AFRL-RI-RS-TR-2020-112

TOWARD A STANDARD MODEL FOR THE COSTS OF CYBERSECURITY ATTACKS

UNIVERSITY OF ILLINOIS

JULY 2020

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2020-112 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
CHAD D. HEITZENRATER
Work Unit Manager

/ S /
JAMES S. PERRETTA
Deputy Chief, Information
Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
JULY 2020	FINAL TECHNICAL REPORT	SEP 2018 – DEC 2019

4. TITLE AND SUBTITLE

TOWARD A STANDARD MODEL FOR THE COSTS OF CYBERSECURITY ATTACKS

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
FA8750-18-1-0076

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Christopher Kanich, Jason Polakis, Sameer Patil, and Huixin Tian

5d. PROJECT NUMBER
DHSE

5e. TASK NUMBER
CO

5f. WORK UNIT NUMBER
N1

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

University of Illinois
851 S Morgan St
Chicago IL 60607-7053

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIG
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2020-112

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Our research agenda set out to build a better understanding of the harms caused by cyber attacks at the scale of individual users. To that end, we mined real-time open source intelligence feeds to better characterize the harms that cause users to seek help on the open Internet. These investigations led to a better understanding of the broad distributions of various types of data, monetary, and temporal harm visited upon users.
Additionally, a broad understanding of the harmful impact of cybersecurity incidents requires an investigation of how people characterize and cope with these adverse experiences in general. To that end, we conducted semi-structured interviews with 21 individuals who reported a variety of cybersecurity incidents, consequences, and coping mechanisms. We found that the experiences can be characterized along a bounded to fuzzy spectrum. As the majority of current cybersecurity efforts focus on relatively bounded incidents, we make the case that fuzzy incidents deserve similar attention because their harmful impacts are deeper and longer-lasting. Our insight can be applied to improve and personalize the delivery of cybersecurity interventions, and unearthed a potential strategic link between general (rather than applied) cybersecurity education and cybersecurity best practice adherence.

15. SUBJECT TERMS
Cybersecurity, incident severity, cybersecurity metrics

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			CHAD D. HEITZENRATER
U	U	U	UU	28	19b. TELEPHONE NUMBER (*Include area code*) N/A

TABLE OF CONTENTS

1 SUMMARY

This work consisted of two joint efforts to better characterize the impacts and extents of cyber harms at the level of individual victims. The first effort modeled time loss, money loss, and chance of success at remediating cyberattacks. During this research, we pursued a visualization strategy for this data in order to better characterize and model cybersecurity attacks. The team prototyped multiple visualizations to use to derive insights from the mined data. In Section 4 we show one of these prototypes. Overall, while we found that there is a broad and reasonable distribution of losses to various forms of cyberattacks, the open source intelligence data available for understanding and accurately modeling the full extent of cyberattack severity distribution would be insufficient for the goals of this project.

The second effort centered on deeply understanding the human results of this research and is the focus of the outputs of this research project. We designed a screening and interview protocol which focused on fully enumerating the various types of harm that could come to users as a result of cyber incidences, along with a better understanding of the magnitude of those harms. We conducted semi-structured interviews with 21 individuals who reported a variety of cybersecurity incidents, consequences, and coping mechanisms. We found that the experiences can be characterized along a bounded to fuzzy spectrum. Our main insight from this research is that many of the more traditionally understood forms of cyberattacks can be considered “bounded” cyberattacks in the minds of participants, like phishing and ransomware. These “bounded” attacks cause real harm for users, but do not leave significant impacts on the behavior of the participants. Rather, so-called “fuzzy” attacks like cyberstalking and online harassment are “lumped in” with more traditional cyberattacks when discussing harm that comes to users as a result of using information technology. Interestingly, because of the difficulty with which these attacks are attributed or stopped by the victim, their “fuzzy” nature leads to a much larger feeling of lack of control over the cyber domain for these individuals, leading to withdrawal from the use of information technology. This insight suggests that improved education regarding socio-technical online defenses against things like cyberstalking or harassment might lead to a better cybersecurity posture and outcomes for users when faced with bounded and fuzzy threats alike.

2 INTRODUCTION

Cybersecurity has become an integral aspect of technology, affecting everyone regardless of their technical knowledge or efficacy. At its core, cybersecurity is about preventing harm to users as well as engendering a sense of trust that enables them to use technology safely. Yet, the ubiquity and volume of cybersecurity problems coupled with the tendency to gravitate toward easy-to-characterize and/or high profile attacks could potentially be crowding out investigations of harder-to-measure but no less harmful issues. We contend that a ground-up investigation of lived cybersecurity experiences is required to reveal gaps in the current understanding of the impact of cybersecurity incidents on people's lives. Understanding how users conceptualize, suffer from, and cope with adverse cybersecurity events is the first step toward prioritizing research and development of effective countermeasures. To that end, we report on a broad investigation of adverse experiences with technology with cybersecurity as the focal point.

To surface a wide variety of harmful events, we adopted an open perspective not limited to preexisting definitions of cybersecurity incidents. Since the public's knowledge of cybersecurity is far from complete or standardized, our approach enables an understanding of cybersecurity matters as they are experienced by end users rather than how they are defined by experts. Moreover, trust is an important component of cybersecurity; even if an event does not fit the traditional definition of a cybersecurity incident but lowers trust in technology, it should still be treated as important for the purposes of creating effective cybersecurity countermeasures.

Specifically, we tackled the following research questions:

1. How can open source intelligence allow us to characterize the variety and extent of cybersecurity harms?
2. How can open source intelligence be visualized to better characterize and model cybersecurity harms?
3. How are people's characterizations of adverse experiences with technology connected to cybersecurity?
4. What are the personal consequences of adverse cybersecurity experiences?
5. How do individuals cope with these consequences?

Research questions 1 and 2 were explored but produced negative results. We briefly introduce their methods in Section 3.1; however this investigation was inconclusive, and effort was instead directed toward determining the results of research questions 3, 4, and 5.

We addressed the above questions via semi-structured interviews with 21 individuals. Based on the insight from these interviews, we show that lived experiences of cybersecurity are shaped by negative perceptions and adverse experiences with technology, in general. Importantly, we found that people connect cybersecurity to a diversity of issues along a spectrum with ends that we label as bounded and fuzzy. Bounded incidents are those for which users have reasonably clear conceptualizations and mitigation strategies, and fuzzy are those whose contours and solutions are amorphous or unclear. Our findings suggest that people find fuzzy issues more challenging and stressful. Yet, estimates of cybersecurity incident impacts, especially those cast in economic terms, do not typically include long-term individual consequences of fuzzy issues. Based on this investigation, we make the following contributions:

Broadening the scope. We found that cybersecurity-relevant aspects are intertwined with a diverse set of incidents related to technology. Hence, an ecological treatment of the matters can help bring assessed damages of cybersecurity incidents in better alignment with their true long-term real-world impact.

Assessing the damage of cybersecurity incidents. We propose assessing cybersecurity incidents by placing them along a spectrum ranging from bounded to fuzzy. We show that cybersecurity incidents on the fuzzy side are sources of fear and anxiety caused by ongoing or even unrealized-but-potential threats that impact user decision making and well-being.

Surfacing indirect and long-term impacts. Our findings reveal various indirect and long-term impacts of adverse cybersecurity experiences, such as resignation, distrust, withdrawal, etc.

3 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 OSINT MINING AND VISUALIZATION

The core methods for exploring research questions 1 and 2 were to operationalize a more production-ready version of the preliminary analysis presented in (Amini & Kanich, 2017). To that end, we built a web scraping pipeline for the Bleeping Computer technical assistance forum that can continually perform incremental crawls of the data available from that discussion forum where many users of windows machines would come to request assistance in cleaning up malware infections.

For research question one, regarding the variety and extent of cyber harms to this population, we built heuristic-based models to determine the amount of self-reported time and money lost by users who asked for assistance on this discussion forum, as well as an estimate of how many of those requesters successfully resolved their requests for help.

In an exploration of an approximately five year dataset, we found that of those who reported an amount of time lost was non-trivial but non-substantial, with a median value of three days. These results are shown in Figure 1. Likewise, the median claimed amount of money lost was $100, with an overall distribution shown in Figure 2.

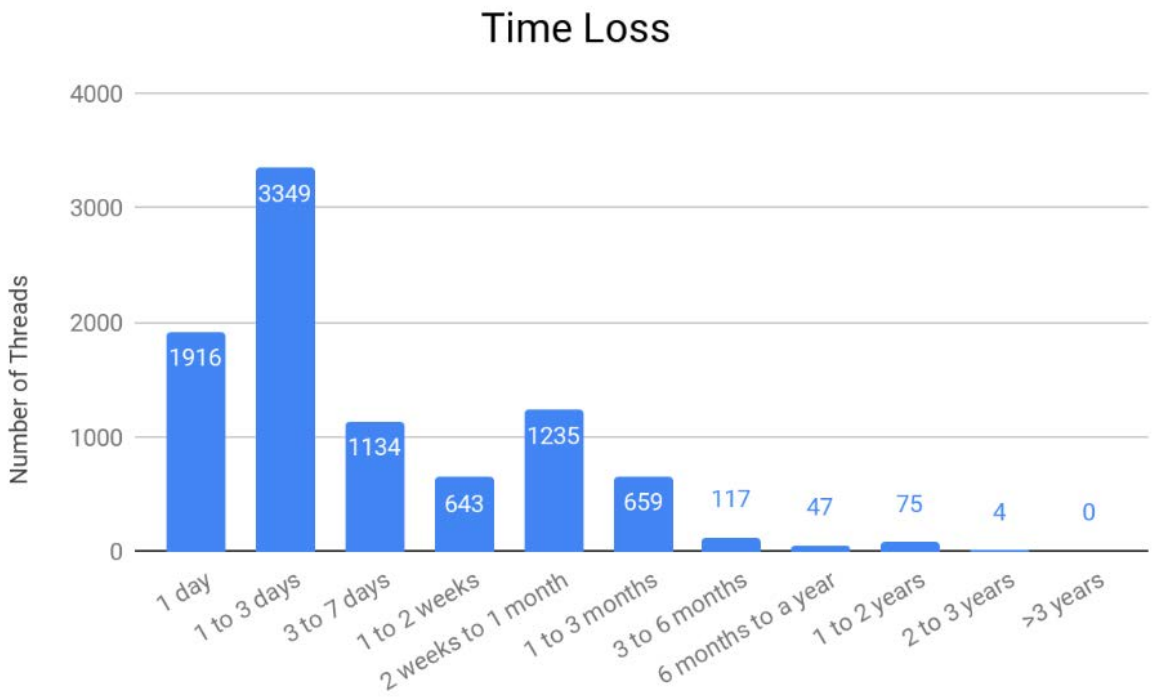

Figure 1. Self-reported time lost as a result of malware infection.

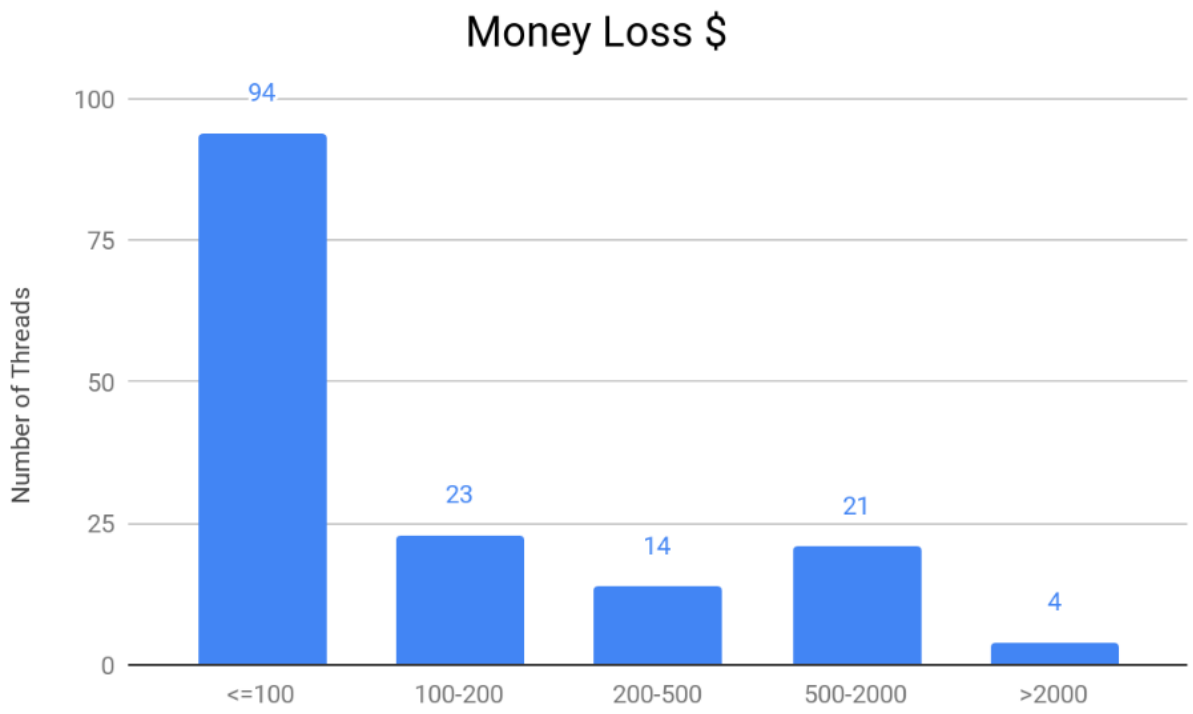

Figure 2. Self-reported money lost as a result of malware infection.

Alongside working on this data pipeline and analysis task, we had the opportunity to use visualization to more deeply investigate this data. As the data consists of hundreds of thousands of rows and somewhat high dimensions, and the analysis task is concerned with finding overall trends or correlations within that data, the parallel coordinates plot was chosen among several contenders as the most relevant data visualization technique. An example using our live collected data is reproduced here in Figure 3.

While this data visualization is effective at splitting out the high dimensional data, the overall trends were inconclusive. Likewise, the data analysis of the up-to-date data did not provide any deeper insights than provided by the preliminary results. Due to the abbreviated timeline of the overall research effort, the team decided to devote the majority of their resources to expanding upon and completing the research surrounding answering research questions 3-5.

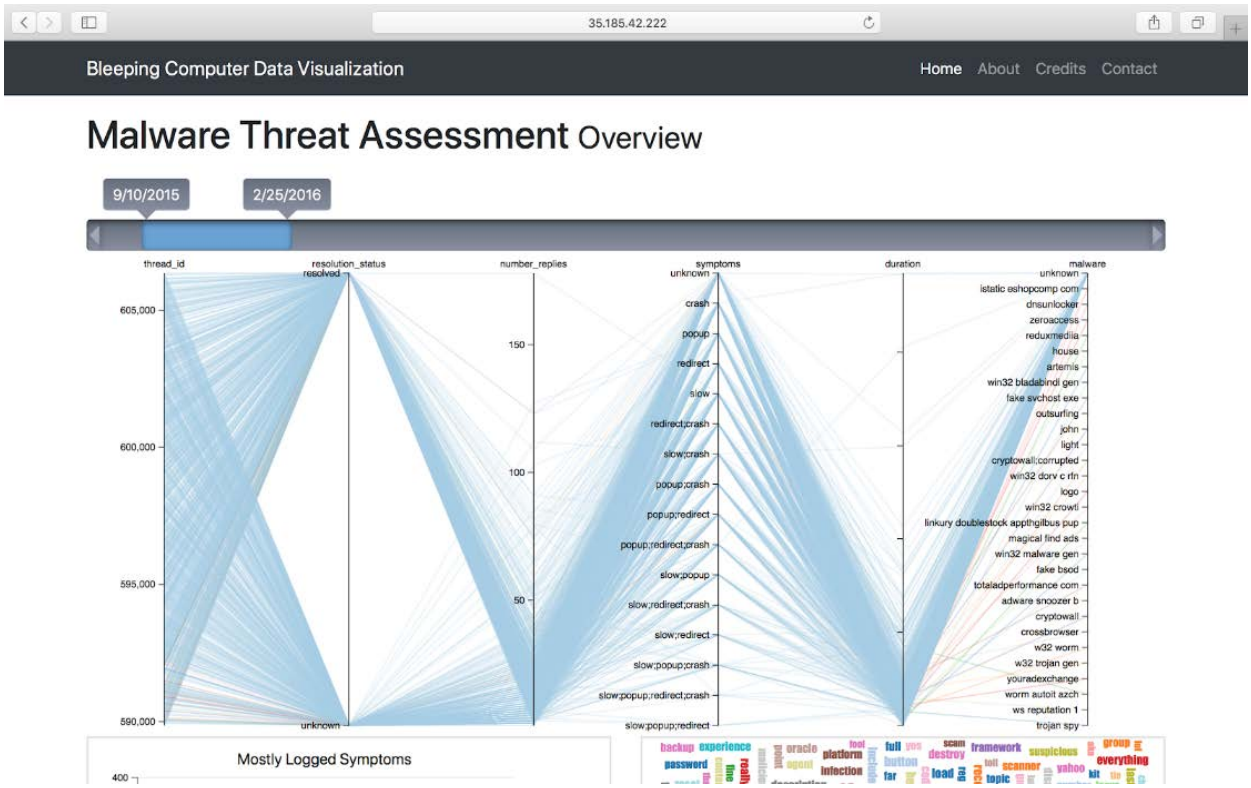

Figure 3. Parallel coordinates plot example for malware remediation forum data.

3.2 INTERVIEW-BASED INCIDENT HARM EXPLORATION

To address our research objectives, we conducted semi-structured interviews with 21 individuals who had indicated one or more adverse cybersecurity experiences. To avoid priming, we framed the study without revealing our specific interest in cybersecurity. The following subsections provide details of our recruitment and study procedures along with the characteristics of our sample. All study materials and procedures were approved by our Indiana University's Institutional Review Board (IRB).

Recruitment and Screening. We recruited participants during Spring and Summer 2019 via flyers posted across Bloomington, Indiana. In addition, we posted advertisements on online forums and mailing lists. The flyers and advertisements included a link to a screening questionnaire. To ensure truthful responses, the questionnaire did not reveal the screening criteria. We limited participation to those 18 years of age or older who reported one or more adverse cybersecurity experiences from a list compiled based on the collective expertise of the authors. Further, we selected interviewees such that the sample would be as diverse as possible in terms of demographics, professions, technical expertise, etc.

Participants. As expected in a university town, the sample contained a large proportion (~60%) of undergraduate and graduate students. However, the participants cover a broad age range (21-78) and a diversity of fields and occupations. Nearly a quarter (5) were town residents not affiliated with the university. One-third of the participants were from minority ethnic backgrounds. The sample contained slightly more females than males (8 male, 12 female, and 1 non-binary).

Interview Protocol. Each interview lasted 45-60 minutes. With consent, we audio-recorded the interviews for transcription and analysis. A graduate student conducted the first seven interviews as a course project (six in-person and one via online conferencing). These initial seven interviews broadly covered any negative experiences with technology to facilitate an open-ended early exploration. Based on the analysis of these initial interviews, we revised the interview protocol to sharpen the focus on adverse experiences with technology, their impact on people's lives, and their connections to people's backgrounds. The first seven interviews underscored that people's characterizations of cybersecurity incidents cover a broad spectrum, and the corresponding personal experiences are deeply contextual. Therefore, in subsequent interviews, we encouraged participants to share stories of specific incidents and followed up with questions focusing on behavior, short-term and long-term impacts, and connection to other aspects of their lives. The goal of asking participants to recall stories was to stimulate their reflection for comprehending their own experiences and enable them to engage actively in joint knowledge production. The subsequent 14 interviews using the revised protocol were conducted in-person by the first author. We provide the interview protocol in an Appendix.

4 RESULTS AND DISCUSSION

Our broad investigation of lived cybersecurity experiences revealed a complex picture of attribution, resolution, and coping strategies influenced by age and technical efficacy, connecting cybersecurity to a diverse variety of adverse experiences with technology.

Table 1. Cybersecurity incidents reported by each participant.

ID	Phishing/ Spam	Viruses/Malware/ Hacking	Scam/Ransom/ Blackmail	Unauthorized use of bank accounts/cards	Unpleasant encounters on social media	Online tracking/ Collection of personal information	Stalking
4	✓	✓		✓	✓	✓	
6	✓	✓				✓	
7	✓	✓				✓	
8	✓	✓					
10	✓	✓				✓	
12	✓	✓	✓				
16	✓	✓			✓	✓	✓
19	✓	✓		✓	✓	✓	
22	✓	✓			✓	✓	✓
34	✓	✓	✓				
37	✓	✓		✓		✓	
47	✓	✓		✓		✓	
57	✓	✓		✓	✓	✓	
58	✓	✓		✓	✓	✓	
59	✓	✓		✓			
65		✓			✓		
68	✓	✓			✓		
69	✓	✓		✓	✓	✓	
71	✓	✓	✓	✓	✓		
79	✓	✓		✓			
88	✓	✓		✓		✓	
TOTAL	**20**	**21**	**3**	**11**	**10**	**13**	**2**

4.1 DIVERSITY OF CYBERSECURITY INCIDENTS

Table 1 shows the major cybersecurity incidents reported by each participant. Notably, each reported multiple incidents, with every participant affected by malicious software or actors and nearly every participant encountering phishing or spam. On the other hand, blackmail was reported by only two participants. When narrating their experiences, all participants expressed negative emotions, such as frustration, anger, anxiety, annoyance, etc. Such an orientation sometimes translated to cybersecurity

being connected to seemingly unrelated adverse aspects of using technology, such as addiction to devices, services, or apps.

We found that the growing volume and variety of cybersecurity incidents leads to frustration as well as a sense of inevitability or resignation. This reveals a crucial complementary dimension to prior reports of users' feelings of resignation due to the abundance of cybersecurity-related advice, guidelines, and requirements (Stanton, Theofanos, Prettyman, & Furman, 2016) (Turow, Hennessy, & Draper, 2015). Ten out of 21 participants believed that adverse experiences are unavoidable in the current technological environment; P69 described such problems as a part of life: “I feel like it's just kind of part of life, like bullying's always been a part of high school. But now since we have Facebook and stuff, it's just going to happen online…I'm kind of in the space where I grew up most of my life with a lot of technology…it's just part of life, so it feels normal that sometimes my credit card is going to be stolen or I know that I got viruses on my computer.”

Resignation can dissuade people from attempting to diagnose and fix the issues they face. Some, however, choose to rely on experts, as indicated by P4: "Maybe I haven't learned the lessons of the last 5 or 10 years. But experts in that field have maybe learned those lessons so that I could go to those sources of information ... maybe I can go through a checklist of things that I can do better ... just because I am not an expert. But I know that other people are experts and care about this issue ... So to me it seems logical that there's a lot of effort put into [solving the problems]."

Alternatively, people rely on technology to address such issues on their behalf. People further expect the technological solutions to be simple, comprehensible, and useful, as noted by P47: "If it's not easy to use then it's potentially not helpful. If you can't figure out how to use it, how is it going to help you?" To this end, eight of the interviewees believed that appropriate training would be beneficial or mentioned having benefited from training, echoing the findings of prior studies on the positive effects of training (e.g., for avoiding phishing (Kumaraguru, et al., 2009)). Additionally, when asked how she dealt with the worries and anxiety created by these experiences, P79 responded: "I think just learning more about technology and different things like spam filters and how phishing schemes and hacking work. The IT people in our company did a little presentation about that just so we would all be aware. I just make sure that I go to those and I'm engaged, just trying to learn more, so I can feel more comfortable, like accessing different things on the Internet."

Participant responses indicated that their characterizations of cybersecurity incidents fell along a spectrum anchored at one end by incidents that we characterize as Bounded and at the other end by those we term as Fuzzy.

4.2 BOUNDED INCIDENTS

Bounded incidents have well-defined boundaries such that they can be circumscribed and limited to specific periods, systems, devices, events, etc. Matters such as malicious software, phishing, hacking were often experienced and characterized in these terms. Moreover, a clear solution to the problem is often available. Although these types of incidents are the ones most commonly covered by the media and cybersecurity research, we discovered that participants found them comparatively less stressful. All participants reported finding a solution when faced with a relatively bounded incident. For instance, remediation options can be found in online forums dedicated to helping users recover from malware infections (Amini & Kanich, 2017).

More than half of the participants reported bounded incidents involving unauthorized access to their bank accounts and/or credit cards. Interestingly, the vast majority (9 out of 10) solved the issues through the respective financial institutions. Their losses ranged from small amounts to hundreds of dollars, causing anxiety and negative emotions. As P71 reported: "Somebody got hold of my ATM card and spent $500 on a dating site. So that's why I'm a little panicky now. ... I was married at the time, so why would I go to a dating site?" Notably, the participants could not provide clear or conclusive explanations regarding the origins of the unauthorized access.

Typically, participants did not incur financial costs for addressing bounded incidents because free solutions or software were adequate for resolving the issue. Only three participants needed to purchase software to clean their infected devices. However, we identified more extreme remediation approaches as five participants purchased a new device instead of fixing an infection. Yet, they treated the purchase as a routine device upgrade rather than the cost of a cybersecurity incident. Only P88 reported financial burden and emotional frustration due to a large amount of money spent to fix a bounded incident. This was counter to our expectations, as we anticipated a larger number of participants expressing strong negative emotions regarding monetary expenses incurred to handle cybersecurity incidents. This may be attributed to the aforementioned view on the unavoidable nature of such incidents, and users' becoming more resigned to such costs.

While security experts often classify cybersecurity incidents based on operational characteristics, we found that the same kind of incident can vary in terms of its crispness, thus leading to a variation in "boundedness." For instance, P34 recounted an incident where a pop-up alerted him that his machine was infected with a virus, and he was asked to call a phone number to resolve the issue. This type of scam, referred to as a technical support scam (Miramirkhani, Starov, & Nikiforakis, 2016), typically aims to deceive users into providing remote access to their machines. In this case, P34 stated that the scammer already had access to his machine but simply gave up after he refused to pay: "So I call the number. I come to find out it was a scam to get money. This guy actually had access to my laptop. He was going through there and doing all this stuff. ... He can even disable my laptop so that I couldn't do anything on it. I said I ain't gonna pay you $99. I just refused, and all of a sudden, my laptop started working again. They were just trying to give me the scare to get me to pay $99 ... I was wondering how he was able to manipulate my computer." While the participant ultimately suffered no monetary loss, others may have paid and/or experienced disruption, resulting in the same kind of incident differing in boundedness across users and situations.

Bounded incidents can cause substantial damage. However, the silver lining is that users are often aware that an attack is taking place, which is a necessary precondition for resolving the problem. Even if a victim does not fully understand the technological mechanism, the stress caused by the attack is relatively muted, and the harms related to it are primarily lost time and money. Interestingly, those who reported the loss of a device as an adverse experience (except P16) were much more worried about the possibility of the data falling in the wrong hands and leading to the leakage of private information than about the considerable personal inconvenience or monetary costs.

4.3 FUZZY INCIDENTS

In contrast to bounded incidents, several reported incidents were amorphous, where operational detail and boundaries were ambiguous, fluid, unclear, or unknown. We consider such experiences as fuzzy incidents, which typically include tracking of online activities, privacy violations, and unpleasant online encounters in general. These issues often do not have clear-cut solutions as the issue or the problem itself is often not clear-cut to begin with.

Participants reported considerable difficulties and stress in dealing with fuzzy incidents, indicating uncertainty, insecurity, and confusion. When people felt unable to understand and solve an issue, they resorted to denial or avoidance as coping strategies. In this regard, participants engaged in a wide range of practices. On the one hand, P22 ignored the issue as an unavoidable aspect of online activities: “I'm not the best person in dealing with insults and harassment ... One of the most effective ways that I have found to deal with people who want to make your life difficult is just to ignore them." Similarly, P79 chose passive acceptance, justifying it by pointing to a lack of agency: "“My biggest negative thing is some kind of ignorance, not knowing a lot about many different viruses. ... I think I just haven't done enough research to know if there are license agreements or terms ... if the antivirus software runs out at a certain time, do I have to renew it? Going back to ignorance and me not doing enough back end research, I just don't know how that works. I guess ignorance is bliss in some ways." On the opposite end, P65 was driven to complete withdrawal: "I don't post on Twitter or Facebook, and I deleted everything that I thought was kind of iffy. Yeah, so I don't post anything, that's why there's no cyberbullying." Similarly, P71 did not want to "play the game" and deleted her Instagram account and used a pseudonym on Facebook.

Nonetheless, not participating may not be as feasible for younger participants, given the more ubiquitous use of social media among younger individuals (McAndrew & Jeong, 2012). Further, cyberbullying incidents can have severe repercussions, as highlighted by P19: "I know a kid in my high school who attempted suicide because of cyberbullying ... Someone kept reaching out to him on Facebook, like attacking all his posts, messaging mean stuff. ... It was kind of crazy. They created fake accounts to message him." Indeed, studies have linked the use of social networking sites to depression in younger populations (Błachnio, Przepiórka, & Pantic, 2015) (Jelenchick, Eickhoff, & Moreno, 2013) (Tandoc, Ferrucci, & Duffy, 2015), and users frequently encounter cyberbullying, meanness, and harassment on these platforms (Rosenthal, Buka, Marshall, Carey, & Clark, 2016) (Cao, Khan, Ali, & Khan, 2019) (Saeidi, da S. Sousa, Milios, Zeh, & Berton, 2020).

Online tracking (Englehardt & Narayanan, 2016) was among the most common fuzzy incidents reported by the participants, leading to concerns about how sensitive data about their activities was collected and used by various entities. For instance, six participants were bothered by social media advertisements being based on their Web search history even though they did not comprehend or grasp the complexities of the ad ecosystem. The annoyance reported by our participants regarding the collection of their information for advertising echoes findings of prior studies on advertising that cover targeting based on sensitive traits (e.g., substance abuse, race, etc.) or other potentially sensitive user information (Lécuyer, et al., 2014) (Datta, Tschantz, & Datta, 2015) (Venkatadri, Lucherini, Sapiezyński, & Mislove, 2019) (Andreou, et al., 2019). Redmiles et al. (Redmiles, Kross, & Mazurek, How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior, 2016) have similarly reported that confusion about targeted ads creates the feeling of being watched. Some participants expressed their worries as a larger concern about personal information becoming profitable for businesses without consent (P19, P58, P68) and available for governmental surveillance (P58, P69).

The abundance of information explicitly shared online by users (e.g., in social networks (Polakis, et al., 2010) or discovered through other means (Snyder, Doerfler, Kanich, & McCoy, 2017) can lead to stalking, online and/or in the physical world (Gross & Acquisti, 2005). For instance, P22 talked about an individual who tracked down his workplace and showed up to confront him over a denied rental application; the harassment briefly continued over email. P22 outlined the additional security-related precautions he took to protect his online accounts, recounting the use of "a code generator that helps

protect the account from being hacked" and "really long passwords" that are frequently changed and stored in a fingerprint-protected note on his smartphone.

In another case, P16 recounted a traumatizing online stalking experience that lasted several years and significantly affected her online behavior. Specifically, a person located overseas followed her mother's blog when she was a kid and systematically started contacting her and following her online accounts: "When I was 16, he somehow found my Facebook without my full name being on my mom's blog. ... He sent me a happy birthday message. ... We blocked him on Facebook. Then on my 18th birthday ... he messaged me again." The participant continued mentioning the different services where the stalker located and messaged her, even when she used distinct handles. This experience resulted in her making all accounts private and being suspicious of all incoming messages which had a negative effect on her overall experience and resulted in the rejection of connection requests from actual friends: "So I have to change all my handles for Instagram and Snapchat and Twitter, and now I'm set to private so no one can see my posts or follow me or message me without me approving it. That's really frustrating. ... I have to be so careful what I post, and I don't post any pictures of my house or anything unless I'm inside. I don't put any full name on my posts." These experiences highlight the shortcomings of current countermeasures to defend against such incidents.

4.4 GENERATION GAP

We found that participants' reactions and actions to adverse experiences were impacted by age and technical efficacy (which are correlated characteristics (Lauricella, Cingel, Blackwell, Wartella, & Conway, 2014)). Specifically, we found notable differences between the experiences of those born before 1980 and those born later. The latter group came of age as the personal computer and Internet were gaining traction and reaching ubiquitous adoption and is referred to as "digital natives" (Prenksy, 2001).

While fuzzy incidents were greatly stressful for both generations, bounded incidents were less troublesome for the younger generation. The disparity stems largely from differences in technical knowledge and efficacy. For instance, prior work has found a correlation between efficacy and security-related behavior pertaining to phishing (Sun, Yu, Lin, & Tseng, 2016). Younger participants tried to find solutions by turning to various online resources, such as forums, technical support pages, etc. In contrast, older participants tended to rely on offline resources, such as volunteers in public libraries, technology support events in community gatherings, etc. Even so, three of the older participants had limited knowledge of offline public resources for dealing with technology challenges. Since age is correlated with technical efficacy and capabilities, our findings corroborate prior results showing that the ability to obtain security-related advice depends on a user's skill level (Redmiles, Kross, & Mazurek, How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior, 2016).

Younger participants were much more likely to experience a loss of productivity due to incidents that led to a temporary or permanent loss of their device(s). Compared to older participants, younger participants tended to approach cybersecurity matters with a somewhat cavalier and passive attitude, as reflected by the frequent occurrence of expressions like "there is nothing to be done." In contrast, older participants reported active protective steps such as being mindful when sharing information (P58, P88), turning trackers off (P88), and minimizing the use of "unnecessary" services. As P34 stated: "I still don't [pay bills online]. I still like to do that the old-fashioned way. ... I was born in the 60s. You pay your bills in person, that way you know they're paid. I've bought stuff on Amazon, but I've never paid bills on the Internet."

P58 highlighted privacy concerns regarding data collection because it can facilitate mass surveillance and enable radical policing based on tracking people: "I think it's good that Google offers a way where you can look at what data they have on you, what data they're collecting. Right now, my phone is tracking my location. I don't want you tracking my location. ... They're doing the facial recognition thing in China, and they're going to do it at major airports in the United States." This is a valid concern as prior research has demonstrated real-time tracking attacks not affected by the location privacy countermeasures deployed in popular services (Polakis, Argyros, Petsios, Sivakorn, & Keromytis, 2015). Moreover, location information enables the inference of other sensitive information (Drakonakis, Ilia, Ioannidis, & Polakis, 2019) (Patil, Norcie, Kapadia, & Lee, 2012) including social ties (Backes, Humbert, Pang, & Zhang, 2017). P58 knew of privacy-invasive practices by foreign and local governments, reflecting the public's increasing awareness and concern regarding government-driven data collection.

Correspondingly, younger participants expressed smaller emotional reactions to adverse experiences, casting them as an unavoidable aspect of using modern technology and the Internet: "If somebody bad wants to access it, there are leaks and hacks that happen all the time. I might as well take advantage of the convenience of doing all the online stuff because it's not going to change." Older participants took these experiences less lightly and exhibited greater anxiety and confusion, corroborating prior reports on the challenges and confusion that older adults face when using technology (Hawthorn, 2007) (Broady, Chan, & Caputi, 2010).

Importantly, the two generations differ in regards to the long-term impacts of cybersecurity incidents. Long-term considerations for the younger generation are typically about making relevant adjustments to their practices, such as avoiding certain topics on social media. In contrast, older individuals are likely to lose confidence in their ability to use technology in general. Older people typically need to expend significant effort in learning to use technology, and even small setbacks accumulate and lead to long-term loss of confidence. Yet, older participants reported that resources to learn about the use of technology, which are needed for overcoming the loss of confidence and dealing with cybersecurity incidents, are often unsuitable for older adults, who typically need them the most. As a result, older people are likely to suffer greater disruption to their lives from cybersecurity incidents and may even be specifically targeted by malicious actors. For example, P71 narrated a story about a ransomware attack experienced by her father: "He was in his 80s when this [ransomware attack] happened. He was not really tech-savvy, but he would use the computer for his little business. He called me ... he said, `you know, somebody wants money to give me my computer back.' I said, `Don't give them any money.' He was on the phone with these people for six hours, and I think he ended up giving away $200 before he called me."

However, digital natives are not necessarily well-prepared and knowledgeable (Hargittai, 2010). Although no young respondent reported difficulties in learning about technology, P79, an account manager whose work involves intensive use of digital communication tools, reported worries and fears owing to a lack of knowledge of risks and dangers of the online environment. She was concerned that her knowledge and preparation would not be enough to avoid harmful cybersecurity incidents: "There's always a kind of fear that [hacking] could happen. At my work, there were things that we got kind of trained on by our IT team, making sure to watch out for suspicious links or emails from people who weren't us or emails from people impersonating someone else. ... I think just kind of the fear of phishing scams or not knowing if links are acceptable to click on or if attachments are going to have a virus in them. ... So far, for the most part, I have avoided any major crises, but I am always worried that I could easily click on something or open something that might have a virus I don’t know about."

4.5 DISCUSSION

It should come as no surprise that the participants viewed the cybersecurity aspects of technology in a negative light. These matters were a source of stress and anxiety and often found to be opaque in terms of attribution and operation. The differences based on age, which is often a proxy for differences in technical efficacy, were along the lines noted in the literature (e.g., (Nicholson, Coventry, & Briggs, 2019)).

Our contribution surfaces the details of the disconnect between users' lived experiences and experts' impact assessments. One of the highlights of our findings is the recognition that people seem to lump a diversity of issues under the single umbrella of "cybersecurity-related matters" that fall along a bounded-fuzzy spectrum. It should be emphasized that bounded and fuzzy are not binary categorizations based on specifics of the technology, but intended to anchor two ends of a spectrum. For instance, depending on the situation or the user, a virus infection could be a bounded incident resolved quickly with a virus scan or a fuzzy one that leads to a loss of personal data and subsequent identity theft. For example, one participant reported a virus that enabled a hacker to take control of his machine and demand ransom. Whether an incident is bounded or fuzzy is based not on the technological detail (i.e., viruses) but the experience of the user. Similarly, cyberbullying could turn out to be more bounded than fuzzy. Our point is that understanding where an incident may fall along the spectrum can facilitate a more accurate and nuanced assessment of end-user impact.

There have been other attempts to categorize cybersecurity issues. For example, Kim et al. (Kim, Jeong, Kim, & So, 2011) created a taxonomy of technology-centric matters, such as spam emails, malware, and phishing, and non-technology-centric matters, such as scams, cyberbullying, and misinformation. In contrast to such classifications based on technical detail or specific concepts defined by cybersecurity experts, our spectrum is grounded in the experiences as described by end users. We call for incident characterization, prioritization, and response to be adjusted appropriately based on the placement of an incident along the bounded-fuzzy spectrum. Our findings suggest that attention should given to the personal characterizations of an incident. We argue that such an approach is instrumental for surfacing the true costs borne by end users and can yield a more accurate judgment of the real-world impact of an incident.

Typically, most research efforts and media stories on cybersecurity focus on a single issue (e.g., malware) or a discrete event (e.g., data breach). While such a focus is important--in fact, participant characterizations of bounded incidents were similar to such a focused orientation--it deals with issues that people find less stressful and easily addressable. Part of this is most likely a result of greater exposure and experience with these issues over the years as their prevalence and reporting has continually grown. Our findings suggest that further gains in user education for practicing better "cybersecurity hygiene" would require increased attention to fuzzy incidents, which tend to involve greater social and behavioral considerations and require a sociotechnical approach for resolution.

Further, dealing with the interconnectedness and long-term impacts of cybersecurity incidents described by the participants requires an ecological orientation that situates cybersecurity matters within specific contexts of the users' lives. As our findings show, the impact of the same issue can vary noticeably across individuals depending on factors such as age, occupation, technical efficacy, financial means, etc. Moreover, the impact may involve indirect and long-term effects such as loss of self-confidence, technology avoidance, etc. However, users currently do not have easily understandable and personalized metrics that help them gauge the potential impact of various cybersecurity issues, especially for fuzzy incidents. For instance, nudges to encourage secure practices and/or discourage potentially harmful

actions can be presented as potential savings or losses in terms of time, money, effort, etc., respectively, wherein the values of these metrics are personalized to the individual user.

In the cybersecurity discourse, incidents are a common unit of analysis, applied at the societal and/or the individual level. Consequently, characterizations of an incident drive prioritization and resource allocation for appropriate response and, in turn, measurements of its impact. Therefore, it is important that the impact of an incident be understood appropriately. Most estimates of impact typically cover only a specific event (e.g., a spear phishing attack) and are reported in the aggregate over a large population. Further, the estimates are generally framed in terms of loss of money or time. While time and money metrics are certainly useful, our findings suggest that they are not adequate. Additionally, the short-term focus of these metrics ignores indirect and long-term effects, thus likely underestimating the overall impact of an incident by a significant amount. Moreover, the judgments are derived by cybersecurity domain experts, typically without input from end users. Our findings can bridge this important gap. In that vein, the bounded-fuzzy spectrum reflects how end users view these matters. For users, the emotional and cognitive impact (Modic & Anderson, 2015) of fuzzy incidents is far more salient compared to bounded incidents that result in short-term pain or are ignored altogether.

The resignation and passive acceptance reported by some participants is a cause for alarm, especially since such attitudes were expressed by the younger generation. In this regard, greater exposure to technology seems to be a double-edged sword; it increases technical efficacy and comfort at the same time creating long-term "security fatigue (Stanton, Theofanos, Prettyman, & Furman, 2016) due to constant exposure to adverse incidents. The inability to deal with these problems may also be due to a lack of adequate user agency, leading to a sense of inevitability and resignation. P69 said: "I think I'm on the very end of the millennials ... was born in 95. So I can understand the anxieties. It's just that I don't feel very anxious about it. I know there are always different ways that people hurt other people [online]. It's just our reality." Boosting user agency by educating and incentivizing users to take more active steps regarding cybersecurity matters will require multidisciplinary solutions covering technology as well as public policy. Our findings suggest that the younger generation may benefit the most from such efforts. P57, a young male who is relatively mindful and active in coping with cybersecurity issues, suggested: "I think it's more reactive as opposed to proactive. We do things to minimize the risk as much as possible, but I think some of it is just inevitable. So we just watch closely and make sure that nothing bad is going on."

Our findings suggest that the approach to cybersecurity guidance needs significant improvement when it comes to those who are not digital natives. Many of these individuals have needed to spend time and effort in learning the basics of technology; needing to learn about cybersecurity on top creates a significant challenge. As P71 reported: "My dad used to open every single email that ever came to him, because he didn't know better. ... He was very trusting. ... He thought that they were trying to help him fix it." Based on our findings and prior studies, we suggest that cybersecurity training and solutions be customized based on age and technical efficacy.

The practices of our participants indicate that technology is viewed as a means to an end, thus resulting in relatively less attention to specific devices and technologies and more to the tasks and the data. Devices may be seen as expendable, as evidenced by those who upgraded the device as a solution to fixing a malware infection. P59 suggested this choice was encouraged and enhanced by product design: "It [infection] might seem like an incentive to buy a new device rather than fixing the current product. ... I know that Apple products are designed pretty intentionally not to be open to the user in the same way that other computer products are ... it's almost impossible to repair sometimes without specialized tools. ... Oftentimes, it's cheaper to just buy a new phone ... depending on what's going wrong." Interestingly,

device purchases are opportune moments for prompting changes in security behavior (Parkin, Redmiles, Coventry, & Sasse, 2019).

Surprisingly, data loss was rarely mentioned as a cybersecurity incident, perhaps because of the increasing use of cloud services for storage and backup. This may explain why only 4% of ransomware victims reported paying the ransom (Simoiu, Bonneau, Gates, & Goel, 2019). On a positive note, fluid device switching makes it possible to create convenient solutions for bounded issues limited to a specific device. Still, accessing data and services via multiple devices creates interdependencies and increases the attack surface. Yet, typical cybersecurity solutions operate with a single-device per user assumption and may overlook the larger attack surface.

5 CONCLUSIONS

We address three separate, yet complimentary, dimensions: people's characterizations of adverse cybersecurity experiences, their perceptions of the severity of the ensuing harms, and their coping strategies in future interactions with technology. Our work suggests that classifying cybersecurity incidents along a bounded-fuzzy spectrum can be useful for gauging their harmful impact and determining appropriate mitigation strategies, especially for non-experts. To that end, our findings make the case for personalized cybersecurity metrics and mitigations that incorporate individual differences in the nature and severity of the experienced harm. Considering user trust and comprehension in system design and cybersecurity communication is crucial for avoiding adverse cybersecurity experiences being treated as an unavoidable fait accompli of technology use. Otherwise, we risk non-experts being exposed to increasing harm in a technology-saturated world.

6 REFERENCES

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies, 42*, 249–274. doi:10.1086/671754

Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., . . . Upton, D. M. (2016). Cyber harm: Concepts, taxonomy and measurement. *Saïd Business School WP, 23*.

Amini, S., & Kanich, C. (2017). Characterizing the impact of malware infections and remediation attempts through support forum analysis. *2017 APWG Symposium on Electronic Crime Research (eCrime)*, (pp. 70–78).

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., . . . Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-39498-0_12

Andreou, A., Silva, M., Benevenuto, F., Goga, O., Loiseau, P., & Mislove, A. (2019, 2). Measuring the Facebook Advertising Ecosystem. *NDSS 2019 – Proceedings of the Network and Distributed System Security Symposium*, (pp. 1–15). San Diego, United States.

Backes, M., Humbert, M., Pang, J., & Zhang, Y. (2017). Walk2friends: Inferring Social Links from Mobility Profiles. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and*

Communications Security (pp. 1943—1957). New York, NY, USA: Association for Computing Machinery. doi:10.1145/3133956.3133972

Błachnio, A., Przepiórka, A., & Pantic, I. (2015). Internet use, Facebook intrusion, and depression: Results of a cross-sectional study. *European Psychiatry, 30*, 681–684. doi:https://doi.org/10.1016/j.eurpsy.2015.04.002

Blackwell, L., Dimond, J., Schoenebeck, S., & Lampe, C. (2017, 12). Classification and Its Consequences for Online Harassment: Design Insights from HeartMob. *Proc. ACM Hum.-Comput. Interact., 1*.

Broady, T., Chan, A., & Caputi, P. (2010). Comparison of older and younger adults' attitudes towards and abilities with computers: Implications for training and learning. *British Journal of Educational Technology, 41*, 473–485. doi:10.1111/j.1467-8535.2008.00914.x

Cao, X., Khan, A. N., Ali, A., & Khan, N. A. (2019). Consequences of Cyberbullying and Social Overload while Using SNSs: A Study of Users' Discontinuous Usage Behavior in SNSs. *Information Systems Frontiers*. doi:10.1007/s10796-019-09936-8

Chachra, N., Savage, S., & Voelker, G. M. (2015). Affiliate Crookies: Characterizing Affiliate Marketing Abuse. *Proceedings of the 2015 Internet Measurement Conference* (pp. 41–47). New York, NY, USA: Association for Computing Machinery. doi:10.1145/2815675.2815720

Chandrasekharan, E., Samory, M., Srinivasan, A., & Gilbert, E. (2017). The Bag of Communities: Identifying Abusive Behavior Online with Preexisting Internet Data. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 3175—3187). New York, NY, USA: Association for Computing Machinery. doi:10.1145/3025453.3026018

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., . . . Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. *2018 IEEE Symposium on Security and Privacy (SP)*, (pp. 441-458).

Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated experiments on ad privacy settings. *Proceedings on Privacy Enhancing Technologies, 2015*, 92–112.

Drakonakis, K., Ilia, P., Ioannidis, S., & Polakis, J. (2019). Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data. *NDSS 2019 – Proceedings of the Network and Distributed System Security Symposium.*

Duggan, M. (2017, 7). Experiencing online harassment. *Experiencing online harassment*.

Englehardt, S., & Narayanan, A. (2016). Online Tracking: A 1-Million-Site Measurement and Analysis. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1388—1401). New York, NY, USA: Association for Computing Machinery. doi:10.1145/2976749.2978313

Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., . . . Telang, R. (2016, 6). Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (pp. 97–111). Denver: USENIX Association.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). ``A Stalker's Paradise'': How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on*

Human Factors in Computing Systems (pp. 1—13). New York, NY, USA: Association for Computing Machinery. doi:10.1145/3173574.3174241

Gallagher, K., Patil, S., & Memon, N. (2017, 7). New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (pp. 385–398). Santa: USENIX Association.

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (pp. 71–80). New York, NY, USA: Association for Computing Machinery. doi:10.1145/1102199.1102214

Hargittai, E. (2010). Digital Na(t)ives? Variation in Internet Skills and Uses among Members of the ``Net Generation". *Sociological Inquiry, 80*, 92–113. doi:10.1111/j.1475-682X.2009.00317.x

Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., & Ristenpart, T. (2019, 8). Clinical Computer Security for Victims of Intimate Partner Violence. *28th USENIX Security Symposium (USENIX Security 19)* (pp. 105–122). Santa: USENIX Association.

Hawthorn, D. (2007). Interface design and engagement with older people. *Behaviour & Information Technology, 26*, 333–341. doi:10.1080/01449290601176930

Ion, I., Reeder, R., & Consolvo, S. (2015, 7). ``…No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 327–346). Ottawa: USENIX Association.

Jelenchick, L. A., Eickhoff, J. C., & Moreno, M. A. (2013). ``Facebook Depression?" Social Networking Site Use and Depression in Older Adolescents. *Journal of Adolescent Health, 52*, 128–130.

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015, 7). ``My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 39–52). Ottawa: USENIX Association.

Khan, M. T., Huo, X., Li, Z., & Kanich, C. (2015). Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting. *2015 IEEE Symposium on Security and Privacy*, (pp. 135–150).

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems, 36*, 675–705. doi:https://doi.org/10.1016/j.is.2010.11.003

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training. *Proceedings of the 5th Symposium on Usable Privacy and Security*. New York, NY, USA: Association for Computing Machinery. doi:10.1145/1572532.1572536

Lauricella, A. R., Cingel, D. P., Blackwell, C., Wartella, E., & Conway, A. (2014). The Mobile Generation: Youth and Adolescent Ownership and Use of New Media. *Communication Research Reports, 31*, 357–364. doi:10.1080/08824096.2014.963221

Lécuyer, M., Ducoffe, G., Lan, F., Papancea, A., Petsios, T., Spahn, R., . . . Geambasu, R. (2014, 8). XRay: Enhancing the Web's Transparency with Differential Correlation. *23rd USENIX Security Symposium (USENIX Security 14)* (pp. 49–64). San: USENIX Association.

Marciel, M., Cuevas, R., Banchs, A., González, R., Traverso, S., Ahmed, M., & Azcorra, A. (2016). Understanding the Detection of View Fraud in Video Content Portals. *Proceedings of the 25th International Conference on World Wide Web* (pp. 357–368). Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee. doi:10.1145/2872427.2882980

McAndrew, F. T., & Jeong, H. S. (2012). Who does what on Facebook? Age, sex, and relationship status as predictors of Facebook use. *Computers in Human Behavior, 28*, 2359–2365. doi:https://doi.org/10.1016/j.chb.2012.07.007

Miramirkhani, N., Starov, O., & Nikiforakis, N. (2016). Dial One for Scam: Analyzing and Detecting Technical Support Scams. *ArXiv, abs/1607.06891*.

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy, 13*, 99–103.

Nicholson, J., Coventry, L., & Briggs, P. (2019). ``If It's Important It Will Be A Headline'': Cybersecurity Information Seeking in Older Adults. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1–11). New York, NY, USA: Association for Computing Machinery. doi:10.1145/3290605.3300579

Parkin, S., Redmiles, E. M., Coventry, L., & Sasse, M. A. (2019). Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change. *Proceedings of the Workshop on Usable Security and Privacy (USEC `19).*

Patil, S., Norcie, G., Kapadia, A., & Lee, A. J. (2012). Reasons, Rewards, Regrets: Privacy Considerations in Location Sharing as an Interactive Practice. *Proceedings of the Eighth Symposium on Usable Privacy and Security.* New York, NY, USA: Association for Computing Machinery. doi:10.1145/2335356.2335363

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., & Xu, S. (2016, 12). A Survey on Systems Security Metrics. *ACM Comput. Surv., 49*. doi:10.1145/3005714

Polakis, I., Argyros, G., Petsios, T., Sivakorn, S., & Keromytis, A. D. (2015). Where's Wally? Precise User Discovery Attacks in Location Proximity Services. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 817—828). New York, NY, USA: Association for Computing Machinery. doi:10.1145/2810103.2813605

Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T., & Markatos, E. P. (2010). Using Social Networks to Harvest Email Addresses. *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society* (pp. 11–20). New York, NY, USA: Association for Computing Machinery.

Prenksy, M. (2001, 10). On the Horizon. NCB University Press.

Redmiles, E. M., Bodford, J., & Blackwell, L. (2019, 7). ``I Just Want to Feel Safe'': A Diary Study of Safety Perceptions on Social Media. *Proceedings of the International AAAI Conference on Web and Social Media, 13*, 405–416.

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2016). How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. *Proceedings of the 2016 ACM*

SIGSAC Conference on Computer and Communications Security (pp. 666—677). New York, NY, USA: Association for Computing Machinery. doi:10.1145/2976749.2978307

Rosenthal, S. R., Buka, S. L., Marshall, B. D., Carey, K. B., & Clark, M. A. (2016). Negative Experiences on Facebook and Depressive Symptoms Among Young Adults. *Journal of Adolescent Health, 59*, 510–516.

Saeidi, M., da S. Sousa, S. B., Milios, E., Zeh, N., & Berton, L. (2020). Categorizing Online Harassment on Twitter. In P. Cellier, & K. Driessens (Ed.), *Machine Learning and Knowledge Discovery in Databases* (pp. 283–297). Cham: Springer International Publishing.

Sharif, M., Roundy, K. A., Dell'Amico, M., Gates, C., Kats, D., Bauer, L., & Christin, N. (2019). A Field Study of Computer-Security Perceptions Using Anti-Virus Customer-Support Chats. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1—12). New York, NY, USA: Association for Computing Machinery. doi:10.1145/3290605.3300308

Simoiu, C., Bonneau, J., Gates, C., & Goel, S. (2019, 8). ``I was told to buy a software or lose my computer. I ignored it'': A study of ransomware. *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019).* Santa: USENIX Association.

Snyder, P., & Kanich, C. (2015). No Please, After You: Detecting Fraud in Affiliate Marketing Networks. *Workshop on the Economics of Information Security.*

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing. *Proceedings of the 2017 Internet Measurement Conference* (pp. 432–444). New York, NY, USA: Association for Computing Machinery. doi:10.1145/3131365.3131385

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. *IT Professional, 18*, 26–32.

Strauss, A., & Corbin, J. M. (1997). *Grounded theory in practice.* Sage.

Sun, J. C.-Y., Yu, S.-J., Lin, S. S., & Tseng, S.-S. (2016). The mediating effect of anti-phishing self-efficacy between college students' Internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior, 59*, 249–257. doi:https://doi.org/10.1016/j.chb.2016.02.004

Tandoc, E. C., Ferrucci, P., & Duffy, M. (2015). Facebook use, envy, and depression among college students: Is Facebooking depressing? *Computers in Human Behavior, 43*, 139–146.

Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. *SSRN 2820060*. Retrieved from https://ssrn.com/abstract=2820060

Venkatadri, G., Lucherini, E., Sapiezyński, P., & Mislove, A. (2019). Investigating sources of PII used in Facebook's targeted advertising. *Proceedings on Privacy Enhancing Technologies*, (pp. 1–18).

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). ``I Regretted the Minute I Pressed Share'': A Qualitative Study of Regrets on Facebook. *Proceedings of the Seventh Symposium on Usable Privacy and Security.* New York, NY, USA: Association for Computing Machinery. doi:10.1145/2078827.2078841

Wash, R., & Rader, E. (2015, 7). Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 309–325). Ottawa: USENIX Association.

APPENDIX A - INTERVIEW PROTOCOL

A.1. SCREENING QUESTIONNAIRE

Thank you for your interest in participating in our Study on Adverse Experiences with Technology.

Please fill out this brief 3-minute questionnaire about yourself and your experiences with technology. We will use your answers to determine if you are eligible to participate in the study.

If you qualify for participation, we will contact you via e-mail for a 45-60 minute interview session conducted on campus at Indiana University Bloomington. As a token of our appreciation for your participation in the interview, you will receive \$10 cash or cash equivalent, such as an Amazon gift certificate.

If you do not qualify, your responses will be discarded safely.

- What is your Year of Birth?
- What is your Gender?
    - Male
    - Female
    - Something else. Please specify:
    - Prefer not to answer
- What is your occupation?
- What is your ethnic background? (Select all that apply)
    - African American
    - Asian
    - Hispanic
    - Native American
    - White (Caucasian)
    - Something else. Please specify:
- Are you a resident of Bloomington, Indiana?
    - Yes
    - No
- Are you affiliated with Indiana University Bloomington?
    - Yes
    - No
- [If affiliated with Indiana University Bloomington] What department or school are you affiliated with?
- [If student] What is your major/field of study?
- On an average day, how much time do you spend actively on Internet-connected devices, such as a computer, phone, tablet, etc.?
    - None

    - Less than 1 hour
    - 1-2 hours
    - 3-4 hours
    - 5-7 hours
    - 8 or more hours
- Which of the following devices do you use? (select all that apply)
    - Tablet
    - Smartwatch
    - Smartphone
    - Digital camera
    - Desktop
    - Voice assistant (e.g. Amazon Echo)
    - Fitness tracker (e.g. Fitbit)
    - Gaming console (e.g. Playstation, Xbox, Wii, etc.)
    - Laptop
    - Other. Please specify:
- Which operating system do you use for your laptop? (If you use multiple laptops, select the operating system for the laptop you consider as your primary laptop.)
    - Microsoft Windows
    - MacOS
    - Linux
    - Chrome OS
    - I don't know
    - Something else. Please specify:
- Which operating system do you use for your desktop? (If you use multiple desktops, select the operating system for the desktop you consider as your primary desktop.)
    - Microsoft Windows
    - MacOS
    - Linux
    - Chrome OS
    - I don't know
    - Something else. Please specify:
- Which operating system do you use for your mobile phone? (If you use multiple mobile phones, select the operating system for the mobile phone you consider as your primary mobile phone.)
    - Android OS (Google)
    - iOS (Apple)
    - Something else. Please specify:
- Which of the following tasks have you ever done? (Select all that apply.)
    - Hacked device or online account
    - Phishing
    - Bugs in software or apps
    - Identity Theft

    - Stalking
    - Leak of sensitive personal information
    - Cyberbullying
    - Viruses or other unwanted/malicious programs (such as spyware, adware, etc.)
    - Unauthorized access to your bank account
    - Theft/unauthorized use of your credit or debit card
    - Demand for ransom to restore access to device or data
    - Something else. Please specify:
- What did you do in response to the adverse experience(s)?
    - Repaired device using advice from an online forum
    - Notified the financial institution
    - Purchased security software
    - Obtained a loaner device
    - Purchased a new device
    - Notified the credit card company
    - Took device to a repair shop
    - Repaired device with anti-virus/anti-malware software
    - Nothing
    - Something else. Please specify:
- What were the consequences of the adverse experience(s)? (Select all that apply.)
    - Loss of productivity
    - Violation of privacy
    - Loss of funds from a bank or credit card account
    - Cost of replacing a device
    - Damage to credit profile
    - Time without a device (while it was being repaired)
    - Loss of confidence in the use of technology
    - Reduced ease of use of a device
    - Reduced sense of security
    - Loss of data (e.g., documents, pictures, etc.)
    - Cost of purchasing security software
    - Cost of repairing the device
    - Loss of employment
    - Embarrassment
    - Time spent learning to repair a device
    - Something else. Please specify:
- Are you able to attend an in-person interview at a location on the campus of Indiana University Bloomington?
    - Yes
    - No
    - Maybe
- If you cannot attend in person, which of the following could work?
    - Audio/video conference (e.g. Zoom, Skype)

    - Telephone
    - Other. Please specify:
- If you qualify for the study, which email address should we use to contact you for scheduling an interview?

A.2. SEMI-STRUCTURED INTERVIEW PROTOCOL

A.2.1 Initial Briefing

This research focuses on adverse experiences with digital technologies. It can include any situations where you felt unpleasant, unsatisfied, worried and concerned while using digital technologies.

By doing the interviews, we hope to know more about how people characterize experiences of adverse incidents when they use digital devices and services and how they perceive, understand, and respond to those experiences.

A.2.2 Background Information.

- Tell me a bit about yourself.
- What is your occupation? If you are a student in college or graduate school, what is your major?
- If you don't mind, when were you born?
- What digital devices and services do you use regularly? For what purposes?

A.2.3 Adverse Experiences

- You mentioned in the questionnaire that you have had adverse experience using these devices/services. What specific incidents caused the adverse experience? [If the participant cannot remember, go through the list of adverse experiences mentioned by the participant in the screening questionnaire.]
- Could you tell me about a particularly prominent incident? What were the exact details? Let's start with (key elements) such as the device/service you were using.
    - [Follow-up: Detection] How did you detect the incident?
    - [Follow-up: Reaction] How did the incident make you feel when you detected it? What was your reaction to the incident?
    - [Follow-up: Solution] Did you solve the issue?
- (If not) How is it going now? Are you still facing the issue? How does it make you feel? What has it cost you?
- (If yes) How did you solve the issue? How did you figure out the solution? What specific tools or resources did you use?
- Did it cost you anything (if so, what or how much)? How did it make you feel?
- Did you try any other solutions before you finally solved the problem? If so, what were they? What were the key elements?
- Did you have any other adverse experiences? If yes, please tell me about them one by one. [Follow the same questions as above for each incident.]

- [If needed, prompt the participant using the following examples of adverse experiences: Hacked device or online account, Phishing, Bugs in software or apps, Identity Theft, Stalking, Leak of sensitive personal information, Cyberbullying, Viruses or other unwanted/malicious programs (such as spyware, adware, etc.), Unauthorized access to your bank account, Theft/unauthorized use of your credit or debit card, Demand for ransom to restore access to device or data.]

A.2.4 Influences

- Did the experiences you described above have any influence on you?
- [If no, skip this category.]
- [If yes, continue.]
- What were the influences in the short term?
- What were the influences in the long term?
- What did you learn from these incidents and solution-seeking experiences?
- [Follow-up, if needed:] For example, did these experiences affect your habits or preferences regarding using the involved devices or services? Did they alter your views of digital technologies in general? Did they influence your social or professional relationships?
- Is there anything else you find important that we did not cover? Do you have any questions?

Thank you very much for sharing your experiences. Your responses were very helpful. If you have any questions later, please feel free to contact the researchers.