, S., Churchill, E.: "privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 127–142. USENIX Association, Baltimore, MD (Aug 2018), https://www.usenix.org/conference/soups2018/presentation/sambasivan
32. Sambasivan, N., Rangaswamy, N., Cutrell, E., Nardi, B.: Ubicomp4d: Infrastructure and interaction for international development–the case of urban indian slums. In: Proceedings of the 11th International Conference on Ubiquitous Computing. p. 155–164. UbiComp '09, Association for Computing Machinery, New York, NY, USA (2009). https://doi.org/10.1145/1620545.1620570
33. Seng, S., Kocabas, H., Al-Ameen, M.N., Wright, M.: Poster: Understanding user's decision to interact with potential phishing posts on facebook using a vignette study. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. p. 2617–2619. CCS '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3319535.3363270
34. Stobert, E., Biddle, R.: The password life cycle. ACM Transactions on Privacy and Security **21**(3), 1–32 (2018)
35. Sukwong, O., Kim, H., Hoe, J.: Commercial antivirus software effectiveness: an empirical study. Computer (3), 63–70 (2010)
36. Sultana, S., Saha, P., Hasan, S., Alam, S.M.R., Akter, R., Islam, M.M., Arnob, R.I., Al-Ameen, M.N., Ahmed, S.I.: Understanding the sensibility of social media use and privacy with bangladeshi facebook group users. In: Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS'20). p. 317–318. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3378393.3402235

37. Vashistha, A., Anderson, R., Mare, S.: Examining security and privacy research in developing regions. In: Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS'18). COMPASS'18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3209811.3209818
38. Weiner, A.J., Ne'man, R.: Fallback identity authentication techniques (October 3, 2017), US Patent 9,781,105
39. Williams, C.: 620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts (February 11, 2019), https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/
40. Zhang-Kennedy, L., Chiasson, S., van Oorschot, P.: Revisiting password rules: facilitating human management of passwords. In: 2016 APWG symposium on electronic crime research (eCrime). pp. 81–90. IEEE, IEEE, Toronto, ON, Canada (2016)
41. Zou, Y., Mhaidli, A.H., McCall, A., Schaub, F.: " i've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 197–216 (2018)