Unraveling the Real-World Impacts of Cyber Incidents on Individuals

Danielle Renee Jacobs[1(✉)], Nicole Darmawaskita[2], and Troy McDaniel[3]

[1] School of Computing and Augmented Intelligence, Arizona State University, Tempe, AZ 85281, USA
danielle.r.jacobs@asu.edu
[2] The Polytechnic School, Arizona State University, Mesa, AZ 85212, USA
[3] School of Manufacturing Systems and Networks, Arizona State University, Mesa, AZ 85212, USA

Abstract. With the increase in ubiquitous technology and the rise in cyber threats, individuals are exposed to cyber events that can cause significant harm. Every individual is at risk, even those with expertise and experience. The cascading harms of a cyber-attack can lead to short-term and long-term consequences for the victim. The narratives that emerge from individual experiences with cyber threats paint a vivid picture of the prevailing harm landscape. Here, we describe a semi-structured interview study of 18 participants who were either victims of a cyber-related incident or have been exposed to threats, providing a more comprehensive picture of everyday people's challenges, harms, and needs. This paper examines the research question: What experiences do individuals face after a cyber-related incident? Several key themes are presented in this article.

Keywords: Cybersecurity · Human factors · Information security · Privacy · Usability · Cyber harm · Cyber risk

1 Introduction

Cybersecurity is increasingly becoming an issue for individuals as they rely on more information and communication technology (ICT). The unprecedented outbreak of the COVID-19 pandemic further amplified this issue, leading to an increase in phishing attacks through clickbait that focused on exploiting the hysteria [19]. Before the uptake in cybercrime, Americans had a 1 in 3 chance of being hacked; it stands to reason that the chances of being hacked have only increased [30]. Organizations, often faced with similar challenges, albeit at a very different scale, use modeling, risk assessments, statistical analysis, and technical expertise to inform policies that mitigate the harm of adverse events. Unfortunately, the average person does not have the tools or resources organizations

The authors thank Arizona State University and the National Science Foundation for their funding support under Grant No. 1828010.

A. Moallem (Ed.): HCII 2024, LNCS 14729, pp. 40–55, 2024.
https://doi.org/10.1007/978-3-031-61382-1_3

rely on to become more secure and, therefore, depends on software, hardware, and top-down policy solutions. The nuances and intricacies of harm are murky, particularly given limited data on the subject [13].

Prior work has examined what harms users' experience and sought to look at it through several different lenses. Often, prior research has focused on the impact of specific incidents on people [17,31]. For example, Zangerle and Specht [31] examined Twitter data to capture the impacts of Twitter account breaches on individuals. Previous work has documented mental models from cyberattacks with some discussion of harmful impacts [5,12,15] or explored the socio-technological relationships with technology in cyberspace [3,9,21]. Emami-Naeini et al. [9] looked at how security factors into Internet of Things (IoT) device purchase behavior and found that people reported security information difficult to find. Haney et al. [10] gathered user opinions about smart home devices and responsibility. According to the survey results, users and manufacturers are perceived to hold the most ownership in securing devices because of the knowledge manufacturers possess and the onus users take on when adopting a device. Bada and Nurse [4] provide a chapter summarizing cyber-attacks' social and psychological impacts to both individuals and organizations. Meanwhile, other authors have explored harms by examining the impacts of cyberbullying [6,7]. Scheuerman et al. [25] capture user experience with harmful content (e.g., Hate Speech, Violence) and have taken strides towards capturing the severity of harm. These efforts move the needle toward understanding the user experience and the near- and long-term consequences users suffer, but still miss capturing the impacts and stories across a variety of different threats. While targeted studies that look at technologies, demographics, or narrow types of harm are crucial to building human-centered cybersecurity policies and tools, it is also essential to document how incidents impact people.

By documenting real-world experiences, impacts, and harms, we take a step towards garnering valuable insights. These insights are critical in shaping meaningful policy and technical solutions. Before framing our study, we surveyed the literature to identify prevalent cyber threats users encounter. This list became the criteria for participation in the study. However, the data does not represent every type of cyber-related incident. Nevertheless, our diverse pool of respondents provides a citizen-centered picture of people's challenges, harms, mindsets, and needs.

Our research revolves around a central question: What experiences do individuals face after a cyber-related incident? Throughout the study, several themes emerged. Some of these insights echo previous studies, such as the need for cybersecurity education [26,29]. In contrast, some findings are unique to our research, like the frequent appeal from affected participants for a platform to share experiences and heighten awareness. The paper is the first in a series that translates the qualitative findings around experiences into a framework to help build better ways to understand harm.

2 Methods

We conducted a literature survey and 18 semi-structured interviews with victims of a cyber-related incident or individuals exposed to potential cyber incidents. The authors performed a literature review to catalog different cyber threats researchers have recorded users encountering. This list became one of the main criteria for participation in the study and helped to scope a broad topic down to previously documented experiences. Second, we interviewed 18 people who met the criteria about their experience. The interviews underwent several rounds of qualitative coding, emphasizing In Vivo, Thematic Analysis, and Narrative Coding [24].

2.1 Identifying Areas of Cyber Incidents

The authors examined the experiences and impacts on individuals reported in the literature through a literature review and open-coding process. This was to help better scope the interview questions and ensure that definitions used in the study reflected existing work. In particular, this literature review informed what the study considered a cyber experience and therefore influenced the criteria for inclusion into the study. The first author of this study performed the literature review. Search criteria included individuals, not groups, and terms like cyber-harm, cyber-incident, and cyber consequences of users. Incidents discussed across the papers included things such as harmful cyber online content, ransomware, scams, cyberbullying, data breaches. The final list is reflected in Table 1. It is important to note that these are not always mutually exclusive events.

Table 1. List cyber incidents reported across the surveyed papers. Experiencing an item in the list was a requirement to participate in the study.

Previously Reported Cyber Experiences
Email or Website Scam (Phishing)
Denial of Service (DoS)
Victim of Data Breach
Ransomware
Cyberbullying
Fraud or Identity Theft
Harmful Online Content
Invasive spyware, device recording, data usage
Virus, malware, data corruption
Physical loss or damage of computer, phone, device

2.2 Interview Design

Participants needed to be 18 years or older and experienced one of the cyber-events in Table 1 within the past 12-months. We chose a 12-month time frame because the literature reported that an event within 12 months was recent enough to have good recall but broad enough to find participants who qualify [6]. Another motivating factor for the 12-month requirement is the data variety. We could see the long-term impacts of participants nearer to a year since the cyber incident and the short-term emotions of participants whose experience is fresh. We also collected a short demographic survey to capture standard background information and details such as the interviewee's background with computers. To develop interviews that elicit narratives about the subjects experience, the interview questions focused on capturing the different impacts due to cyber-harms [2,25]. Two colleagues, who met the criteria, participated in a pilot study to test the interview protocol. The pilot led to integrating more targeted questions. After the final study design, we obtained Institutional Review Board (IRB) approval for human subjects research.

2.3 Participant Recruitment

Recruitment ran from September through October of 2023. We used social media posts, flyers, email, and snowballing to find participants. The initial study design aimed to collect 15 to 25 participants for the semi-structured interviews. These numbers are informed by previous exploitative qualitative interview research in cybersecurity [28,32]. Participants were compensated with a $50 Amazon gift card. The authors tried to recruit a collection of cyber-related experiences from Table 1. However, it was not an expectation to have an even distribution of experiences or every experience from the table represented, considering some types of experiences are much more prevalent.

2.4 Data Collection

We conducted 18 semi-structured interviews that ranged from 30–60 min via online video conferencing. During the interview, participants were asked questions about the recent cyber-incident, but allowed to discuss other incidents, even if the other incidents were older than 1 year. After the interview, the participants completed a short demographic survey. Each participant was assigned a study identification number. The transcript, video, audio, and survey were then named with the study number and not attached to personal data. Prior to the start of the recording, the participant's name in the video conferencing software was updated to match the identification number.

2.5 Interview Data Analysis

Analysis of interview data used an In Vivo Coding process. The primary coder performed two rounds of coding. The first cycle used In Vivo Coding on 10

interviews. The two coders met to review the results of the first cycle and then developed a codebook to group the data into thematic categories [24]. The discussion helped standardize definitions for the codes. For the data analysis, the team used QSR International's Nvivo Software [16].

The second cycle of coding used partner coding. In the second cycle, both coders used the established codebook on all 18 interviews. Throughout the process, if there were concerns over the initial codebook, including changes to definitions or new code suggestions, the two researchers met to discuss, align, and update the codebook. Table 2 shows the final codebook, resulting definitions.

Table 2. Final Codebook from the interviews.

Codebook	
Name	Definition
Needs	Necessities (governance, policy, justice, education, cultural, awareness, technology changes) subject identified because of the incident
Response	The way in which the participant reacted to the event. Includes both systemic responses (e.g., calling the bank) or personal responses (e.g., talking to friends)
Financial Harm	Impact to the subjects' finances
Operational Harm	Impact to how a subject usually operates
Physical Harm	Impact to the subjects' physical being or physical access or physical impact to the device
Psychological Harm	Impact to a subjects emotions, feelings, and psychology
Social Harm	Impact to how subjects interact with others

3 Results

In this section, we report the results from the surveys and interviews. For the interviews, we first report unique stories. After providing an overview of some of the interviews, we present the results of the coding process and thematic analysis.

3.1 Survey

Details of the survey results can be found in Table 3. One person did not answer the survey correctly, and the results for that participant have been omitted. Another participant did not submit an answer to the cyber experience survey question and, therefore, is not reported in the variable Cyber Experience. However, the subject's answers to other variables are included. Cyber Experience is reported as a count and all other results are reported as percentages out of 17

total participants, due to the one in-valid survey. The variable Cyber Experience was a self-reported question intended to capture the cyber-related experience the participant wanted to discuss. Participants were allowed to select multiple options for the question because the categories are not mutually exclusive. For example, a phishing attempt may be related to a data breach. In total, twelve participants selected more than one answer. Definitions and examples of the cyber experiences were provided to the participants in the survey. Nearly half of participants reported having previous training in information technology systems. The survey results also show a wide range of ages, education, and income.

Table 3. Survey Results

Variable	Results
Age	18–24 years (35%)
	30–34 years (29%)
	35–39 years (6%)
	40–44 years (18%)
	54–59 years (12%)
Gender	Man (29%)
	Woman (71%)
Level of Education	High school (6%)
	Bachelor's Degree (47%)
	Master's Degree (29%)
	Professional degree (18%)
Related Education	I have an education in or experience in computer science, computer engineering, or IT. (47%)
	I do not have an education in or experience in computer science, computer engineering, or IT. (53%)
Income	Under $15,000 (6%)
	$15,000 to $24,999 (12%)
	$35,000 to $49,999 (6%)
	$75,000 to $99,999 (12%)
	$100,000 to $149,999 (12%)
	$150,000 or above (35%)
	Prefer not to say (18%)
Cyber Experience	Email or Website Scam (Phishing) (8)
	Denial of Service (DoS) (3)
	Ransomware (0)
	Cyberbullying (3)
	Fraud or Identity Theft (including social media account hack/stolen) (7)
	Harmful Online Content (7)
	Invasive Spyware, Device Recording, or Data Usage (3)
	Virus, Malware, or Data Corruption (4)
	Physical Loss or Damage (1)

3.2 Interviews

This section presents the results of the 18 interviews. First, we present a profile of the experiences where similar incidents are grouped. Interview questions focused on the impacts and harms participants faced. Coding also focused on capturing financial, physical, social, operational, and psychological harms shared in the interviews. In presenting the experiences across different incidents, we rely on the different categories of harm to characterize the experiences. After profiling different stories, we review other thematic analysis results.

Profile of Experiences. One challenge academics face is finding good data and resources. For companies and governments cyber experiences are characterized in news reports and case studies [11]. These sources can be used to evaluate the impacts on organizations [2,4]. The same understanding and data should exist for individuals. This next section gives a profile of participants' experiences to fill the gap and provide a resource for researchers.

The Banking Incidents. There is no denying that financial fraud is a significant driver for cyber-criminals. The participants in this research were no exception. Out of the 18 participants in the study, 11 reported stories related to banking fraud. Of the 11 participants, seven discussed stolen credit card or debit card numbers. A participant who reported knowledge of being a victim of several high-profile data breaches also suffered the opening of illegal checking accounts in his name. Additionally, participants discussed threats to banking and payment applications, such as a hacked Venmo account.

Two participants included stories of older family members falling for social engineering attempts to gain access to bank accounts. In one narrative, P15's family member lost roughly $3,000 from retirement savings. Participant P05 shared a story of an older relative who nearly gave away her Unified Payment Interface (UPI) pin through a social engineering attack. In India, UPI allows multiple accounts to be managed on one interface and seamless fund transfers [20]. Most of these transfers require a UPI pin; if the criminal has enough information, the pin can serve as the final stopgap. Giving the pin away after already providing account information is paramount to giving away money. P05 interrupted the call with the scammer and prevented the pin from being leaked, thereby stopping the theft.

Most participants in this group reported no long-term financial loss due to the bank's ability to credit fraudulent purchases back to the individual. Only one participant, P15, discussed a significant financial loss because she could not help her older family member avoid a scam. Nevertheless, participants suffered financial loss in other ways. Many reported taking time from work or valuable personal time to deal with the issue. As one participant put it, *"but the time and effort spent to remedy the situation was significant" (P17).* The same participant suffered checking account fraud and raised a concern that, while he did not lose

money, he believed the accounts were likely used in money laundering. Participant P07, who reported a Venmo account hack, did not lose any money but had to spend time on her account responding to everyone the hacker contacted.

In credit and debit cases, participants often reported a slight impact on how they interact with friends and family. P09 reported challenges in repaying her boyfriend: *"It's definitely changed my relationship."* She reflected more on how limited funds impacted her other relationships, *"Then also, I feel like, during the time where my card was hacked, I had to cancel all the social things I planned because I didn't have any access to funds" (P09).* While the effects were not life-changing, they did cause inconvenience to friends and family. For participants who shared stories of older family members, the impact often resulted in more responsibility to assist the older adult. P05, who stopped his mother from giving the UPI pin to the criminals, reported that he and his familly built a new system where he checks any UPI requests for his mom.

In addition to the impacts on how the participants operated and interacted with friends and family, there were physical impacts reported by participants who had card fraud. For some, these physical impacts had workarounds, such as utilizing digital payment systems. Others were not so lucky. P09 had her account frozen, *"I called my bank to freeze it [the card], but the woman who I was talking to kind of confused me, and she put a hold on my entire bank account, not just that debit card".*

Participants suffered other impacts on how they usually operate due to the threats. People who suffered credit card and debit card fraud reported issues in accessing and using the cards. P10 reported, *"The week following it affected the speed through which I was able to do some things. Like if I wanted to order something on Amazon, if I wanted to refill my Starbucks card..."* Overall, participants who suffered banking-related incidents found it impacted the way they were able to use their money, *"I can't really figure out any other way to pay" (P07).*

Suffering through all of the impacts, participants reported several emotions. Among the most reported emotional impacts were anger and frustration. We found that seven of the banking related interviews mentioned emotions akin to anger and frustration at least once. For example, P12 remarked they, *"generally just felt frustrated."* Feelings of sadness, panic, and stress were shared among the participants. P17 highlighted the invasion of privacy that many participants reported, *"The initial reaction was, let's say, one of violation and shock because someone's using your personal information."*

Participants took a variety of actions. While many reactions to dealing with the situation vary from person to person, some responses stand out either by being a common response or as a mitigation technique. In the credit and debit card theft, the participants relied heavily on the banking system to help recover the stolen money. One participant recalled the bank's response, *"they were able to respond very quickly. Like in that moment, I spoke to like a real person, not just a machine. And he was able to reinstate a new card in that moment" (P10).* When working with older family members who experienced social engineering attacks

to gain access to bank accounts, P15 and P05 built-in checks to help family avoid scams in the future. Participant P17, who had checking accounts opened in his name, filed an affidavit with the police department. He then ensured that more checking and savings accounts could not be opened by using a service called ChexSystems to place a freeze. ChexSystems' website says, "A security freeze is designed to prevent approval of checking, savings, credit accounts, loans, or other services from being approved in your name without your consent" [8]. P17 also put credit freezes in place with the three major credit bureaus.

Phishing. In the interview pool, eight participants reported stories of phishing attempts. Of these phishing schemes, most were messaging-related scams or smishing. The smishing scams involved messages about package deliveries or banking alerts. Some phishing attempts overlap with card fraud or bank account theft, such as participant P08, who recalled, *"I got a text message that a package from UPS was being delivered, but it could not finish the delivery because it needed an updated address... Because of the change in location, there was a fee... you had to insert your credit card information in order to pay the small fee to get the package relocated. And I did it."*

Of the eight phishing experiences, only two participants discussed unique phishing scenarios. For one, an email phishing attempt used information from a previous data breach. Participant P01 described, *"the subject of that email was my old password that I had used across many different accounts, and websites, online platforms, different apps."* The phishing email threatened to share lies about P01 unless P01 sent Bitcoin to the scammer. Another participant, P04, was a victim of a phishing attempt on Discord that used a QR code.

Participants reported minimal financial impact, except for P15's family member who lost retirement savings. Other financial impacts took the form of time lost dealing with the phishing attempt and money spent on resources to protect information better. One participant recalled the time spent responding to the Discord hack: *"It did cost me a lot of time to fix all of the things that went wrong... people say time's money" (P04).* Other participants spent money on extra storage due to a large number of phishing scams, while another participant spent money on authentication tools to better protect accounts. For example, P01 described the benefit of purchasing a security service, *"if anything happens to my account, I'll be notified and now have a team of experts to reach out to, so that's one option that I took."*

Most participants impacted by phishing reported only minimum impacts to their social life. Most cited the time it takes to clean out phishing emails or concerns over more vulnerable family members. For example, P16 mentioned, *"a lot of close family members of mine, especially the people who are older, 60 plus... I've seen them falling for it" (P16).* The Discord QR Code hack, however, led to significant social consequences. Hackers sent inappropriate information to every contact P04 had on Discord. While close friends understood that P04 had been hacked, not everyone did. P04 reflected, *"It was just a stupid mistake on my side, and just a little embarrassing for me to tell my friends that this happened.*

Professionally, it did impact me, because I was kicked out of a few groups related to networking with tech communities." P04 suffered some of the more extreme social and professional impacts of those interviewed.

Study results showed that the experiences, even if participants do not fall for a phishing or smishing attempt, have a psychological impact. Three participants reported feelings of frustration. For example, one subject noted *"I get frustrated, to be honest, because I mean, these web, email services are trying their best to auto filter them from showing up in an inbox, but they still keep happening" (P16).* Stress was another common consequence, voiced by four participants. For example, the P04 commented, *"it was very stressful for me to deal with because, like, I didn't want to be the person that they associated this with."* Similarly, the email incident used password information in the subject line, leading to prolonged stress for P01, *"for two straight days, I was scared because it was my personal password."*

Participants did speak of habit changes to avoid falling victim again. P16 described the constant influx of phishing attacks: *"When I click on an email or click on any link, I have to re-check it multiple times to make sure that I'm not being phished. I think that adds a lot of overhead to my day-to-day life and how I operate."* Other participants discussed implementing practices to prevent future mistakes. P08, P15, and P11 described trying to read messages when more alert.

Participants took noteworthy actions to respond to the phishing attempts and prevent future incidents. Many participants attempted to research more information about the incident, including googling information about the phishing attempt. Others crowd-sourced information from family, friends, or more official institutions like banks. P08 reported a need to verify with those around, *"I make my husband look and read it and say, do you think this is real?"* P12 also needed too ask workers and friends before making a decision.

Online Harm. Outside the banking and phishing experiences, participants discussed various other cyber incidents online. This group of interviewees had other, more unique stories. Participants P17 and P06 spoke about their experience as a victim of a data breach. P17 mainly focused the interview on checking fraud, but noted his data had been impacted by several data breaches. One participant, P14, shared her story of cyberbullying, and another, P03, recounted her experience with an Instagram account hacker who held P03's account ransom.

While many participants did not experience any financial impact, among those who discussed data breaches, there was a sense that impacts could still be unknown. For example, a participant remarked, *"I'm just surprised that I haven't seen something come up for an account being opened in my name" (P06).* Meanwhile, the participant who experienced an Instagram account hack acknowledged that there could have been a financial impact had the response to the attacker gone differently. In response to the targeted online hate, P14 paid for a digital cleanup service to help her remove her digital presence, paying extra to ensure her family was also covered. P14 noted that she *"ended up shelling out a good deal of money for the utilization of this service."*

The participants who experienced a Instagram hack and cyberbullying recounted impacts on family and friends. The hacker who took over P03's Instagram account contacted all her family and friends, asking for money. She noted, *"I had to call many of my family through WhatsApp, and just tell them, 'Hey, listen, just be very careful because of the hacker"' (P03).* P14 noted that she had to protect her loved ones, like adding her spouse to the data online cleanup service and removing photos online. She reflected on removing photos with a family member: *"To protect her, I, you know, locked down and went private on all my various accounts" (P14).* In contrast, those who suffered only data breaches reported no significant social impact.

Participants reported changes in how they operate due to the incident. All of the participants spoke of long-term changes in habits. Once she got her Instagram account back, P03 noted, *"I get Instagram requests for friends, and I'm just hesitant to accept because I'm traumatized."* P03 goes through extra steps to verify that the person is her friend, like communicating verbally before accepting a request. P17 noted that after the checking account fraud and being a victim of numerous data breaches, he has methods in place to protect his credit, but this comes with more steps and does burden his ability to operate normally. For example, P17 confided, *"So if I want to buy a house, buy a car with credit, take out a new credit card, or open up a new checking account, I'm going to have to go through several additional steps to do that."* Finally, since essentially removing her online presence due to cyberbullying, P14 continuously thinks about what information is available online. She remarked, *"I will often try to look up and see what people can find about me if they really wanted to, with enough time."*

Participants described a variety of emotional and psychological responses to the experiences. There was no common feeling reported, but rather a range between the participants. P06 reflected she felt frustration, anger, and irritation at having her medical data exposed in a data breach. P03 reported feelings of violation after the account was hacked followed by concern and guilt for the people the hacker reached out to asking for money. P14 described feelings of isolation. She noted that during the incident, she *"felt afraid, felt kind of despondent and depressed" (P14).* All participants had negative emotions both in the moment and after the incident had passed.

Responding to the incidents took many different forms. P14 used a service to help clean up her information online and deleted her social media accounts. P03 relied on friends to help her login and remove all of the emails and phone numbers the hacker was using. Since the hacker could tell every time P03 tried to reset her account, P03's friend found when the hacker was offline. P03 and her friend used that time to take back her account and reset the password.

Other Social Engineering with Deep Fakes. Finally, the last incident discussed in the interviews was a hostage scam call asking for money. Participant P02 described her experience of receiving a call threatening her daughter's life if she did not continue to send money. The scammer used social engineering and deep fakes to make the situation believable. While not a traditional cyber-

incident, the use of online data to create the deep fakes and the money transfers made this experience a candidate for inclusion in our study. P02 did experience financial loss due to the experience, *"I ended up losing $500."* P02 described the experience as shock and fear. She also noted leaving work to deal with the call and losing valuable work time. It was her coworkers and husband who discovered that something was wrong. They worked to find her and inform her she was in the middle of a scam, indicating that the incident impacted P02's family and friends. In response to the experience, P02 has identified steps to prevent a similar scenario. For example, she suggested using a code word. P02 describes the idea, *"So our family all has a code word now... I would ask for that code word. And if the deep fake doesn't give it to me, then I'll know. So it's like a dual authentication."*

3.3 Themes

Besides coding for the different harms, we also focused on identifying beliefs interview participants discussed. It was surprising how often participants voiced similar needs and wants, even if they took slightly different forms. This section reviews what we found.

Raise Awareness. Five of the participants spoke of awareness. One participant spoke of concern for populations who might not be as aware of phishing attacks, *"So there are people who are not aware of the kind of phishing attempts that are going on; it's really easy to steal all of the information and financial data" (P18).* Four participants volunteered to participate in the study to call attention to their experiences and *"spread this story around as much as possible" (P02).* P01 told the interviewer, *"I wanted to spread what has happened to me; I just don't want anyone else to be part of such."* P04 had a similar motivation, *"I think there should be some kind of awareness that spreads saying that don't, you know, don't scan QR codes that you're not meant to scan."*

Education. Education was another common theme in the interviews. While education can be very similar to awareness, it was essential to separate them. In the interviews, education appeared in the context of formal training, such as integrating cybersecurity into school. P09 reflected that cybersecurity should be taught as a life skill in the classroom. Similarly, P16 mentioned that "education will be more important in this space for everyone that is using the web." After her experience getting hacked, P03 learned about password strength and best practices from a friend, reflecting that learning to protect herself was important.

Justice. Finally, the interviews demonstrated people believe that the government needs to put more effort into holding criminals accountable. When reflecting on money stolen in an online scam from years ago, P12 mentioned, *"I wish that person would go to jail."* For others, there was a wish to be able to find out

how the incident even occurred. For example, P09 mused, *"I do wish they could be held a little bit liable, or I wish I could at least have the resources to track down the source of how they got my information."* P17 noted that the checking fraud, while illegal, is only a misdemeanor. P16 was passionate about systemic solutions to this problem, *"so there needs to be tighter control... when it comes to web-related security, we don't have tighter regulations yet."* While some participants complained about the lack of support and regulation, others explained how good it would be to get revenge or justice. For example, *"I would literally pay to know what his facial expression was,"* P03 mused after she got her account back from the hacker.

4 Discussion

Other user-focused research has looked at how aware participants are of data breaches [17], beliefs on IoT device security [10], how vulnerable populations are affected by tools and security best practices [1,18,27], how threat models impact understanding of an account breach [23], how stories impact how users understand security [22], and even how mental models can be generated to understand security [5,14]. This research adds to the prior work by capturing the experiences of victims and those exposed to cyber threats, providing a more comprehensive picture of everyday people's challenges, harms, and needs. We found that there is a wide variety of experiences, but users often experience immediate and long-term harm.

Participants valued awareness and education after the experience. When asked about ways to raise awareness, P04, who suffered the Discord hack, recommended that platforms such as Discord take a more proactive approach to raise awareness. P04 also mentioned that social media influencers, such as a Gaming YouTuber P04 follows, have a platform to raise awareness. As P04 put it, *"Maybe the YouTuber can talk about instances like this... because that he's the one bringing people in, so he can also like give a disclaimer on what could happen. What could go wrong."*

There may be other avenues to raise awareness. One participant noted that she spoke about her experience on the news to help call attention to the issue. Since we saw that googling was a typical response among participants, Google search could help build broader knowledge by pointing to trusted resources. News sources, podcasts, and other information outlets can also release segments about cybersecurity to raise community awareness.

As academics, we have the opportunity to research new ways to integrate cybersecurity awareness and education into existing structures. There is a need to understand the impacts of technology. As one interviewee put it, *"I think that all technology that's developed, we should put it to the test and say how is this going to be a benefit to humanity rather than so many ways that you could use it as a weapon" (P02).*

Participants called for the ability to understand how the incident happened in the first place, hold criminals accountable, and build policies protecting users

online. The community should re-examine how we think of cybercrime. Currently, cybercrime is too hard to track or too petty of a crime for legal attention. From these experiences, we see that there are real impacts, and as cybercrime rises, it is essential to find ways to hold criminals accountable.

This work is limited to a relatively small sample size of 18 interviewees. However, the number of participants is informed by previous qualitative interview research in cybersecurity [14,28,32]. Increasing the participant pool can help develop more generalized findings. Future work will seek to apply inter-rater reliability scores to the codes to verify that the codes accurately represent the intended topics. This work also focused on recruiting users who recently experienced a cyber threat, although users were allowed to discuss other experiences. Future improvements may look across a larger time scale. That would provide more context on an attack's short- and long-term impacts.

While there are limitations to this work, it takes a step and documents the consequences users suffer from different cyber incidents. Understanding the consequences across different attacks helps characterize the environment and risks. Researchers often use documented real-world case studies to demonstrate the new frameworks when understanding the cyber landscape in organizations and governments. These user experiences may serve as case studies of users to support similar analyses.

5 Conclusion

This research describes the experiences 18 participants faced after a cyber incident, focusing on the harms and consequences. We also highlight the areas of change participants voiced, such as more education, awareness, and governance. Prior efforts take steps toward understanding the user experience but are limited by narrow scope. We provide breadth by discussing several cyber-attacks and how the attacks impacted participants. Based on the results, we suggest areas of future research. The authors will use this study to understand and represent the harms that humans experience in cyberspace.

References

1. Abdolrahmani, A., Kuber, R.: Should i trust it when i cannot see it? Credibility assessment for blind web users. In: ASSETS 2016 - Proceedings of the 18th International ACM SIGACCESS Conference on Computers and Accessibility, pp. 191–199. Association for Computing Machinery, Inc (2016). https://doi.org/10.1145/2982142.2982173
2. Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S., Upton, D.: A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. **4** (2018). https://doi.org/10.1093/cybsec/tyy006
3. Ahmed, T., Shaffer, P., Connelly, K., Crandall, D., Kapadia, A.: Addressing physical safety, security, and privacy for people with visual impairments. In: Proceedings of the 12th Symposium on Usable Privacy and Security, SOUPS 2016, p. 341 (2016). https://www.usenix.org/conference/soups2016/technical-sessions/presentation/ahmed

4. Bada, M., Nurse, J.R.: The social and psychological impact of cyberattacks. In: Emerging Cyber Threats and Cognitive Vulnerabilities, pp. 73–92. Elsevier (2020). https://doi.org/10.1016/b978-0-12-816203-3.00004-6
5. Bravo-Lillo, C., Cranor, L.F., Komanduri, S.: Bridging the gap in computer security warnings: a mental model approach. IEEE Secur. Priv. **April**, 18–26 (2011)
6. Camacho, S., Hassanein, K., Head, M.: Cyberbullying impacts on victims' satisfaction with information and communication technologies: the role of perceived cyberbullying severity. Inf. Manag. **55**(4), 494–507 (2017). https://doi.org/10.1016/j.im.2017.11.004
7. Cao, B., Lin, W.Y.: How do victims react to cyberbullying on social networking sites? The influence of previous cyberbullying victimization experiences. Comput. Hum. Behav. **52**, 458–465 (2015). https://doi.org/10.1016/j.chb.2015.06.009
8. Security freeze information. https://www.chexsystems.com/
9. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring how privacy and security factor into IoT device purchase behavior. In: Conference on Human Factors in Computing Systems - Proceedings, pp. 1–12 (2019). https://doi.org/10.1145/3290605.3300764
10. Haney, J., Acar, Y., Furman, S.: "It's the company, the government, you and I": user perceptions of responsibility for smart home privacy and security. In: Proceedings of the 30th USENIX Security Symposium (2021). https://www.lexico.com/en/definition/responsibility
11. Ashley madison revisited: legal, business and security repercussions. Infosec Institute (2015). https://resources.infosecinstitute.com/topics/news/ashley-madison-revisited-legal-business-and-security-repercussions/
12. Ion, I., Reeder, R., Consolvo, S.: "...No one can hack my mind": comparing expert and non-expert security practices. In: Proceedings of the 11th Symposium on Usable Privacy and Security, pp. 327–346 (2019)
13. Jacobs, D., McDaniel, T.: A survey of user experience in usable security and privacy research. In: Moallem, A. (ed.) HCII 2022. LNCS, vol. 13333, pp. 154–172. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-05563-8_11
14. Krombholz, K., Busse, K., Pfeffer, K., Smith, M., von Zezschwitz, E.: "If HTTPS were secure, i wouldn't need 2FA"-end user and administrator mental models of HTTPS. In: IEEE Symposium on Security and Privacy (SP), vol. 2019-May, pp. 246–263. IEEE (2019). https://doi.org/10.1109/SP.2019.00060. https://ieeexplore.ieee.org/document/8835228/
15. Lin, J., Amini, S., Hong, J.I., Sadeh, N., Lindqvist, J., Zhang, J.: Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, UbiComp 2012, pp. 501–510. Association for Computing Machinery, New York (2012). https://doi.org/10.1145/2370216.2370290
16. Nvivo (2020). https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home
17. Mayer, P., Zou, Y., Schaub, F., Aviv, A.J.: "Now i'm a bit angry:" individuals' awareness, perception, and responses to data breaches that affected them. In: 30th USENIX Security Symposium (USENIX Security 2021), pp. 393–410. USENIX Association (2021). https://www.usenix.org/conference/usenixsecurity21/presentation/mayer
18. McDonald, A., Barwulor, C., Mazurek, M.L., Schaub, F., Redmiles, E.M.: "It's stressful having all these phones": investigating sex workers' safety goals, risks, and practices online. In: Proceedings of the 30th USENIX Security Symposium, pp. 375–392 (2021)

19. Naidoo, R.: A multi-level influence model of COVID-19 themed cybercrime. Eur. J. Inf. Syst. **29**(3), 306–321 (2020)
20. UPI: Unified payments interface - instant mobile payments | NPCI (2024). https://www.npci.org.in/what-we-do/upi/product-overview
21. Pearman, S., Zhang, S.A., Bauer, L., Christin, N., Cranor, L.F.: Why people (don't) use password managers effectively. In: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security, SOUPS 2019, pp. 319–338. USENIX Association, USA (2019)
22. Rader, E., Wash, R., Brooks, B.: Stories as informal lessons about security. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS 2012. Association for Computing Machinery, New York (2012). https://doi.org/10.1145/2335356.2335364
23. 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 (2019). https://doi.org/10.1109/SP.2019.00059
24. Saldaña, J.: The Coding Manual for Qualitative Researchers, 4th edn. SAGE Publications Limited, Thousand Oaks (2021)
25. Scheuerman, M.K., Jiang, J.A., Fiesler, C., Brubaker, J.R.: A framework of severity for harmful content online. Proc. ACM Hum.-Comput. Interact. **5**(CSCW2) (2021). https://doi.org/10.1145/3479512
26. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J.: Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2010, pp. 373–382. Association for Computing Machinery, New York (2010). https://doi.org/10.1145/1753326.1753383
27. Simko, L., Lerner, A., Ibtasam, S., Roesner, F., Kohno, T.: Computer security and privacy for refugees in the united states. In: 2018 IEEE Symposium on Security and Privacy (SP), pp. 409–423 (2018). https://doi.org/10.1109/SP.2018.00023
28. Soneji, A., et al.: "Flawed, but like democracy we don't have a better system": the experts' insights on the peer review process of evaluating security papers. In: 2022 IEEE Symposium on Security and Privacy (SP), pp. 1845–1862 (2022). https://doi.org/10.1109/SP46214.2022.9833581
29. Vitak, J., Liao, Y., Subramaniam, M., Kumar, P.: "I knew it was too good to be true": the challenges economically disadvantaged internet users face in assessing trustworthiness, avoiding scams, and developing self-efficacy online. Proc. ACM Hum.-Comput. Interact. **2**(CSCW) (2018). https://doi.org/10.1145/3274445
30. Walsh, R.: Why There is a 1 in 3 Chance You'll get Hacked in 2016 (2016). https://proprivacy.com/privacy-news/get-hacked-one-in-three
31. Zangerle, E., Specht, G.: "Sorry, i was hacked": a classification of compromised twitter accounts. In: Proceedings of the 29th Annual ACM Symposium on Applied Computing, SAC 2014, pp. 587–593. Association for Computing Machinery, New York (2014). https://doi.org/10.1145/2554850.2554894
32. Zeng, E., Mare, S., Roesner, F.: End user security & privacy concerns with smart homes. In: Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, SOUPS 2017, pp. 65–80. USENIX Association, USA (2017)