Hacker, Their Actions, and Fear Appeal: A First Look Through the Lens of Children

Rizu Paudel
rizu.paudel@usu.edu
Utah State University
Logan, Utah, USA

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

ABSTRACT

With the increasing use of computers and smartphones by children, their online safety has become a major concern due to the lack of security awareness. Prior studies pointed to children's poor password habit and vague perceptions on the significance of passwords. While users must be sufficiently motivated to perform a target behavior, a little study to date, focused on understanding how we can encourage children towards strong password creation. As we begin to address this gap, we examined children's perceptions of adversary's actions that instill fear in the context of password compromise. Our semi-structured interviews with 20 children (aged between 8 and 12) reveal their concerns around a hacker, which inform future designs how fear appeal can be leveraged as a motivational tool for children towards strong passwords.

CCS CONCEPTS

• **Human-centered computing** → **User studies**.

KEYWORDS

Children, Fear Appeal, Authentication

ACM Reference Format:
Rizu Paudel and Mahdi Nasrullah Al-Ameen. 2024. Hacker, Their Actions, and Fear Appeal: A First Look Through the Lens of Children. In *Companion of the 2024 Computer-Supported Cooperative Work and Social Computing (CSCW Companion '24), November 9–13, 2024, San Jose, Costa Rica.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3678884.3681888

1 INTRODUCTION

In 2015, 94% of children in the United States, ranging from 3 to 18 years old, had access to a computer at home, with 86% having Internet connectivity [29]. By 2019, ownership of smartphones among children as young as 11 reached 53%, escalating to 84% among teenagers [44]. While security breaches have alarmingly risen in recent years [22, 54], it is particularly concerning for children [14, 27, 41, 52, 58], where despite the existence of laws (e.g., COPPA: Children's Online Privacy Protection Act) to protect children in the digital world, a wide array of applications are found collecting their personal information [39]. To this end, it has become more important than anytime before to understand the security and privacy perceptions of children, where a body of work [9, 39, 52] emphasized a strong foundation in children's password practices – a crucial step towards their online security protection. In this section, we first present a brief overview of prior work on children's password practices and highlight the gap in existing literature that we addressed in our work, followed by a summary of our contributions.

1.1 Background and Motivation

A longitudinal study [58] conducted over eight years demonstrated an increase in children's use of technology without a parallel improvement in their safety awareness. Children are found more vulnerable to cyberattacks and identity theft than adults due to their limited concerns and awareness [53, 57]. To this end, the studies [26, 27, 40] focusing on children's password composition strategies reveal that most of them use predictable items in passwords, making them vulnerable to guessing attacks, where younger children's passwords are easier to guess due to simplicity. Despite creating a weak password, children do not typically worry about the risks associated with it [41], where they believe that their passwords would be difficult to guess by strangers [27]. A recent study [52] further revealed their poor password habit and vague perceptions on the significance of passwords. In another study [24], Kumar et al. explored children's strategies that they employ to address their privacy and security concerns. Despite acknowledging these concerns, children are found to share personal information that could lead to privacy vulnerabilities. Here, authors did not delve into how children perceive adversaries and how they form these perceptions [24]; we have addressed these gaps in our work.

In order to perform a target behavior, users must be sufficiently motivated, be prompted, and attain the ability, as asserted by Fogg's Behavior Model (FBM) [18]. Although the use of digital technology by children has substantially increased in recent years [19, 38], they are not aware and motivated to adopt secure online behavior, e.g., the creation of strong passwords [9, 39, 40]. While prior research, as noted above explored the aspects of ability (e.g., how children create passwords), there is a dearth in existing literature on how to motivate children towards strong password creation. Here, FBM emphasizes fear appeal, i.e., anticipation of something bad to happen, to encourage people towards desired behavior [18, 33]. To this end, we investigated the following research question in our work: *How do children perceive an adversary and their actions that instill fear in the context of password compromise?*

1.2 Contributions

To address our research question, we conducted semi-structured interviews with 20 children in the USA, who use computer and were between 8 and 12 years old [1]. The findings from our study

CSCW Companion '24, November 9–13, 2024, San Jose, Costa Rica

ACM ISBN 979-8-4007-1114-5/24/11.
https://doi.org/10.1145/3678884.3681888

[1] We chose this age group as per the guideline from prior studies [10, 20, 57].

PID	Gender	Age	Race	School Level	No. of Passwords
P1	Girl	9	White	Elementary	1-3
P2	Boy	12	White	Middle	More than 10
P3	Girl	10	White	Elementary	4-7
P4	Boy	11	White	Elementary	8-10
P5	Boy	11	White	Elementary	1-3
P6	Girl	9	White	Elementary	1-3
P7	Girl	9	White	Elementary	1-3
P8	Boy	10	White	Elementary	1-3
P9	Girl	10	White	Elementary	4-7
P10	Girl	12	White	Middle	4-7
P11	Girl	8	White	Elementary	1-3
P12	Boy	10	White	Elementary	1-3
P13	Girl	10	White	Elementary	1-3
P14	Boy	8	White	Elementary	1-3
P15	Boy	9	White	Elementary	1-3
P16	Girl	11	White	Elementary	1-3
P17	Boy	9	White	Elementary	1-3
P18	Girl	11	White	Elementary	4-7
P19	Boy	8	White	Elementary	4-7
P20	Boy	11	White	Middle	1-3

Table 1: Demographics and Number of Passwords of Children

shed light on children's perceptions of an adversary's [2] actions and intentions, contributing to our understanding of fear appeal in protecting their devices and accounts. Getting their academic work sabotaged represents a common fear among children. They reported similar concerns about photos and email in the realm of exploiting personal information. We observe that children's concerns extend beyond an individual's personal space, including the leakage of sensitive information and credentials of others (e.g., friends and family) from a shared device. We also found instances reflecting children's fear to be tracked by an adversary, and getting exposed to inappropriate digital contents. Here, children perceive personal grudge or anger as the motive behind hacking.

While fear appeal is an effective tool in encouraging users towards desired behavior [17, 18, 33, 48], it is crucial to understand the perceptions of target population for its effective use in specific contexts. To the best of our knowledge, our work is the first to unpack children's perceptions and concerns around a hacker, which informs how fear appeal can be leveraged in future designs to motivate children towards secure passwords. For instance, the password creation interface of a website could present a visual design in the form of a story depicting the consequences of a weak password; in such context, our findings on children's perceptions of adversary's actions offer insights into leveraging the fear appeal.

2 METHODS

2.1 Participant Recruitment

We conducted one-on-one interviews with 20 children. To take part in our study, a child had to be between 8 and 12 years old, who uses computer. We reached out to potential participants through their parents. To this end, we contacted the employees at our university over email, and used snowball sampling recruiting a few participants from the recommendation of participants' parents who had taken part in our study. Our study was approved by the Institutional Review Board (IRB) at our university.

2.2 Procedure

When the parent emailed us informing about their child's interest to take part in our study, we emailed them the Informed Consent Document (ICD), which included Parental Consent and Child Assent forms. As they agreed to ICD, we scheduled a study session. During the study conducted over Zoom (recorded), we first asked children about their general computer usage. Thereafter, we presented participants with a scenario prompting them to imagine that an adversary has hacked the password and got access to their computer; we then asked about their perceptions on the intention of hacker behind such act, and the possible consequences of this incident, i.e., how they could exploit the information they gained access to. Then the participants responded to a set of demographic questions, hosted in Qualtrics [3]. On average, each session took between 15 and 20 minutes to complete. Each participant was compensated with a $15 Amazon.com gift card.

2.3 Analysis

We performed thematic analysis [5–7] on the transcription of audio recordings, where we took an inductive approach. In this ground-up approach, codes are derived from the data without preconceived

[2]In this paper, the terms: 'hacker' and 'adversary' are used interchangeably in the contexts of password guessing attacks.

[3]Qualtrics is an online survey platform used to create, distribute, collect, and analyze survey data (www.qualtrics.com)

Participant	1	2	3	4	5
Percentage of Themes Covered	20	40	40	60	80
Participant	6	7	8	9	10
Percentage of Themes Covered	80	80	80	100	100
Participant	11	12	13	14	15
Percentage of Themes Covered	100	100	100	100	100
Participant	16	17	18	19	20
Percentage of Themes Covered	100	100	100	100	100

Table 2: Attaining Theoretical Saturation

notions, which allows the narrative to emerge from the raw data itself without trying to fit it into the preconceptions [5–7]. We then organized the codes into higher level categories. Each participant's data was coded by two researchers. They read through all the transcripts together at the same time, and came up with the codes that they discussed, and resolved the conflicts if exist.

3 RESULTS

In this section, we present the findings from our study, representing children's perceptions of adversary's actions (see §3.2–§3.6) and motives (see §3.7). Following the guideline from prior research [35, 49, 51], for consistency, we use these terms throughout the manuscript based on the frequency of comments in participants' responses: a few (0-10%), several (10-25%), some (25-40%), about half (40-60%), most (60-80%), and almost all (80-100%).

3.1 Participants

A total of 20 children (10 girls, 10 boys), aged between 8 and 12 years, participated in the study. All participants identified as White. Seventeen of our participants were in elementary school, and the other three children were in middle school (see Table 1 for details). As we inquired about their computer usage, we found that all of them regularly use computer for educational purposes, including schoolwork, assignments, and learning new languages. They also mentioned using the computer for recreational activities, such as playing games, watching YouTube videos, sports, and movies. Most participants reported having one to three passwords in real life.

3.2 Exploitation of Personal Information

Several participants pointed to the identity theft and financial fraud as consequences of personal information compromise. P19 said, *"...If...they have like your name and stuff, they could write, like a check to them...if they have...your name, they could use your name on different things...like if they did a crime...they would use your name...they could use your email for something...like payments..."* Several participants expressed concern that the adversary could assume their identity and engage in revengeful activities by sending inappropriate messages from their hacked account; for instance, P18 mentioned, *"I'm not okay with just random people hacking into my emails and texts, because they can also email and text those people from that position and say things that can ruin friendships, and relationships in general."*

A few of our participants were concerned about the possibility of an adversary stealing their information and selling it to others for financial gain, where P4 mentioned, *"...I'd learn that...they can like sell it to people, I think...It can just...take the stuff and sell it to other people."* We found instances where participants pointed out that an adversary, upon gaining access to their online account, could exploit their personal information for targeted advertisement and clickbait. For example, P9 commented, *"And maybe the things I like, like, if I go on to Amazon, they can see what I like to buy. So send me ads...like clickbait."*

Some participants reported concern about an adversary getting access to their personal photos, resulting in exploitation or destruction. For instance, P18 said, *"...My photos, I have pictures of people and times and places...they're special and important to me...I don't want somebody getting in and destroying, erasing them, ruining them, exploiting them."* Another participant (P13) worried that an adversary could cause physical harm to them upon finding their address of residence through hacking their online account: *"Um, I don't want to get hurt by them...they could like find my address and do something..."*

3.3 Sabotaging Academic Work

About half of the children in our study perceived an adversary's actions as potentially destructive, envisioning scenarios where the adversary could sabotage their academic work. P17 elaborated: *"So with Google Docs, they can delete any of my writing...they can read it, and then like, make comments about it. And they can just learn...a lot about my life. And then with grades...the hacker...might try to get my grades lower...they could like hide them from me...then it might be harder for me in school...if he or she made comments about me on my Google Docs [it] might make me feel bad...it would be harder for me to access my accounts and stuff."*

Our participants expressed concern about an adversary ruining their assignments; for instance, P1 commented, *"They could ruin those [assignments] and do really anything like they could delete...type in...bad things and add bad things..."* They also pointed to the potential waste of time and effort due to an adversary's action; P6 said, *"Because if you work on something really hard, and then someone just ruins it, then you'll have to do it all over again."* P5 echoed similar sentiment: *"And with the messing with my assignment. I don't want to like restart on most of my assignments I've worked hard on..."*

Children expressed concern about the potential impact of an adversary's action on their academic performance, particularly fearing that it could lower their grades. For instance, P10 said, *"Because on my school account, I like doing things correctly...I like getting good grades...So um, it would not be good because they could...submit some other things to the teachers that are not like, right, and then my grade could drop because they did that."* Another participant (P11) echoed the similar sentiment: *"It might accidentally erase off or...like typing random things...like typing a book I haven't read...and then take a test on it. And that could get me [low grades]. Well, I love points. And I won't be able to get the big prize..."*

3.4 Beyond Personal Harm

Our participants reported concern about the safety of others, highlighting their fear that adversaries might target people they care

about, if they gain access to their information. P3 stated, *"Because of the safety of others, because I don't want other people to get targeted too and I don't want them to feel unsafe, or those kinds of things...They could send like bad emails. And...it's like trying to scare...threaten [them]..."* Several participants were particularly worried about the potential compromise of their parents' information from a shared family computer. For instance, P2 said, *"...my parent's computer like their social security number...or other personal items that I need to keep confident...With my email, they could attack me and use it to...get a hold of the things that I need for school or that I've been sent by other people that has important information on it."* P10 also mentioned the potential impact on their parents highlighting consequences that could extend beyond an individual's personal space: *"...And with mom's Girl Scout things, it's like she runs two troops. So that's a lot of things on there like a lot of ideas and a lot of things on there that are very important to in order to run meetings correctly. And it would not be good at all if they did something with that"*

Our participants also pointed to the possible financial loss of their parents and family members if a hacker gets access to their online accounts; where P15 mentioned, *"...the Amazon account...they can just steal all your Amazon money. And then...Google account..they could steal lots of things off of it...they probably [can] buy new games on it."* A few participants reported concern that if an adversary hacks into their email account, they could access others' sensitive information and personal photos and leak them online. P18 elaborated, *"My emails and texts...they can be about serious things that like people have problems with and they [hackers] can give away...other people's personal information, which I wouldn't want to be the reason that I give away one of my friend's information, or like an embarrassing moment that I have a funny picture of and I wouldn't want that all over the Internet..."*

3.5 Tracking Individuals

Several participants pointed to how an adversary might use their information to stalk and track them in both the digital and physical realm. For instance, P18 commented, *"...my personal information is personal for a reason. You know, like, I wouldn't want somebody in internet stalking me like...how healthy I was, how tall, how much I weighed...gender...when people like, get into my photos, they can also see other things about me...who my family is...what I do, where I live...They they'll have an easier time stalking me finding where I live..."* Another participant (P9) talked about the hacker accessing search history on their computer and exploiting that to track their online activities: *"...And search history it's like, they know what I'm doing like maybe if I'm listening to audiobooks, they know that I'm on the audiobooks...they can find me there."*

3.6 Challenging Moral Compass

Several participants expressed concern about an adversary exposing them to inappropriate content on YouTube, which might go against their personal values. For instance, P5 commented, *"Umm for bad stuff on YouTube, I kind of just don't want to be watching stuff, I shouldn't because if I do or like accidentally do I'd just feel really guilty...And umm the music, I kind of just feel like with the YouTube. I just don't want to be listening to bad music because, again, it makes me feel guilty."* This emphasizes participant's moral considerations and the potential impact of inappropriate content on their well-being. In these contexts, participants also reported concern about the potential manipulation of their preferences by an adversary, where P12 stated, *"...if they got into my stuff on my computer, they could know what, what I like, and what I like to watch, [and they] might be able to, like influence that in a bad way."*

3.7 Children's View towards Adversary's Motives

In exploring children's perceptions of an adversary's sentiment related to hacking, we observed them associating it with anger or passion. We found evidences where participants perceived personal conflict as a trigger behind hacking. For instance, P17 said, *"...Mad...because they...really want to hack into your computer and...they're mad at you..."* Similar sentiment was echoed by P13: *"...[they are] angry at you...they know who you are and they are...trying to do it [hack] because you...did something to them."*

Some participants see hacking as an act of passion, associating it with a feeling of thrill and achievement. P7 explained, *"Because they like doing it...they might do it a lot and they feel happy about it."* Similar sentiment was echoed by P5: *"Because people can get happy, whenever they're like, Oh, I got this guy's information..."* A few participants pointed to the excitement of an adversary as they successfully hack in pursuit of taking a revenge. For instance, P2 commented, *"...they could be excited...happy that they got in...it's somebody that they know and they're mad at them..."* P10 further elaborated, *"...He [adversary] would...feel accomplished...because he got through your computer, and also probably happy because that's what he wanted to do."*

4 DISCUSSION

A body of work [11, 25, 55] shed light on adults' mental models of privacy and security. Younger adults define privacy in terms of the control over information and consent before disclosure, while older adults often relate privacy to their personal space [25]. A sense of futility is reported by users about their ability to protect themselves online [11, 50], where the unexpected consequences, often related to potential misuse and unintended use of security tools can arise from partial or incomplete security mental models of users [16, 36, 45, 47]. In this regard, users are found to prioritize protection strategies against online threats based on their conceptualizations of adversaries [4, 55]. Thus, it is crucial to understand user's perceptions and concerns around an adversary.

As we begin to address this gap, we focused on children in our study. In particular, the findings from our study shed light on children's perceptions of adversary's actions and intentions, contributing to our understanding of the factors that create fear appeal for them in protecting their devices and accounts. In this section, we discuss the implications of our findings leading to design recommendations and guideline for future research (see Figure 1 for an overview of our findings and corresponding implications.).

4.1 Interplay between Motives and Actions

Our participants view hacking as an act of either revenge or passion, associating these intentions with the familiarity between an

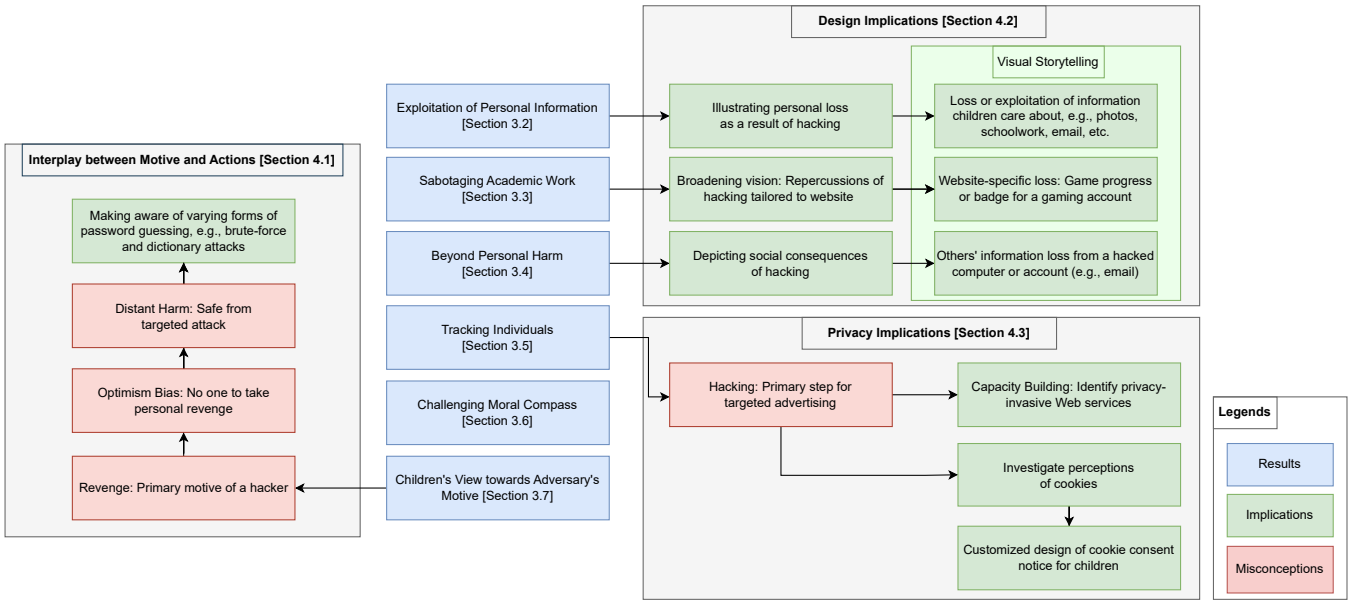

Figure 1: Overview of Findings and Implications

adversary and the victim. They perceive that when there is no personal connection between an adversary and the victim, senses of passion and thrill ignite the hacker's intention to break into other's accounts. On the other hand, they believe that an adversary who knows the victim, would commit hacking only for the purpose of taking a personal revenge. According to them, a hacker's grudge against an individual could result in varying consequences; for instances, destroying personal photos and academic work, challenging their moral compass through inappropriate videos, and damaging their relationship with others through impersonation. Here, children see a clear motive behind hacking when an adversary personally knows the victim. That means, they comprehend password hacking as a form of targeted attack, e.g., guessing by an acquaintance [2, 34, 43].

Our findings support the essence from prior work that pointed to children's overall lack of understanding of security vulnerabilities [26, 27, 53, 57]. They perceive hacking as a 'distant harm' [31], where our findings offer a possible explanation to their perceptions. We found children viewing personal revenge as a motive behind hacking, and thus, it is possible that not finding such intentions among the people within their family and social circle could lead to an optimism bias that their devices and accounts are safe from being a target of hacking. To address such limited understanding of password guessing, our findings indicate the need of making children aware of diverse forms of hacking, including brute-force and dictionary attacks [53, 57].

4.2 Design Implications

Fogg's Behavior Model [18, 33, 48] points to the potential of leveraging fear appeal in designs aimed at motivating people towards desired behavior. To this end, the findings from our study provide guideline for future research to investigate design opportunities in motivating children towards strong passwords. In one such direction, we will create and evaluate digital storytelling [4] based designs to show the consequences of weak passwords. Such a visual design would be presented prior to password creation, with a goal of encouraging users towards a strong password. Further, we encourage future research to build on our findings and conduct a large-scale study with the participants from diverse demographics to unveil the differences in their perceptions around adversaries, which in turn, would provide more in-depth insights into leveraging fear appeal in security designs, contextualized to the demographic traits of users.

Our study builds the foundation to create storytelling based security designs for children, where their perceptions of the adversary's actions offer insights into leveraging fear appeal in these contexts. For example, our findings shed light on the personal information children care about, e.g., photos, schoolwork, email, etc., which could be depicted as accessed by an adversary in a design aimed at portraying personal loss as a result of hacking. In another instance, we observe that children's concern around adversary's actions extend beyond their personal loss, where they worry that hacking into their computer or account could lead to the leakage of others' (e.g., friends and family) personal information and credentials. These findings are in line with prior work [21, 30] on empathy and social cognition in the contexts of adults showing that people do not typically want others to suffer as a result of their action. To this end, we will explore designs for children illustrating the social implications of hacking; for instance, portraying the consequence as a social harm, where hacking may impact not only an individual but also the people they are associated with.

[4] Digital storytelling represents a form of art that combines graphics and text to be able to tell a story about a subject or topic [28, 37, 42, 56]

Our results indicate that children see personal revenge as a primary motive of an adversary to hack into their account; we found instances where their understanding is limited to a specific consequence (e.g., sabotaging academic work). Building on the insights from our findings towards the necessity of broadening their vision on password vulnerabilities, we believe that tailoring the consequences of a weak password to children's understanding and experience of an online platform would better help them to comprehend the potential risks of losing valuable information and sensitive credentials. We found that children avail a wide range of online services (e.g., email, games, video streaming, etc.) in addition to accessing their school account. To this end, we will create and evaluate designs for children, where the consequences of a weak password would be tailored to the type of a website presenting that design during password creation. Here, the type of information vulnerable to be accessed by an adversary can vary across online services; for instances, an unauthorized access to a child's school account can result in the loss or manipulation of assignments, grades, and personal information of the child and their guardians, where for a gaming account, the loss may include the achievements (e.g., badges) and progress in a game.

4.3 Privacy Implications

In this section, we highlight the implications of our results that extend beyond our focus on authentication. The findings from our study point to children's perceptions of targeted advertisement, who believe that the adversary needs to garner user's personal information through hacking, in order to send them targeted advertisement. While personal information leaked through hacking could be exploited in tracking individuals, it is unclear whether the children see hacking as an essential step towards tracking users. While online tracking is a major concern in privacy landscape [1, 23], children, the next-generation Internet users demand appropriate attention from the privacy designers and practitioners to build capacity in identifying privacy-invasive Web services and applications.

We also observed children's misconceptions around tracking, where in one instance, the participant reported that an adversary could access their search history on computer browser upon hacking, and use that information to track their online presence, e.g., what they do on a particular website at a given time. While cookies are often used to track individual's online activities [8, 32], children's perceptions of cookies is unclear from our study – also, out of the scope of this work. We found evidences of children's use of varying Web services; we suspect, many of those websites ask them to set cookie preferences – a common practice in today's Web usage. We thus, encourage future research to investigate children's perceptions of cookies, and their understanding of underlying settings. Such insights could lead to customize the design of cookie consent notice as per children's comprehension and preferences.

5 LIMITATIONS AND CONCLUSION

We followed the widely-used methods for qualitative research [3, 5, 6, 12, 13] focusing in depth on a small number of participants and continuing the study until no new themes emerged (Table 2 illustrates how we have reached saturation). We acknowledge the limitations of these studies that a different set of samples might yield varying results [15, 46]. Thus, we do not draw any quantifiable, generalizable conclusion from this study. A few of our participants were recruited via snowball sampling. In snowball sampling, participants who have taken part in the study nominate people for recruitment whom they know well; thus, it may suffer from sampling bias. In addition, self-reported data might have limitations, like recall and observer bias.

Despite these limitations, our study makes valuable contributions in understanding children's perceptions and concerns around a hacker, which inform future designs how fear appeal can be leveraged to motivate children towards strong passwords. In the next step, we will conduct participatory design sessions with children towards the creation and evaluation of storytelling based designs, centered around hacker's actions and intentions reported in this paper. We encourage CSCW community to extend the findings of this work in the contexts of different domains and field sites, and use other methods as well, if required.

ACKNOWLEDGMENTS

We would like to thank the reviewers for their valuable feedback. This material is based upon work supported by the National Science Foundation under Award No. CNS-1949699.

REFERENCES

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2020. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology* 30, 4 (2020), 736–758.
[2] Mahdi Nasrullah Al-Ameen, SM Taiabul Haque, and Matthew Wright. 2016. Leveraging autobiographical memory for two-factor online authentication. *Information & Computer Security* 24, 4 (2016), 386–399.
[3] Kathy Baxter, Catherine Courage, and Kelly Caine. 2015. *Understanding Your Users: A Practical Guide to User Research Methods* (2 ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.
[4] Arezou Behfar, Hanieh Atashpanjeh, and Mahdi Nasrullah Al-Ameen. 2023. Can Password Meter be More Effective Towards User Attention, Engagement, and Attachment?: A Study of Metaphor-based Designs. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*. 164–171.
[5] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development*. sage, Thousand Oaks, CA, USA.
[6] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
[7] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology* 18, 3 (2021), 328–352.
[8] Quan Chen, Panagiotis Ilia, Michalis Polychronakis, and Alexandros Kapravelos. 2021. Cookie swap party: Abusing first-party cookies for web tracking. In *Proceedings of the Web Conference 2021*. 2117–2129.
[9] Yee-Yin Choong, Mary Theofanos, Karen Renaud, and Suzanne Prior. 2019. Case study–exploring children's password knowledge and practices. (2019).
[10] Porter E Coggins III. 2013. Implications of what children know about computer passwords. *Computers in the Schools* 30, 3 (2013), 282–293.
[11] Paul Dourish, J Delgado De La Flor, and Melissa Joseph. 2003. Security as a practical problem: Some preliminary observations of everyday mental models. In *Proceedings of CHI 2003 workshop on HCI and security systems*.
[12] Prakriti Dumaru and Mahdi Nasrullah Al-Ameen. 2023. "After she fell asleep, it went to my next podcast, which was about a serial killer": Unveiling Needs and Expectations Regarding Parental Control within Digital Assistant. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*. 17–21.
[13] Prakriti Dumaru and Mahdi Nasrullah Al-Ameen. 2024. "It's like educating us older people...": Unveiling Needs and Expectations Regarding Educational Features within Parental Control Tools. In *Extended Abstracts of the 2024 CHI Conference on Human Factors in Computing Systems (CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 387, 8 pages. https://doi.org/10.1145/3613905.3651113

[14] Prakriti Dumaru, Bryson D Hackler, Audrey Flood, and Mahdi Nasrullah Al-Ameen. 2024. "I feel like he's looking in the computer world to be social, but I can't trust his judgement": Reimagining Parental Control for Children with ASD. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–25.

[15] Prakriti Dumaru, Ankit Shrestha, Rizu Paudel, Arezou Behfar, Hanieh Atashpanjeh, and Mahdi Nasrullah Al-Ameen. 2023. "I Have Learned that Things are Different here": Understanding the Transitional Challenges with Technology Use After Relocating to the USA. In *International Conference on Human-Computer Interaction*. Springer, 201–220.

[16] Prakriti Dumaru, Ankit Shrestha, Rizu Paudel, Cassity Haverkamp, Maryellen Brunson McClain, and Mahdi Nasrullah Al-Ameen. 2024. "… I have my dad, sister, brother, and mom's password": unveiling users' mental models of security and privacy-preserving tools. *Information & Computer Security* 32, 3 (2024), 282–303.

[17] Marc Dupuis, Anna Jennings, and Karen Renaud. 2021. Scaring people is not enough: an examination of fear appeals within the context of promoting good password hygiene. In *Proceedings of the 22nd Annual Conference on Information Technology Education*. 35–40.

[18] Brian J Fogg. 2009. A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology*. 1–7.

[19] Donell Holloway, Lelia Green, and Sonia Livingstone. 2013. Zero to eight. *Young children and their internet use* 14 (2013).

[20] Casey Lee Hunt, Kaiwen Sun, Zahra Dhuliawala, Fumi Tsukiyama, Iva Matkovic, Zachary Schwemler, Anastasia Wolf, Zihao Zhang, Allison Druin, Amanda Huynh, et al. 2023. Designing Together, Miles Apart: A Longitudinal Tabletop Telepresence Adventure in Online Co-Design with Children. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference*. 52–67.

[21] William John Ickes. 1997. *Empathic accuracy*. Guilford Press.

[22] Emma Johns. 2020. Cyber security breaches survey 2020. *London: Department for Digital, Culture, Media & Sport* 4, 1 (2020), 1–4.

[23] Garrett A Johnson, Scott K Shriver, and Shaoyin Du. 2020. Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science* 39, 1 (2020), 33–51.

[24] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–21.

[25] Michelle Kwasny, Kelly Caine, Wendy A Rogers, and Arthur D Fisk. 2008. Privacy and technology: folk definitions and perspectives. In *CHI'08 Extended Abstracts on Human Factors in Computing Systems*. 3291–3296.

[26] Dev Raj Lamichhane and Janet C Read. 2017. Investigating children's passwords using a game-based survey. In *Proceedings of the 2017 conference on interaction design and children*. 617–622.

[27] Sumbal Maqsood, Robert Biddle, Sana Maqsood, and Sonia Chiasson. 2018. An exploratory study of children's online password behaviours. In *Proceedings of the 17th ACM Conference on interaction design and children*. 539–544.

[28] Sorin Adam Matei and Lucas Hunter. 2021. Data storytelling is not storytelling with data: A framework for storytelling in science communication and data journalism. *The Information Society* 37, 5 (2021), 312–322.

[29] Joel McFarland, Bill Hussar, Jijun Zhang, Xiaolei Wang, Ke Wang, Sarah Hein, Melissa Diliberti, Emily Forrest Cataldi, Farrah Bullock Mann, and Amy Barmer. 2019. The Condition of Education 2019. NCES 2019-144. *National Center for Education Statistics* (2019).

[30] Margherita Melloni, Vladimir Lopez, and Agustin Ibanez. 2014. Empathy and contextual social cognition. *Cognitive, Affective, & Behavioral Neuroscience* 14, 1 (2014), 407–425.

[31] Ugnė Paluckaitė, Kristina Žardeckaitė-Matulaitienė, et al. 2017. Adolescents' perception of risky behaviour on the internet. *European Proceedings of Social and Behavioural Sciences* 30 (2017).

[32] Emmanouil Papadogiannakis, Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos P Markatos. 2021. User tracking in the post-cookie era: How websites bypass gdpr consent to track users. In *Proceedings of the web conference 2021*. 2130–2141.

[33] Sarakard Pasupa and Krit Pasupa. 2017. The potential of digital storytelling in encouraging sustainable lifestyle. In *SUIC International Conference*.

[34] Rizu Paudel and Mahdi Nasrullah Al-Ameen. 2024. Priming through Persuasion: Towards Secure Password Behavior. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–27.

[35] Rizu Paudel, Prakriti Dumaru, Ankit Shrestha, Huzeyfe Kocabas, and Mahdi Nasrullah Al-Ameen. 2023. A Deep Dive into User's Preferences and Behavior around Mobile Phone Sharing. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–22.

[36] Rizu Paudel, Ankit Shrestha, Prakriti Dumaru, and Mahdi Nasrullah Al-Ameen. 2023. " It doesn't just feel like something a lawyer slapped together." Mental-Model-Based Privacy Policy for Third-Party Applications on Facebook. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*. 298–306.

[37] Anna Podara, Dimitrios Giomelakis, Constantinos Nicolaou, Maria Matsiola, and Rigas Kotsakis. 2021. Digital storytelling in cultural heritage: Audience engagement in the interactive documentary new life. *Sustainability* 13, 3 (2021), 1193.

[38] Suzanne Prior and Karen Renaud. 2020. Age-appropriate password "best practice" ontologies for early educators and parents. *International Journal of Child-Computer Interaction* 23 (2020), 100169.

[39] Dhanush Kumar Ratakonda, Tyler French, and Jerry Alan Fails. 2019. My Name Is My Password: Understanding Children's Authentication Practices. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children*. 501–507.

[40] Janet C Read and Brendan Cassidy. 2012. Designing textual password systems for children. In *Proceedings of the 11th international conference on interaction design and children*. 200–203.

[41] KwangCheol Rim and SoYoung Choi. 2015. Analysis of password generation types in teenagers–focusing on the students of jeollanam-do. *International Journal of u-and e-Service, Science and Technology* 8, 9 (2015), 371–380.

[42] Bernard R Robin and Sara G McNeil. 2012. What educators should know about teaching digital storytelling. *Digital Education Review* 22 (2012), 37–51.

[43] Stuart Schechter, AJ Bernheim Brush, and Serge Egelman. 2009. It's no secret. measuring the security and reliability of authentication via "secret" questions. In *2009 30th IEEE symposium on security and privacy*. IEEE, 375–390.

[44] C Sense. 2019. The common sense census: media use by tweens and teens. 2015.

[45] Ankit Shrestha, Arezou Behfar, and Mahdi Nasrullah Al-Ameen. 2024. "It is Luring You to Click on the Link With False Advertising"-Mental Models of Clickbait and Its Impact on User's Perceptions and Behavior Towards Clickbait Warnings. *International Journal of Human–Computer Interaction* (2024), 1–19.

[46] Ankit Shrestha, Prakriti Dumaru, Rizu Paudel, and Mahdi Nasrullah Al-Ameen. 2023. Understanding the Challenges in Academia to Prepare Nursing Students for Digital Technology Use at Workplace. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*. 96–100.

[47] A Shrestha, A Flood, B Hackler, A Behfar, and MN Al-Ameen. 2024. TOWARDS THE DESIGN AND EVALUATION OF CLICKBAIT EDUCATION CONTENT: LEVERAGING USER MENTAL MODELS AND LEARNING SCIENCE PRINCIPLES. In *INTED2024 Proceedings*. IATED, 1794–1804.

[48] Ankit Shrestha, Audrey Flood, Saniat Sohrawardi, Matthew Wright, and Mahdi Nasrullah Al-Ameen. 2024. A First Look into Targeted Clickbait and its Countermeasures: The Power of Storytelling. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–23.

[49] Ankit Shrestha, Danielle M Graham, Prakriti Dumaru, Rizu Paudel, Kristin A Searle, and Mahdi Nasrullah Al-Ameen. 2022. Understanding the Behavior, Challenges, and Privacy Risks in Digital Technology Use by Nursing Professionals. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–22.

[50] Ankit Shrestha, Rizu Paudel, Prakriti Dumaru, and Mahdi Nasrullah Al-Ameen. 2023. Towards Improving the Efficacy of Windows Security Notifier for Apps from Unknown Publishers: The Role of Rhetoric. In *International Conference on Human-Computer Interaction*. Springer, 101–121.

[51] Ankit Shrestha, Tanusree Sharma, Pratyasha Saha, Syed Ishtiaque Ahmed, and Mahdi Nasrullah Al-Ameen. 2023. A first look into software security practices in bangladesh. *ACM Journal on Computing and Sustainable Societies* 1, 1 (2023), 1–24.

[52] Mary Theofanos, Yee-Yin Choong, and Olivia Murphy. 2021. 'Passwords Keep Me Safe'–Understanding What Children Think about Passwords. In *30th USENIX Security Symposium (USENIX Security 21)*. 19–35.

[53] RITU DUBEY Tiwari. 2019. An analytical study on the awareness of parents about cybercrimes against children. *Int. J. Transform. Media, Journalism Mass Commuication* 4, 2 (2019).

[54] Rishi Vaidya. 2019. Cyber security breaches survey 2019. *Department for Digital, Culture, Media and Sport* 66 (2019).

[55] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 1–16.

[56] Franzisca Weder, Stella Lemke, and Amornpan Tungarat. 2019. (Re) storying sustainability: The use of story cubes in narrative inquiries to understand individual perceptions of sustainability. *Sustainability* 11, 19 (2019), 5264.

[57] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children*. 388–399.

[58] J Zufic, Tomislava Zajgar, and S Prkic. 2017. Children online safety. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 961–966.