YOUTH DISCUSSIONS OF SECURITY AND PRIVACY ON SOCIAL MEDIA

By

Campbell R.Headrick

Thesis
Submitted to the Faculty of the
Graduate School of Vanderbilt University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE
in
Computer Science

May 10, 2024
Nashville, Tennessee

Approved:

Pamela Wisniewski, Ph.D.

Tyler Derr, Ph.D.

ACKNOWLEDGMENTS

For their support throughout this project, I would like to thank the following people who helped me realize this research:

Pamela Wisnieski
Mamtaj Akter
Katie Park
Sarvech Qadir
Ashwaq Alsoubai
Jackie Himel

TABLE OF CONTENTS

Page

1 Introduction 1

1.1 Motivation 1

2 Related Work 3

2.1 Youth Privacy and Security Awareness 3
2.2 Interventions and Education to Increase Youth Privacy and Security Awareness 4
2.3 Peer Support for Privacy and Security and Tech Caregiving 5

3 Methods 6

3.1 IGDD Data Donation 6
3.2 Data Scoping 6
3.3 Participant Demographics 8
3.4 Data Analysis Approach 9
3.5 Ethical Considerations 9

4 Results 11

4.1 RQ1: How do youth share and discuss their privacy and security experiences in private online chats? 15
4.1.1 Youth sought and gave advice to one another on their privacy & security matters . . 15
4.1.2 Youth shared stories of being victims of privacy & security threats 19
4.1.3 Youth recognized potential threats and took protective actions 22
4.2 RQ2: How do youth participate in risky behaviors regarding their digital privacy and security in private online chats? 24
4.2.1 Youth shared sensitive account information with others 25
4.2.2 Youth perpetrated security and privacy threats to others 28

5 Discussion 31

5.1 Youth Privacy & Security Practices and Awareness 31
5.2 Tech Caregiving vs. Risk Taking through Online Peer Support 32
5.3 Implications for Design and Education 33
5.3.1 Design implications 33
5.3.2 Implications for Education 34
5.4 Limitation 34

6 Conclusion 36

References 37

CHAPTER 1

Introduction

1.1 Motivation

In the present day, internet use has become interwoven into the lives of many, particularly youth. As youth explore the freedom the internet provides, they encounter a variety of different experiences that shape their social interactions, personal development, and understanding of security and privacy. This digital landscape can prove both empowering and challenging, making a nuanced understanding of the manners in which youth engage with it critical. This significance is reinforced further by both the growing presence of youth online, as well as the risks they can encounter [41]. Youth have been portrayed as both "digital natives" who are more internet-savvy than previous generations, as well as a particularly vulnerable demographic to a variety of risky behaviors [45]. This tumultuous conception of youth only reinforces the need for further research on their online behaviors.

The prevalence of social media platforms, online gaming, and a variety of other digital communication tools have reshaped the way youth interact and express themselves. With the rising usage of these platforms, understanding and navigating online security and privacy risks has become more critical than ever, especially for youth [24]. Throughout the years, a variety of research has been performed in order to investigate the risks youth encounter online. Prior work has focused on topics such as youth's individual level of awareness about privacy and security [26], as well as how to increase awareness through various interventions [39]. This research has offered valuable insight into youth engagement in security and privacy topics in numerous ways. However, far less research has taken place regarding the interactions youth have with their peers about security and privacy. Focusing on their private online conversations allows for an unobtrusive means of understanding the perspective of youth online behaviors, thoughts, and struggles, through their discussions of security and privacy topics with their peers. This is especially important as most existing research on youth security and privacy has focused on interviews or surveys with youth, which can be prone to effects such as recall bias [40]. Analyzing digital trace data, such as private conversations, offers ways that such biases can be reduced, while also providing information on a distinct dynamic of youth online interaction. In this study, we examine youth private social media interactions with peers and provide novel contributions in the process, guided by the following research questions:

RQ1: How do youth share and discuss their privacy and security experiences in private online chats?

RQ2: How do youth participate in risky behaviors regarding their digital privacy and security in private online chats?

In order to address these research questions, we leveraged Instagram private conversations (i.e., Direct Messages, DMs) that US youth ages 13-21 took part in. The conversation data was donated by youth as part of the Instagram Data Donation Project (IGDD) [41]. This dataset provides access to youth personal online discussions on security and privacy topics with others. We used a set of privacy and security related keywords identified in prior research [50, 29] to retrieve initial conversation data. Then, we manually reviewed the data to sort relevant discussions within this dataset. From this curated dataset, a thematic analysis [13] was performed to identify significant trends within the database. Through this analysis, we present an organic perspective on the ways in which youth engage in conversations about online security and privacy related topics and demonstrate their recurring strengths and weaknesses. We found positive trends in which youth advised each other about overall security and privacy topics, such as discussing the risk of threats, their personal habits with choosing passwords, and more. Often, youth recognized potential threats and hence, took protective actions. They also shared their experiences of being targets of privacy and security threats to raise awareness (RQ1). At the same time, there were concerning trends such as youth sharing sensitive information (e.g., passwords) through private chat and their experience of and/or intentions for privacy and security attacks, followed by social approval from online peers (RQ2). Based on our findings, we provide implications for design and education to promote positive online privacy and security practices for youth.

CHAPTER 2

Related Work

In this section, we first present prior literature regarding the concept of security and privacy for youth. Then, we introduce how intervention strategies to improve youth privacy and security practices are studied in existing literature. Finally, we discuss the role of peer support and tech caregiving for online privacy and security. By synthesizing existing work, we provide motivation and contribution of our research.

2.1 Youth Privacy and Security Awareness

Substantial prior literature has investigated youth perceptions of security and privacy practices. A common means of exploring the security and privacy practices of youth lies in researching their behavior on social media sites, such as Facebook, Twitter, and Instagram [16, 12, 32, 24]. Social media sites have been studied as online spaces with a variety of security and privacy risks for youth, making them prime targets for the investigation of such a subject. Youth security and privacy practices have been understood by analyzing youth's digital trace on social media including their textual posts, images, videos, and interaction with those of others [34]. For instance, a study of adolescent and adult Facebook users found that youth tended to disclose more personal information online and used privacy settings less than adults. However, the two groups had similar predictive factors for online disclosure and held strong awareness of the consequences of poor information control [16]. In other studies, a majority of youth were aware of and practiced varied privacy settings online [31, 30]. Confidence in youth's ability to manage their own security and privacy was also found [1]. In addition, prior literature suggests that youth value their online privacy and they have different boundaries as to what constitutes acceptable privacy based on their personalities and local social norms [12]. That is, youth's willingness to share personal information and privacy awareness greatly varied between youth under different settings [26, 24]. For instance, a strong awareness of security and privacy risks was observed from youth with low socioeconomic status [32]. As such, prior literature showed youth are well aware of their online privacy and security, yet heavily use social media sites and share personal information, albeit with ranging practices from youth to youth.

However, most prior work relied on interviews/survey data which can be prone to effects such as recall bias, which may not reflect the genuine complexity of youth practices online [45]. In addition, many existing works rely on analyzing publicly available digital trace data to understand youth privacy and security behaviors. Yet, the matter of security and privacy can be overlooked when analyzing the threats youth encounter online [19], indicating the need to examine their overall perspectives of privacy and security issues and po-

tential threats. Finally, issues emerge with the prevalence of research on youth privacy and security from the perspectives of adults that may not be reflective of youth behavior [7]. In this study, we focus on youth's private online conversations with their peers to unobtrusively explore their perspectives on security and privacy topics. Private social media conversations of youth can be a rich source of information on a distinct dynamic of youth online interaction related to their privacy and security practices and awareness.

2.2 Interventions and Education to Increase Youth Privacy and Security Awareness

A significant body of research is dedicated to examining the effective education and intervention strategies to improve youth privacy and security practices. Much of such research focused on the role of parents i.e., how effective their practices are at encouraging strong privacy and security practices among youth [44, 50, 42]. A recursive finding was that parental monitoring was an ineffective way of ensuring the privacy and security of youth online. For instance, restrictive mediation of youth online behaviors resulted in greater information disclosure among youth [42]. In addition, restricting youth online interaction denies them opportunities to actively learn and improve their online privacy and security practices [50]. As such, prior literature points towards harsh restrictive practices being ineffective at improving youth privacy and security practices. Instead, secure choices are better encouraged through education and instruction from parents and other family members rather than restriction [42, 20, 4, 3]. It was also encouraged that greater focus be placed on what would help youth learn rather than what their parents desires [50, 21, 10, 4, 3]. Overall, prior literature highlights that while parental restriction is an ineffective approach to promoting positive youth online privacy and security practices, parents can still have a positive educative role in guiding them to make privacy-preserving and secure decisions online.

Beyond parental restriction, existing research has documented the educative practices to promote youth online security and privacy. Some of the specific tools used for education include interactive models youth can undergo in order to learn a variety of strong security and privacy practices beginning from grade school, and can include storytelling elements. [14, 51, 8]. In one instance, a direct workshop program was used in order to educate middle school students about visual digital privacy [15]. While some of these programs for educating K-12 youth are present, they are generally eclipsed by programs aimed at university students [14, 15]. Overall, these programs demonstrate some of the mechanisms aside from parental guidance through which youth learn about proper security and privacy practices. While existing programs cover a variety of security and privacy issues youth encounter online, they often do so with little input from the youth themselves [29]. In this study, we provide suggestions for interventions and education to increase youth online privacy and security awareness based on an in-depth analysis of youth's private online conversations with their peers regarding their online privacy and security practices and perspectives.

2.3 Peer Support for Privacy and Security and Tech Caregiving

Prior research has explored online peer support and tech caregiving for security and privacy issues. For instance, a study found that while those who provided technical security and privacy advice had far greater knowledge on the subject than those they were advising, they were roughly equally effective when managing security and privacy as a team [28]. This demonstrates the usefulness of additional support from others in ensuring overall digital privacy [2, 5], and demonstrates the value of having effective tech caregivers. Additional research has found security and privacy practices to be influenced by one's peers [17, 18, 33, 2]. For instance, social factors held a major role in influencing one's security and privacy practices [18, 5]. In another, it was found that "social proof" can influence privacy and security practices e.g., notifications recommending security practices to be more effective when it indicated that many of their friends used said practices [17]. Also, youth's privacy behaviors were influenced more by individuals than organizations, suggesting that encouragement of strong privacy and security practices from specific people is effective at improving the same practices [33]. As such, prior literature shows that individual peers can have a strong and positive impact on the online security and privacy practices of others.

While much literature exists surrounding peer support and tech caregiving for security and privacy for adult populations, less attention has been given to youth. For instance, Lenhart et al. [30] found that 18% of youth considered peers to be their biggest influence on appropriate internet behavior, yet, the focus was not on security and privacy. Other research has explored youth peer advice seeking for topics such as sexual and mental health advice [23, 48, 6] rather than online security and privacy. This leaves a critical gap in the literature regarding how youth discuss digital security and privacy with peers, and how much their discussions reflect the practices they report elsewhere. Our research seeks to bridge such a gap and explore the discussions youth have about security and privacy with their peers on social media. Through our thematic analysis of youth's private Instagram conversations about security and privacy, we demonstrate how youth discuss the topic of security and privacy. Our work not only demonstrates how youth seek and provide advice about security and privacy, but also paints a detailed picture of their overall perspectives on the subject, their experiences with threats, and their involvement in risky behaviors.

CHAPTER 3

Methods

This section details the process involved in our research which can be broken down into several distinct steps. We began with selecting an available existing dataset of youth messages as a starting point. From there, keyword searches and relevancy coding were performed to scope a smaller dataset of youth discussion with digital security and privacy ramifications. Finally, a qualitative analysis was performed, coding the dataset and analyzing recurring trends in order to extract meaning from it. This entire process was done with proper IRB approval and consideration for the security of participants' information.

3.1 IGDD Data Donation

The original dataset from which we have scoped our data is the Instagram Data Donation (IGDD) project by Razi et al. [41]. This dataset consists of a body of Instagram direct messages (DMs) voluntarily submitted by English-speaking American youth between the ages of 13 and 21. Recruitment occurred through advertising the study on social media sites such as Facebook and Instagram as well as contacting youth-serving organizations. Participants were provided $50 Amazon gift cards as an incentive for completing the study. 195 verified participants contributed their data to the project in total. All participants were required to have had an account for at least 3 months while they were between the ages of 13-21, had direct message conversations with at least 15 different users, and had at least two conversations that they believed made them or another user feel unsafe. Participants downloaded their data from Instagram and uploaded it to a secure web-based system. The entire data collection process followed procedures approved by the original authors' Institutional Review Board (IRB). Prior to submission, each participant was provided with consent forms (provided with parental consent and assent forms, in the case of minors) describing the research, research process, potential benefits, and risks for participation. Due to the wide array of content in unsafe messages, participants were warned against uploading any conversations that included nudity of minors, as such illicit content would need to be reported to authorities. Detailed instructions on how to remove such content were provided in order to minimize incidents.

3.2 Data Scoping

Scoping and relevancy coding was a process that consisted of several distinct steps. First, keywords were selected in order to perform scoped searches for relevant messages. Then, these messages and surrounding messages were organized into a dataset of "sub-conversations." After this dataset was produced, it underwent

additional relevancy coding to ensure the usefulness of its sub-conversations. Below, we explain the details of our data scoping processes.

Locating relevant discussions in the dataset demanded selecting a set of keywords that had significant ramifications for security and privacy. The selected keywords were chosen based on a review of existing literature examining common themes in youth discussions of digital privacy and security threats, where these keywords emerged as significant. For example, Wisniewski et al. found discussions of being "hacked" and having accounts "stolen" were prominent in interviews with adolescents about negative online experiences [50]. Similarly, Kumar et al. noted "scam", "password", and "privacy" concerns emerged repeatedly in focus groups with teens on safety practices [29]. Therefore, the consideration of prior work aided keyword selection to effectively capture relevant youth dialogues around salient digital privacy and security issues. A search was performed seeking messages containing any of these keywords as well as the ten preceding and proceeding messages, forming sub-conversations that provided the necessary context in order to understand the proper connotations of each keyword message. The initial search of these keywords returned 5177 sub-conversations across 2591 conversations. The keywords included in the initial data scoping and the grounds for selecting those keywords are:

- **"Security"**: The inclusion of "security" as a keyword stems from its frequent use in discussions about online safety among youth and was chosen due to its frequent appearance in youth discussions around digital safeguarding and online protection. This keyword represents a broad theme encompassing various aspects of digital safety, which is relevant to the experiences of youth in digital environments.

- **"Privacy"**: The term "privacy" was selected for its central role in conversations about personal data protection and confidentiality in digital spaces. "Privacy" represents a key concern among youth, often discussed in the context of social media usage and online interactions.

- **"Hacked"**: The keyword "hacked" reflects a specific risk scenario frequently encountered online and is included based on its recurrence in dialogues regarding unauthorized access to personal accounts and privacy breaches. This choice is supported in the methodology of Theofanos et al. in their thematic analysis of digital privacy perceptions in children [47].

- **"Password"**: The term "password" was selected to explore discussions regarding secure account management and authentication practices, reflecting a fundamental aspect of online security. This keyword selection is supported by Kumar et al. in conducting focus groups with youth on safety practices [29].

- **"Scam"**: The inclusion of "scam" as a keyword was informed by the need to understand youth encounters with deceptive online practices. Research has shown that youth internet users are often targeted by

online scams, making it a relevant area of concern in our examination of digital safety.

- **"Stolen"**: The term "stolen" was included to cover aspects of digital theft, such as account takeover or unauthorized use of personal information. This keyword addresses a serious concern faced by youth in terms of personal data security and identity protection.

Next, we conducted relevancy coding to isolate the relevant sub-conversations from the irrelevant ones. Sub-conversations were deemed sufficiently relevant when related to digital privacy and security, or discussing a violation of such notions. Irrelevant conversations are those not related to privacy, not related to security, or not online. There were numerous recurring trends that resulted in sub-conversations being marked irrelevant. Some sub-conversations were considered irrelevant as a consequence of using a keyword in a common context unrelated to digital privacy and security. Examples include using the term "security" to refer to security guards, or "password" when sharing a password to a one-time Zoom meeting or video game lobby. Further trends included concepts such as keywords being used in the context of storytelling or role play, as well as the same conversations being submitted by multiple participants. Whenever such duplicate conversations were encountered, a maximum of one instance of its sub-conversations was coded as relevant. Each sub-conversation was documented in a respective spreadsheet, alongside reasons for exclusion in the case of irrelevant instances. All relevancy coding was performed solely by the first author in order to ensure consistent methodology throughout the process. After relevancy coding was complete, 1318 sub-conversations remained across 741 conversations with keyworded messages from 149 youth participants. 52% of sub-conversations contained the word "password," in their central message, while 23% contained "hacked," 12% contained "scam," 7% contained "security," 6% contained "privacy," and 1% contained "stolen." This total percentage exceeds 100% due to some sub conversations containing more than one keyword in their central message.

3.3 Participant Demographics

The body of 149 verified participants included in our dataset was a subset of 195 youth who participated in the original IGDD study. 149 youth had a minimum of 1 and a maximum of 67 messages in their conversations. The median amount of conversations per youth participant was 3, while the mean was 8.85. The ages of youth participants ranged from 13-21, with a mean of 17.26. Of our participants, the majority (69%) identified as female, while the remainder identified as male (22%) or non-binary/preferred to self-identify (9%). Participant race had the following breakdown: 50% of youth identified as White/Caucasian, 26% as Black/African-American, 22% as Asian or Pacific Islander, 23% as Hispanic/Latino, 4% as American Indian/Alaska Native, and 3% preferred to self-identify. This total exceeds 100% as some participants iden-

tified themselves as mixed-race. Finally, for participant sexual orientation, 52% identified as heterosexual or straight, 26% as bisexual, 11% preferred to self-identify, and 11% as homosexual or gay.

3.4 Data Analysis Approach

We performed the thematic analysis proposed by Braun and Clark [13] to identify key trends and themes from our dataset. Due to having performed relevancy coding, the first author already had familiarity with the dataset and began coding based on the initial trends. The first author began coding a set of 500 randomly selected sub-conversations to identify initial codes and group them into major themes. The themes were then arranged based on the research questions they were most relevant to. RQ1 featured themes such as experiences with security threats, and personal practices online, while RQ2 featured themes such as account sharing and involvement in cyber-threats. Next, the co-authors reviewed the themes and codes for each RQ to ensure that they represent the data. Once all authors agreed on the identified themes and codes, the first author coded the entirety of the dataset. The coded dataset was then once again discussed with co-authors, in a continuous process of refinement in order to ensure that the themes and codes we identified represent the trends in data the most.

In our final codebook, we identified five total themes within the data. For RQ1, these themes focused on the overall discussion of youth's security and privacy experiences and perspectives. Such themes were 1) Youth sought and gave advice to one another on their privacy & security matters, 2) Youth shared stories of being victims of p&s threats, and 3) Youth recognized potential threats and took protective actions. For RQ2, themes focused on potential risky behavior youth engage with. These themes were 1) Youth shared sensitive account information with others and 2) Youth perpetrated security and privacy threats to others. For each theme, several individual codes represent more specific trends within the data, and an illustrative quotation is included for each code. The final codebook including these themes is represented in Table 4.1. Lettering and numbering to label users for each message corresponds to an anonymous way of identifying individual speakers in the conversation, as well as distinguishing the youth participant from other users. Further identifying or otherwise sensitive information in the quotes was replaced with words in braces in order to indicate what information was originally present. Emoticons are represented through text in parentheses combined with the amount they are used, such as (smile emote x2). The percentages for each code, theme, and RQ are all calculated out of the total amount of sub-conversations in the entire final relevant dataset.

3.5 Ethical Considerations

An extensive procedure was performed to ensure proper ethical treatment of the sensitive data involved in our research. Our research received IRB approval from our respective institution, and all participants involved

completed IRB and CITI Protection of Minors (POM) courses. When documenting sub-conversations in our project, documentation was done without the original usernames included in order to protect the confidentiality of the original participants, while still having enough info to trace messages to users when useful. This manifests within the codebook as participants having their usernames replaced by generic labeling meant to clarify who the speaker is without giving away any further information about them. Furthermore, identifying information found within the content of the messages themselves was removed from any documentation outside of secure storage. This information was replaced with generic identifiers, such as [NAME] or [PASSWORD] to make the original context clear despite the removed identifying information. No images were directly included within the dataset, and other potentially insecure information, such as hyperlinks, were also assigned generic identifiers. These spreadsheets were saved and stored on university-approved secure storage, and team members were not permitted to save any of these documents to their personal computers or other forms of cloud storage. Furthermore, all access to both the database and the secure storage was performed while connected to the affiliated university Virtual Private Network (VPN).

CHAPTER 4

Results

In this section, we present the major findings on how youth discuss their privacy and security experiences in private online chats and how they participate in risky behaviors regarding their digital privacy and security in private online chats. Youth participants are indicated by a "P" while other users in conversations are labeled with an "O" or "O1/O2" in the case of multiple other participants. The demographic information provided refers to that of youth participants.

Table 4.1: Codebook

Themes	Codes	Illustrative Quotations
RQ1: How do youth share and discuss their privacy and security experiences in private online chats? (61%, n=809)		
Youth sought and gave advice to one another on their privacy & security matters. (29%, n=380)	Regarding potential security and privacy threats (6%, n=81)	*O : Cause I feel like it's a scam* *O : But I knew you'd know maybe* *P : Hey! It's a legit organization and it's great that you got it! They do charge money to join though for little benefit...it's not exactly a scam but you do need to consider if it's worth it* (Female, 18-year-old youth)
	Regarding password practices (6%, n=80)	*P : I have so many passwords that I'm legit confused how I haven't locked myself out already so* *O : ahahaha* *O : all my accounts are under the same password but you didn't hear that from me* *P : I mean they're all variations of the same password for me but hoo boy remembering which one I used is tough* (Female, 19-year-old youth)
	Regarding forgotten passwords (5%, n=66)	*P : I forgot my Kik password lmao* *O : Oh no* *P : Idk why I didn't write it down* *O : Well lol. Why didn't you tho XD* *P : I thought I'd remember it* (Non-binary 15-year-old youth)
	Regarding security issues for technical difficulties (4%, n=56)	*P : I'm so fckn annoyed cuz I know the password n stuff to the acc but it keeps blocking me and saying Im suspicious??* *O : Whattttt* (Male, 21-year-old youth)

Continued on next page

Table 4.1 – continued from previous page

Themes	Codes	Illustrative Quotations
	Regarding external privacy & security events (4%, n=51)	*O1 : YES KPOP STANSS* *O1 : THE POWER WE HAVE* *O2 : I loved people posting blue cartoon characters (laughing emote)* *P : but with anonymous faces* *O3 : and they shut down an app that was meant to expose protestors with fan cams* *O3 : it was absolutely hilarious lemme say* *P : they also hacked michigan's senate website* (Female, 19-year-old youth)
	Regarding shared accounts (4%, n=46)	*O1 : what should the password be* *O1 : Or can I choose it* *O2 : for the announcements do you want to post it or post it on the account's story* *O3 : Hmm* *P : Is the decision of choosing a password that necessary?* *O2 : make sure it's easy to remember* (Male, 14-year-old youth)
Youth shared stories of being victims of p&s threats. (18%, n=232)	Shared scam and hack experiences (10%, n=123)	*P : So I looked online and seen an online shop called.vardon shop and it had an iPhone 12 white fully unlocked for $81.99* *P : So I purchased it but it didn't give me a day it was going to be shipped or nothing (crying emote) I think it was a scam (crying emote) and I lost all my money I only have $18.01 up there now* *P : They better send my stuff or imma get mad* (Female, 18-year-old youth)
	Took protective measures after getting scammed or hacked (4%, n=56)	*P : I got hacked* *O : Ye I saw your story* *O : You fixed it yet?* *P : Yeah, I changed my password and stuff* (Female, 17-year-old youth)
	Reflected on digital security and privacy beyond the internet (2%, n=31)	*P : i'm tired and my parents are gone* *O : Gone gone?* *O : Throw a party LOL* *P : you don't get that we have security cameras all around our house* *O : Oh shit* *O : Nvm lmao* (Female, 17-year-old youth)

Continued on next page

Table 4.1 – continued from previous page

Themes	Codes	Illustrative Quotations
	Warned others about their own hacked accounts (2%, n=22)	*P : If I sent a link, I was hacked and do NOT click it* *P : It's been happening a lot lately, sorry* *O : Ok* *O : No problem* (Non-binary, 13-year-old youth)
Youth recognized potential threats and took protective actions. (15%, n=197)	Identified hacked accounts (6%, n=81)	*P : Be careful with dms like that. My friend's insta got hacked and the person sent dms to me and a bunch of others saying out profiles were rated the worst insta ever with a link* *P : The link asked you to login to insta and it was pretty obvious they were trying to steal people's login info* *O : Oh yeah I got one and it was one about most annoying? Yeah it was obvious that they were hacked* (Female, 19-year-old youth)
	Identified scammers (5%, n=69)	*P : I'm trying to tell whether it's a scam or not but idk* *P : Probably is but who knows* *O1 : whats her @* *O2 : she seems scammy* *P : Yeah ik and she just asked what bank I have, if she asks for my routing number I'll shut it down* (Female, 20-year-old youth)
	Expressed privacy boundaries (4%, n=48)	*O : Hold old are you turning?* *P : I prefer to keep my age a secret, privacy and safety reasons.* *O : ooOo okay* (Female, 19-year-old youth)
RQ2: How do youth participate in risky digital privacy and security behaviors in private online chats? (39%, n=509)		
Youth shared sensitive account information with others. (28%, n=374)	Shared passwords with others (16%, n=215)	*P : The username is [USERNAME]* *O : Do I put [PASSWORD]* *P : The password is [PASSWORD]* (Male, 14-year-old youth)

Continued on next page

Table 4.1 – continued from previous page

Themes	Codes	Illustrative Quotations
	Showed intent to share passwords (5%, n=69)	*P : Welcome new Instagram admins!! After a little more organization we'll give you to password to access the account, and find out what days are best for you to post. There's another, separate chat that consists of all the old/current admins. The other chat is mainly consisted of random content and isn't all that active but feel free to ask to join in on the chaos whenever. Welcome!!* *O1 : Welcome everyone (pink hearts emote) I'm [NAME]!! I can't wait to work with you guys on the account* *O2 : Thanks for choosing me as an admin (heart emote)* (Female, 19-year-old youth)
	Shared their account with peers (5%, n=60)	*P : And [NAME] knows my password to everything* *O : I-* *P : and my phone password is the same as his so* *P : and [NAME] is special* *O : okaY more hurt* *P : so she gets her fingerprint* (Female, 16-year-old youth)
	Shared their account with family members (2%, n=30)	*P : idk my social security number* *O : is your parents still awake* *O : or you might be able to come back to it* *P : i'll just come back to it* (Female, 18-year-old youth)
Youth perpetrated security and privacy threats to others. (10%, n=135)	Attempted to hack or scam others (5%, n=62)	*P : I purposely hacked him lol* *O : LOLOLOLOLOLOL* *O : THIS GENIUS HAHAH* *P : And changed his password to something really different* *P : So he's locked out of his account. . .* (Female, 17-year-old youth)
	Showed intent to hack or scam others (3%, n=43)	*O : Should I accept (smirk emote)* *O : I wanna have him send me the money and then block him* *P : Dont be shy scam him (heart eyes emote)* (Female, 15-year-old youth)

Continued on next page

Table 4.1 – continued from previous page

Themes	Codes	Illustrative Quotations
	Spammed/scammed in group chats (2%, n=30)	*P : Completely free! Up to 30'000 followers and 5000 likes to all your posts! For details go to our main page (right arrow emote) @[LINK]* *P : Up to 30'000 followers and 5000 likes to all your posts! 1. No password required (exclamation point emote) 2. It is 100% safe & secure (lock emote) 3. Completely free (free emote) For details go to our main page (right arrow emote) @[LINK]* (Female, 19-year-old youth)

4.1 RQ1: How do youth share and discuss their privacy and security experiences in private online chats?

In this subsection, we discuss themes regarding how youth share and discuss their privacy and security experiences in online private chats (RQ1). The most salient theme was where **youth sought and gave advice to one another on their privacy & security matters (29%, n=380)**. Here, there were a variety of instances in which youth advised each other about overall security and privacy topics, such as discussing the risk of threats, their personal habits with choosing passwords, and more. There were also a variety of instances where **youth shared stories of being victims of p&s threats (18%, n=232)**. In these discussions, youth described their experiences where they have explicitly suffered from violations of their online security and/or privacy. Finally, there were a variety of cases where **youth recognized potential threats and took protective actions (15%, n=197).** In such discussions, youth recognized potential threats without falling victim to them, and discussed such with one another, as well as establishing ground privacy rules they shape their behavior around.

4.1.1 Youth sought and gave advice to one another on their privacy & security matters

The most frequent privacy and security related topic that youth discussed was broadly seeking and offering general advice and perspectives about privacy and security with one another. The most commonly discussed topic was the potential for threats online and demonstrating awareness of the concept. Discussion of passwords was also frequent, be it personal choices made with them or frustration with having lost them. Youth also sought and offered aid with technical issues with their accounts, as well as security and privacy topics external to their own experiences. Lastly, they also discussed what they believed the appropriate practices for shared accounts to be.

One of the broadest manners in which youth sought and offered thoughts and advice to one another was

instances **regarding potential security and privacy threats (6%, n=81)**. Youth most generally discussed the security and privacy violations they subject themselves to through involvement online. For instance, youth discussed the notion that not only do social media sites have their data harvested for government use, but also that other methods of government tracking exist. This demonstrates familiarity with the potential insecurity of being on social media, particularly around the insecurity of their personal information online. The conversation below is an example of such a notion.

> ***P :*** *Why use tik tok and have your info be stolen and sent to China when you can use this app and have it stolen and sold to China (smile emote)*
> ***O :*** *she acting like the US doesn't track our every move*
> ***P :*** *like we're literally assigned a number at birth and ur scared of china seeing that a random person in florida is watching a dancing video on tiktok*
> (Female, 18-year-old youth)

Another form of general discussion and advice about potential threats that took place were cases of "false alarms." These were instances where youth in chat initially believed something to be a threat to their security and privacy, only to ultimately be mistaken. In some cases, youth make assumptions about their peers and then realize they were incorrect. For instance, a youth is worried their account might have been hacked based on something their peer said, but said peer reassures them that their account is perfectly fine. Such a case demonstrates both youth willingness to be vigilant about potential threats, as well as lower their guard once they realize there isn't an actual issue. It also demonstrates that while youth may not always be correct in their assumptions that they have encountered threats, they nonetheless are conscious of the possibility:

> ***P :*** *u made me spill my water*
> ***O :*** *what i didnt do anytjing*
> ***P :*** *bc when u mentioned my account i got scared*
> ***O :*** *PLSSSS*
> ***P :*** *i thought it was being hacked or somethin*
> ***O :*** *im sorry its not hacked it's completely fine*
> ***P :*** *thanks*
> (Female, 17-year-old youth)

Beyond generally discussing security and privacy threats, youth also gave input **regarding password practices (6%, n=80).** In these instances, youth demonstrated a variety of positive and negative password practices alike. A positive example is found in the below exchange. Here, a youth expresses the use of a

very long (and presumably difficult to guess) password, to their peer's shock. Situations like this demonstrate standout cases of effective password practices, where this user surprises even their peer with the length and presumed complexity of their password. Such cases demonstrate that many youth are aware of strong password practices and make effective use of them:

P : *My password is 30 characters long lol*

O : *oh my god*

P : *3 capitals*

(Male, 14-year-old youth)

While youth discuss positive password practices at times, they also discuss negative ones as well. In these cases, youth express notions such as frequently using the same password for a variety of different accounts. In the instance below, no meaningful feedback is provided by others as well, merely an exclamation of amusement before moving on. This is a recurring trend: when poor password practices come up, rarely is advice provided on how to improve upon them. Rather, peers express they are in the exact same situation with their own weak password practices, or don't acknowledge the notion much at all. Such a trend is concerning as undesirable practices are not challenged nor is meaningful feedback provided on them:

O1 : *i change my pas every 2748383 years*

O2 : *I have a lot but yeah I do I just didn't know which was which*

P : *i change my password never*

O2 : *LMAO*

(Female, 17-year old-youth)

While passwords are often discussed in terms of overall practices, another noticeable trend we observe is that youth have numerous conversations **regarding forgotten passwords (5%, n=66),** a common cause for issues accessing accounts. Youth shared this issue by expressing that a password was lost with varying levels of feedback from peers. Commonly, conversation partners found amusement in the situations or affirmed they have made similar mistakes. An example of the former is found below with a sarcastic response. In this case, one youth mentions they forgot their password, and their peer pokes fun at them for not having better practices for remembering it. Conversations like this demonstrate youth's tendency to forget passwords at times, and the common sort of response to it:

P : *I just forgot the password lmao*

O : *nice job*

P : *Ikr*

(Female, 18-year-old youth)

While forgotten passwords were the most common cause for issues with account access youth discussed, they were not the only ones. Youth also held conversations **regarding security issues for technical difficulties (4%, n=56),** along with other barriers to full access to their accounts. For instance, youth encountered issues other than a forgotten password that locked them out of their account entirely. In cases of such issues, the youth's peers regularly offered advice on how to resolve the issue, trying to help them sort out the situation. In the example conversation below, in response to hearing one youth's frustration with accessing an account, one of their peers tries to figure out what's wrong to help them through the situation. While they are ultimately unsuccessful, their interest in trying to help talk through the situation still demonstrates a willingness to offer support to the best of their ability. It also shows how youth can help walk their peers through technical issues they encounter:

P : *I have an account but it won't let me in. Tried to reset password but got no fucking email anywhere from the dozen times I've done it throughout the say so I had to create an account with my valencia email*

O : *You had to, its required by Valencia for each math class*

O : *Except for the one you did in person cause duh*

P : *I used the service, but I never had to do all this certification stuff*

O : *Well what did you use the service for then?*

P : *I don't remember*

O : *Hmm*

(Female, 18-year-old youth)

While many of the discussions youth had regarding security and privacy directly related to their own experiences and perspectives, they also held conversations **regarding external privacy & security events 4%, n=51).** In these instances, youth generally discussed security and privacy related topics that had no direct influence on their friends and family but were nonetheless significant. This generally fell into one of three instances of whose security and privacy were discussed: strangers, governments, and celebrities. As with many instances, these conversations were held with a range of emotions regarding the topic, such as frustration with a celebrity having their security breached. In the example below, users, including the youth participant, are upset that a popular YouTube content creator they admire has been hacked. The example demonstrates youth are following current events regarding security and privacy, noting the experience of others whom they know little, and discussing significant events on the subject impacting public figures:

O1 : *My head hurts*

O2 : *Same... Markiplier was hacked...*

O2 : *The group got 100k and to celebrate, hacked him...*

O1 : *WHAT*

O1 : *ON INSTAGRAM?!?!?*

P : *What group hacked him?*

...

O2 : *OurMine Team*

O2 : *It makes me sick. He's an amazing person and a YouTuber*

(Female, 19-year-old youth)

Finally, youth held discussions and exchanged advice **regarding shared accounts (4%, n=46)**. Here, they discussed what they believed to be appropriate security practices for the accounts they shared with others. Their conversations covered topics such as what kind of information or credentials are appropriate to share with others, and with whom. In the example below, a youth asks for feedback on their practices in sharing accounts and receives an affirmative response. Such examples demonstrate youth's considerations for what are and are not acceptable practices for shared accounts from a security and privacy perspective:

P : *Also I have the password for my gf's account.... Is that bad?*

O : *No. It shows you trust each other*

(Non-binary, 15-year-old youth)

4.1.2 Youth shared stories of being victims of privacy & security threats

At times, youth have been targeted by the malicious actions of others online, often suffering consequences. In many of these instances, they spoke out to their peers, describing their experiences with malicious actions against them. In other cases, they would explicitly present their victimization as a warning to others, in hopes they would not fall prey to the same forms of attacks they did. In numerous instances, the youth shared how they actively performed measures to recover lost accounts and protect themselves from future attacks. In further instances, youth reflect on their experiences with digital privacy and security equipment such as cameras. In each of these cases, youth demonstrate a conscious awareness of the direct threat of malicious actors and a willingness to speak about them. They would often make positive choices in either trying to improve their own practices or seeking to warn others.

The most common way youth expressed their victimization was cases where they **shared scam and hack experiences (10%, n=123)**. Here, the youth did not provide significant input on recovery steps or offer

warnings, simply describing that a breach of their privacy or security had occurred with varying emotions. At times, youth shared their experiences indifferently without emotions. The lack of clear emotion in such instances makes it difficult to discern the youth's perspective on the attack, but they took it seriously enough to share. In other cases, the youth were clearly alarmed and agitated, or even lightheartedly joked about these circumstances. An example of a more alarmed case describing a security breach is found below. Here, a user is distraught after believing they were hacked, and a peer is upset that this would happen to them:

P : *I THINK THEY HACKED MY SPOTIFY*

P : *I WAS SCARED*

O : *thank god i do zaful i-*

O : *WHAT*

P : *BUT IDK IF IT WAS that*

O : *SUE THEM*

(Female, 18-year-old youth)

While many cases of sharing experiences with scams and hacks were prompted by the victim, at times, users confirmed what had happened to them after somebody else assessed their victimization. In this instance, not only does a youth correctly identify their friend has been hacked, but they also provide advice to them on how to resolve this circumstance. Such a trend is notable not only for demonstrating youth's (often correct) assumptions that their friends have been victimized but also for a willingness to share advice on what could help them recover from such attacks. It is worth noting that in these cases, users do not mention their account was compromised until somebody else brings it up first. This indicates the role peers have in bringing out users' discussions of attacks they suffered:

P : *Uh dude I think you might be hacked*

O : *Ya I am*

P : *Gotta change that password then*

(Female, 18-year-old youth)

Next, in many cases, youth shared their experiences with how they **took protective measures after getting scammed or hacked (4%, n=56)**. An example of this is found in the below exchange. Here, as a direct response to suffering from a threat, the victimized youth successfully managed to resolve the issue by making a strong choice with their protective practices. Changing passwords was the most common practice employed, indicating that this is common knowledge among youth. Examples also show that even when youth get attacked, there are many instances where they know how to recover their accounts:

P : *I got hacked*

O : *Ye I saw your story*

O : *You fixed it yet?*

P :: *Yeah, I changed my password and stuff*

O :: *Oh hey that's great*

(Female, 17-year-old youth)

Beyond cases where direct threats have occurred, youth also demonstrate awareness of digital measures for ensuring physical security. In numerous cases, youth **reflected on digital security and privacy beyond the internet (2%, n=31),** displaying awareness of protective practices such as cameras. This commonly occurred through discussing the camera usage of individuals they know. This instance features a youth discussing the theft of their stepfather's car, and how they were able to discern what had happened through a neighbor's security camera. While the youth was not the victim in this situation nor did they own the cameras, cases like this demonstrate awareness of how digital equipment can help in resolving security and privacy situations, even physical ones.

P : *My stepdads car got stolen last night*

P : *Like full on gone*

O : *Bro*

O : *The fuck u mean*

P : *His car, with his keys and wallet inside*

P : *Got stolen*

P : *We just found some security footage from a meighbor*

P : *There was a dude walking around trying cars and shit, he hit jackpot with my stepdads*

(Female, 20-year-old youth)

Finally, in numerous cases where they were victimized, youth sought to try and prevent such occurrences from happening to anyone close to them. In these cases, youth **warned others about their own hacked accounts (2%, n=22)**. Frequently, this manifests as youth telling people to ignore the messages their account had posted, often being quite apologetic about it. In the below example, one of the youth's peers offers support to them for their guilt in making such a mistake. Instances like this demonstrate clear cases where youth try to protect others from suffering the same violations they did and demonstrate a strong form of peer support in the process:

P : *I'm sorry I got hacked change you password right now if you logged into that website!*

O : *i didn't lmao*

P : *I'm really sorry! I copy and pasted that message just in case someone one else was a big gullible idiot like me...*

O : *nooo it's okay (Crying emote x2)*

(Female, 16-year-old youth)

4.1.3 Youth recognized potential threats and took protective actions

Even in cases where they were not victims, youth demonstrated consciousness of potential security and privacy threats. Oftentimes, youth detect and thwart potential threats before they can harm anybody. They also share how they establish boundaries for maintaining privacy on the internet. In each of these instances, youth demonstrated familiarity with online threats to recognize situations under which security or privacy violations occur.

The most common cases where youth recognized and took action against potential threats were ones where youth **identified hacked accounts (6%, n=81)**. In some such conversations, youth expressed confidence that an account outside the conversation was hacked, often the account of somebody they know. Sometimes, their confidence was expressed with frustration; other times, merely indifference. In the example below, two users discuss an account they believe has been hacked dispassionately. A youth participant brings up that the account was hacked, while their peer verifies that they also recognized it was hacked. The fact that it is presented as a warning also demonstrates another trend that youth try to warn each other to avoid dangerous accounts. Such a trend confirms that youth are able to identify threats to their security and privacy and avoid engaging with them, as well as inform their friends to do the same:

P : *Be careful with dms like that. My friend's insta got hacked and the person sent dms to me and a bunch of others saying out profiles were rated the worst insta ever with a link*

P : *The link asked you to login to insta and it was pretty obvious they were trying to steal people's login info*

O : *Oh yeah I got one and it was one about most annoying? Yeah it was obvious that they were hacked*

(Female, 19-year-old youth)

In some instances, youth directly call out instances of their own Instagram conversations being compromised. For instance, in the example below, the youth encounters a message they deem suspicious and immediately asserts that the account, presumably originally one of their friends, has been hacked (for the second time) and it is not worth engaging with the account's offer. This demonstrates that youth do not see their Instagram conversations as a safe space from attacks and are prepared for potential threats within them,

just as they are outside the conversations:

> ***O :*** *[NAME](credit card emote) this is crazy, I actually got a $1000 VisaGiftCard and all I had to do was participate a little bit and they gave me one. I used it too pick up a new laptop I've been eyeing Haha!! I thought u might want to get one since you follow me. Hurry tho there's only a few of them left!! Go*
>
> ***O :*** *[NAME] sent an attachment.*
>
> ***P :*** *y'all really hacked her twice, fuck is wrong with y'all*
>
> (Male, 21-year-old youth)

In a similar manner, in many instances, youth effectively **identified scammers (5%, n=69)**. Here, the youth identified cases where malicious actors sought to take advantage of them and others. Unlike hacked accounts, scams inherently tended to be discussed in a consistently informative manner. An example of a clear warning about a scam outside of the conversation is the below conversation. Here, one user is excited about having won something, but after a youth participant points out that needing to pay for it seems like a scam, they agree. The example shows another strong case of how the warnings youth provide about scams can help protect each other from falling prey to security and privacy breaches:

> ***O :*** *I won a backpack*
>
> ***O :*** *A 100 dollar backpack*
>
> ***O :*** *It's sick*
>
> ***P :*** *Oh dang, get it girl*
>
> ***O :*** *Ikr. I only have to pay the shipping which is $23*
>
> ***P :*** *Sounds like a scam tbh*
>
> ***O :*** *Ya*
>
> (Female, 17-year-old youth)

Another shared trend with the discussion on hacked accounts is that youth were able to identify scams within their own conversations. A concrete example of this is the below conversation. Here, in response to a suspicious message advertising a service, a youth immediately recognizes it as a scam. Ending with a "lol" suggests they find some humor in this attempt, which was commonly observed in similar instances. Similarly to the hacked instances, recognizing scams like this one within these Instagram conversations demonstrates the vigilance of youth against potential threats:

> ***O :*** *Hey girl, some of us are doing a little support follow loop for women only accounts on instagram! If you want to join(heart emote)you will get at least 1200 followers just by following*

all 15 people and help our community grow :-) all you have to do is follow the steps below...

P : *i think this is a literal scam lol*

(Female, 21-year-old youth)

Beyond security risks, youth also **expressed privacy boundaries (4%, n=48)** on the internet, often through describing the practices they apply to maintain their privacy. At a personal level, youth discussed their choices in when to withhold personal information from others, such as using a false name to maintain anonymity. The example below shows a situation where youth are okay with sharing their actual name in this Instagram conversation but use a false one elsewhere. This example demonstrates a manner in which youth choose to maintain their privacy, while they do feel comfortable sharing more personal information through some private chats online:

P : *I'm [NAME], [PRONOUNS], also a lesbian! :))*

P : *I use [FALSE NAME] on that acc for privacy u know*

(Non-binary, 13-year-old youth)

In other instances of privacy discussion, youth discuss with each other what they consider to be acceptable privacy on the internet. This topic comes up at both a personal level of each other's boundaries, as well as in broader discussions on what level of privacy is acceptable on the internet. The below instance is a case of the latter. In this conversation, a youth discusses with a peer the conflicting notion that they value being able to learn about their teachers' politics, but find it alarming how much information about people can be found online. Such examples illustrate youth contemplation of the complexities of security and privacy online, acknowledging the benefits they gain from it, as well as the concerns it raises:

P : *it IS interesting to look up teachers' party affiliation and look up people's houses, but there is a valid privacy concern*

P : *it's also helpful when registering ppl to vote if they don't know they're registered*

O : *have public info is iffy yes but being able to see monetary contributions is important imo*

(Non-binary, 18 year old youth)

4.2 RQ2: How do youth participate in risky behaviors regarding their digital privacy and security in private online chats?

In this section, we present themes regarding how youth participants in risky behaviors related to their privacy and security on private online chats (RQ2). The most common form of risky behavior was cases where **youth shared sensitive account information with others (28%, n=374).** Beyond merely discussing the

security practices with shared accounts, youth directly shared their personal account information with others, be it more trivial shared accounts for fun, or potentially more sensitive information. Another major form of risky behavior encountered was instances where **youth perpetrated security and privacy threats to others (10%, n=135).** Here, youth were not victims of attacks, but rather the source of the attacks. Such conversations involved plotting future actions, discussing those that they have already performed, or directly trying to compromise the conversations themselves without being caught and called out.

4.2.1 Youth shared sensitive account information with others

The most common form of risk-taking among youth was sharing their account information with others. For instance, youth shared security information such as passwords immediately with conversation members, and consequently, much of their sensitive information can be found in these discussions. In other instances, youth discussed plans to share their accounts and sensitive information or had already been sharing accounts with others including friends and family inside and outside of the conversations. It is worth noting that not all account-sharing practices are inherently dangerous, and thus nuance is critical to separate specifically concerning practices from innocuous ones.

The most prevalent form of account sharing was youth directly **sharing passwords with others (16%, n=215)**. In these instances, youth shared passwords and similar sensitive information in the conversations or indicated an immediate exchange occurred elsewhere. For instance, an account was shared with multiple users and the credentials for the shared account were shared in private chats in the example conversation below. The mention of "admins" suggests a variety of people share joint ownership of the account discussed, meaning this account is likely dedicated to a shared topic or interest rather than containing much sensitive information. Such account-sharing practices were less risky despite the connotations of account credentials sharing:

> ***O1 :*** *Hey y'all even tho I said I can't admin anymore, I saw BNHA on the recommendations and I'd love to post about BNHA whenever! If you guys need the extra hands.*
> ***O1 :*** *My phone isn't letting me log out of accs so I'm still logged in*
> ***O2 :*** *OoF fam we just got three new admins we're working on to get the password. I'll have to see?*
> ***P :*** *If you need it I'm pretty sure the password is [PASSWORD]*
> (Female, 19-year-old youth)

While many instances of password sharing were not risky, we found some concerning messages with password information shared. In the below example, a user shares their Apple ID account information to

try and have a youth participant help them locate their lost phone. Such account information is much more concerning to share, potentially allowing access to both a large amount of sensitive personal data as well as the ability to abuse the account financially or lock out its original owner. The youth's offer to aid in this exchange suggests they don't find anything odd about this. A willingness to share sensitive account information like this demonstrates that while many users are cautious about sharing sensitive information, some exchange information that should be kept to themselves.

O : *Can you u use find my iPhone for me*

...

P : *yeah sure*

P : *dont i need you email and password tho*

P : *bc i don't have your location on*

O : *YE I'll give u my Apple ID [NAME]*

O : *[USERNAME]*

O : *[PASSWORD]*

(Female, 18-year-old youth)

There were also numerous instances where youth **showed intent to share passwords (5%, n=69).** These cases featured youth offering to share account information in the future rather than doing so directly at the moment or requesting that information from others. The connotations of this intent to share are similar to cases where sharing occurs at the moment, with the risk of sharing varying depending on what exactly is being shared. An example below features users clearly having agreed upon sharing an account as admins, but not having shared the information yet because of a memory issue on one's behalf. This is a common manner under which these discussions take place, with one user asking for information and the youth participant offering to provide it in the future. Overall, similarly to directly sharing passwords, the risk of this behavior ranges with what is being shared, with this being a less risky instance:

O : *I also need information for the account because I can't really post without a passwordjdjd-djjdjssjsj or is that not how we're doing this?*

P : *Nah you're gonna be an admin*

P : *I forgot the password anyways*

P : *Sorry*

O : *Damn*

P : *Someone else should know it??*

P : *I hope*

(Female, 19-year-old youth)

In numerous cases, youth also discussed accounts they had already shared with others. In some cases, youth **shared their account with peers (5%, n=59).** In some instances, the account sharing with friends took place in the conversation we observed, while in others, they described their experiences of sharing accounts with friends elsewhere. The risk involved in this account-sharing heavily depends on the context of what accounts are being shared and what information is found in them. In the below instance, a youth describes an exchange of account information they have performed with a friend, having exchanged passwords to a given (unknown) account as part of a deal. This account-sharing practice could be risky depending on the context of what information these accounts include. It serves as an example of how willingly youth share accounts with each other at times, to the point of seeing it as something to leverage in the form of the deal:

P : *You need to tell me more things*

P : *[NAME] did that kinda exept shorter and I got some things wrong but then she kinda told me some answers and so I did it again and got it close enough and the deal was she'd give me her password so now I know her password*

O : *Nice job! Lol*

(Female, 16-year-old youth)

Beyond sharing accounts with peers, in some conversations, youth discussed how they **shared their account with family members (2%, n=31).** Relative to peers, account-sharing with family is a less risky practice because in many cases, it is for subscription-based services with shared use or accounts where parents may want to keep track of their children's spending. The below example is a case of such an account being shared between the youth and their mother on a commercial platform. The youth expressed that they could not access the account because their mother forgot the credentials, demonstrating needing their parents' consent for the use of such an account. This instance demonstrates a recurring trend throughout these conversations:

O : *I got a phone case*

O : *(smirk emote)*

O : *Wanna see it*

O : *Its pretty basic*

P : *Sure*

P : *I was going to order one but. I just remembered my mom forgot the password for amazon which is the reason why I didn't get the hoodie!!!!(smile emote)*

P : *(upside down face emote)*

(Female, 16-year-old youth)

4.2.2 Youth perpetrated security and privacy threats to others

Another form of risky behavior the youth engaged in was seeking to violate the security and privacy of others. Most frequently, they directly discussed their past and present efforts to hack and scam other individuals or businesses. In other cases, they bring up their plans to perform malicious actions in the future, or directly attempt to compromise the Instagram conversation they are in. Each of these trends demonstrates that while youth can be victims of security and privacy violations, they can also be the perpetrators putting others at risk without considering the consequences.

Most frequently, youth's malicious behavior manifested as cases where they discuss having **attempted to hack or scam others (5%, n=62)**. In many cases, the targets of such attempts were specific individuals, usually ones the youth know firsthand. For instance, in the example below, a youth acknowledges hacking the phone of somebody they are jealous of, and their peer laughs about it. The fact that the youth's peer expresses approval also plays a part in a concerning trend. Rarely do youth face backlash from peers when talking about attacks, often getting responses of approval and amusement. This suggests that some youth do not take these security and privacy violations seriously or mind their friends' involvement in such violations, which can contribute to creating social norms among peers that security and privacy violations are perceived as fun and non-serious:

P : *Can I have a spam account with someone.!?!?*

P : *[NAME] Making me jealous (crying emote x4)*

P : *Oh ya... I hacked onto her phone*

O : *Haha*

(Female, 16-year-old youth)

While attacks toward individuals were the most common connotation when youth discussed violating the security and privacy of others, there was another recurring instance. Youth regularly described their acquisition of pirated software as being "hacked," such as in the below example. Here, the youth makes it clear that they pirated software, and their peer chimes in desiring them to get the software for them as well. While this is a form of violating a company's security by illegally reproducing its products, it could be seen as lower-risk as there is less direct negative impact on youth's privacy and security compared to scams and hacks. Nonetheless, piracy can bring further risks to youth, as pirated downloads can potentially be a front for malware:

P : *Get Sony Vegas pro 14*

O : *What is that?*

P : *The video editing software I use*

P : *Its what you need if you wanna go pro*

O : *That thing is expensiveeee omggg*

P : *Nah I hacked it and got it for free lol*

O : *When i get my computer your hacking it for me okay?*

P : *Bet*

(Male, 20-year-old youth)

Beyond discussing security and privacy threats they have already taken part in, youth also **showed intent to scam or hack others (3%, n=43)**. In these instances, youth openly discuss their plans for malicious actions against others. Similar to the actions already taken, these cases generally were attacks against other people but occasionally were planned for piracy. The below example is a case of the former, with a youth planning to break into somebody's phone through knowing their password to delete a photo they regret sending. This action is encouraged by their peer, with a suggestion to hack the target before the youth even suggests their own plan. This once again confirms a concerning trend in which youth target others with security and privacy threats and are met with approval from peers:

P : *and nice to everyone but i sent [NAME] a pic one time i absolutely regret it wasn't nudes but liie still and he has it so i'm shaking*

O : *Brooo hack into his phone and delete*

O : *Was ur face in it?*

P : *noooo thank god*

P : *ik his password i can just steal his phone. but if only we had school*

(Female, 15-year-old youth)

The final form of malicious action youth took toward others was **spamming and/or scamming in group chats (2%, n=30), without their suspicious messages being acknowledged by others.** In many cases, it was difficult to know whether spam/scam messages were shared by the youth themselves or their hacked accounts as there was no formal resolution to the suspicious messages. Most commonly shared suspicious messages were dedicated to advertising a product or service, often with a link attached, and sometimes sent in succession. The example below is a clear instance of suspicious spam, not commented on or acknowledged meaningfully by those in the conversation. The example also shows that not all suspicious messages in private conversations are ultimately caught:

P : *[LINK]*

P : *All u have to do is click the link and it will*

give me $10 so pls do! This is not a scam thing either

P : *Subscribe to her channel! Just made a new video btw! [LINK]*

P : *Subscribe to her channel! My bestie just made a new video and I'm tryna promote it for her!*

[LINK]

P : *[LINK]*

O1 : *Hello (wave emote) I'm so excited right now*

O2 : *Hello*

(Female, 18-year-old youth)

CHAPTER 5

Discussion

In this section, we discuss the trends in youth privacy and security practices and awareness. Then, we reflect on the positives and negatives of online peer support for youth when discussing privacy and security topics. Based on our discussion, we provide implications for design and education.

5.1 Youth Privacy & Security Practices and Awareness

We found a variety of positive privacy and security practices in youth private online conversations. One of the major trends we observed was that youth were able to recognize potential threats to their security and privacy before they could harm them, as well as recognize instances where their security and/or privacy was breached. In numerous cases of the latter, youth also expressed their initiative to work and recover from the issue after it had occurred. The youth demonstrated several strong practices for ensuring their security and privacy on their own, such as keeping personal information by using false names on accounts or making use of strong password practices. We also observed that youth are familiar with not only data breaches on social media sites for third-party use but also digital surveillance at a social level. This reflects earlier findings that suggest that digital privacy is a concept youth take seriously, and they demonstrate knowledge about a variety of potential threats [31, 30, 12].

Another major trend we observed was youth sharing of online accounts within their close circle. The amount of account and password sharing among youth also reflects prior research suggesting youth are relatively willing to share personal information and credentials online with those they trust [16]. Our findings confirm this trend and show that youth use private online chat as a channel to share credentials of shared accounts. In addition, we showed the nuances of what youth perceive as acceptable privacy and security practices within those shared accounts. We observed that youth sometimes expressed their perception of privacy and security as personal boundaries in their shared accounts. Privacy boundaries are dynamic/turbulent [37] and navigating their boundaries through learning about others' boundaries in private online chat can be a healthy practice for youth. Our findings empirically demonstrated the youth's navigation and negotiation of such boundaries through private online interactions, which they may not share otherwise. At the same time, they are still forming their sense of what behavior is and is not risky, and further guidance is needed to help overcome some remaining risky practices.

Finally, in numerous instances, we saw a discrepancy between the privacy perception and behaviors among youth in which they shared insecure password practices, while they recognized they knew the pass-

words were unsafe. It suggests that even when youth know proper security and privacy practices, they don't always follow them. This so-called "privacy paradox" is not unique to youth as adults face many similar privacy challenges online [35, 38]. Yet, there are online dangers teens can face because of their over-willingness to share personal information via social media [11]. As social norms can make positive impacts on youth development [46], leveraging social interventions (e.g., social media nudges with social comparison with peers' privacy behavior) can be effective in reducing the gap between privacy and security concerns and behavior [22]. We call for further research to design interventions to reduce the discrepancy and encourage positive privacy practices for youth.

5.2 Tech Caregiving vs. Risk Taking through Online Peer Support

Overall, our findings show that online peer support is beneficial for youth to manage privacy and security risks. The fact that youth opt to discuss security and privacy topics with their peers is a positive trait, as it demonstrates their consideration for the subject being great enough to warrant discussing it. Their willingness to seek out advice from others confirms existing research performed with adults surrounding advice seeking for security and privacy, suggesting that similar logic applies to youth [17, 18, 33, 2]. In many instances, youth also sought and provided advice to one another through warnings about potential threats, discussions of resolving technical issues, and advice for recovery from threats. Each of these trends demonstrates the strengths of youth in ensuring their privacy and security and the potential to leverage online peer support to promote positive online privacy and security practices for youth.

Just as youth demonstrated many strong security and privacy practices, they also engaged in numerous risky behaviors in their online conversations such as exchanging passwords of shared accounts. It is worth noting that despite the amount of account sharing that took place in their conversations, not all of these instances are inherently risky. Many of the instances of account sharing with family and sharing impersonal accounts can be beneficial for them. However, cases of sharing more sensitive passwords and leaving digital traces of such information are concerning. Privacy and security breaches on social media are evolving, a recent report documented 26 billion data breaches through popular social media among youth such as Twitter [36]. Private online chat such as Instagram DMs is not an exception [49]. Further studies to gain a deeper understanding of the level of risk involved in youth password and account sharing and design interventions to raise awareness of the potential risks of such practices are needed.

Additionally, we found a concerning trend of youth involvement in security and privacy threats against others in which they found amusement in their actions. The notion of youth involvement in security and privacy attacks against others is also one that has been observed in prior literature [27, 9]. These malicious actions are concerning, especially considering the youth's lack of apparent remorse about the subject [25].

Therefore, educational content is needed to raise awareness of negative consequences to themselves and others to discourage such behavior. A more concerning trend we found was that, when youth shared their attempts to attack others, they hardly faced any meaningful backlash from their peers. This suggests that youth may be encouraged with such actions by social approvals from online peers. The norms and/or culture of peer approval on youth's sharing their attempts are more serious as developmentally, youth are sensitive to social pressure and approval from peers. Prior research suggests that although adolescents are able to understand and reason about some risks, they exhibit greater sensitivity to peer social rewards in risk-taking scenarios [43]. Therefore, strong social norms and guidelines around how risky such privacy and security attacks are and how they are not welcomed need to be set to demote risky behaviors.

5.3 Implications for Design and Education

Our results confirmed both positive and concerning trends in youth's discussion of privacy and security matters through private online chat. In this section, we provide implications for design and education to promote online privacy and security of youth while maximizing benefits and minimizing the negatives of online peer interaction regarding privacy and security topics.

5.3.1 Design implications

In order to address the gaps in youth security and privacy practices, we suggest the following design steps to provide outlets for stronger youth security and privacy practices:

- **Implementation of a Forum for Youth Privacy and Security** In order to fully leverage the strengths of peer-to-peer youth support, a dedicated help forum for discussing security and privacy practices could prove useful, and be tested at a smaller scale to see if youth would actively find use from it.
- **Automated Spam Recognition** While in many cases, youth were able to recognize instances of suspicious messages, there were several times when messages would be spammed and not so much as commented on. Implementation of automated spam recognition to detect and provide warnings in conversations such as these could prove beneficial on social media sites.
- **Warnings for Clicking Links** Many of the potential forms of hacking or scamming on social media involve tricking others into clicking on malicious hyperlinks. While some social media forums provide warnings on the dangers of clicking on external links whenever one attempts to do so before following through, this is not universal and could be a beneficial addition to more social media sites.
- **Incentives for Spreading Awareness of Risks** One potential method of increasing awareness of security and privacy risks among youth would be providing some formal incentive attached to spreading

resources. One notion youth seem to value on social media is attention. If social media sites could allegorically favor accounts that share specific security and privacy-related resources, it could potentially lead to more interest in sharing such resources.

5.3.2 Implications for Education

Beyond design implications, below we suggest opportunities for educative resources to further address forms of risky behavior youth engaged in:

- **Raising Awareness of Embedded Software Risks** A recurring practice youth discussed is piracy of internet software, which can prove dangerous due to the untrustworthy nature of distributors of such software. While educational resources can be found online about the subject, they are relatively out of the way, and the topic could potentially receive greater attention as one to educate youth about beyond topics such as password practices and credential sharing.

- **Discussion of Negative Consequences of Privacy and Security Attacks** In a similar vein, while the focus is dedicated to protecting youth online, fewer resources discourage outright malicious behavior. Similar to the way topics such as cyberbullying are covered, youth could benefit from greater discouragement from involvement in security and privacy threats.

- **Education from Parents without Restriction** Existing research has demonstrated the limitations of relying on parental restriction to protect youth from security and privacy risks rather than education. Further strides could be made to encourage parents to focus more on educating youth about ideal security and privacy practices while discouraging excessive restriction. Resources could be distributed online, or articles written seeking to get parents' attention.

- **Education about Security and Privacy in Schools** While educative tools for students under 18 do exist, the integration of programs educating youth about online security and privacy does not reach the heights of those at a university level. The inclusion of further education for younger audiences through individual-day events and presentations could aid in improving familiarity with positive security and privacy practices.

5.4 Limitation

While our research demonstrates a variety of youth security and privacy practices, there are some considerations worth acknowledging. The original IGDD dataset consists of private conversations donated by English-speaking US youth [41], thus only demonstrating the practices of a specific demographic, rather than all

youth on Instagram. Furthermore, the perspectives and experiences youth share on Instagram do not necessarily demonstrate the full scope of their experiences. Youth may choose not to share certain risky behaviors, for example, or otherwise not be interested in describing the full scope of their security and privacy experiences. Furthermore, sub-conversations do not always carry the full context of the interaction, as at times messages were deleted, or the conversation context attached to certain messages was ambiguous. Even with the limitations stated above, Instagram conversations did provide a unique look into the lives of youth and their security and privacy practices.

CHAPTER 6

Conclusion

In our qualitative analysis of youth Instagram messages, we observed a variety of positive and negative practices regarding youth online privacy and security. We found a strong trend of youth recognizing both the potential for digital threats and cases where they have been victimized by them. As a result, youth demonstrated protective practices in response to security threats and provided advice to others. Yet, concerning trends included youth demonstrating numerous insecure password practices, indicating gaps between their concerns and actual behaviors. Youth regularly participated in account and credential sharing, but the safety of this sharing varied depending on the accounts in question. In other cases, the youth shared experiences of or plans to attack others, which were often approved by online peers. Our analysis presents a nuanced perspective on youth security and privacy, demonstrating both secure practices and perspectives, as well as risky ones. The perspective of youth we provide and the design and education suggestions we propose can pave the way for further improvements to youth security and privacy in the future.

References

[1] Denise E Agosto and June Abbas. "don't be dumb—that's the rule i try to live by": A closer look at older teens' online privacy and safety attitudes. *New Media & Society*, 19(3):347–365, 2017.

[2] Mamtaj Akter, Leena Alghamdi, Dylan Gillespie, Nazmus Sakib Miazi, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. Co-ops: A mobile app for community oversight of privacy and security. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing*, CSCW'22 Companion, page 179–183, New York, NY, USA, 2022. Association for Computing Machinery.

[3] Mamtaj Akter, Leena Alghamdi, Jess Kropczynski, Heather Richter Lipford, and Pamela J. Wisniewski. It takes a village: A case for including extended family members in the joint oversight of family-based privacy and security for mobile smartphones. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, 2023. Association for Computing Machinery.

[4] Mamtaj Akter, Amy J. Godfrey, Jess Kropczynski, Heather R. Lipford, and Pamela J. Wisniewski. From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals? *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW1), apr 2022.

[5] Mamtaj Akter, Madiha Tabassum, Nazmus Sakib Miazi, Leena Alghamdi, Jess Kropczynski, Pamela J. Wisniewski, and Heather Lipford. Evaluating the impact of community oversight for managing mobile privacy and security. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 437–456, Anaheim, CA, August 2023. USENIX Association.

[6] Mario Álvarez-Jiménez, JF Gleeson, S Rice, Cesar Gonzalez-Blanch, and Sarah Bendall. Online peer-to-peer support in youth mental health: seizing the opportunity. *Epidemiology and psychiatric sciences*, 25(2):123–126, 2016.

[7] J Craig Andrews, Kristen L Walker, Richard G Netemeyer, and Jeremy Kees. Helping youth navigate privacy protection: Developing and testing the children's online privacy scale. *Journal of Public Policy & Marketing*, page 07439156231165250, 2023.

[8] Ovidiu-Gabriel Baciu-Ureche, Carlie Sleeman, William C Moody, and Suzanne J Matthews. The adventures of scriptkitty: Using the raspberry pi to teach adolescents about internet safety. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, pages 118–123, 2019.

[9] Sinchul Back, Jennifer LaPrade, Lana Shehadeh, and Minju Kim. Youth hackers and adult hackers in south korea: an application of cybercriminal profiling. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 410–413. IEEE, 2019.

[10] Karla Badillo-Urquiola, Zainab Agha, Mamtaj Akter, and Pamela Wisniewski. Towards assets-based approaches for adolescent online safety. In *Badillo-Urquiola, Agha, Z., Akter, K., Wisniewski, P.,(2020)"Towards Assets-Based Approaches for Adolescent Online Safety" Extended Abstract presented at the ACM Conference on Computer-Supported Cooperative Work Workshop on Operationalizing an Assets-Based Design of Technology,(CSCW 2020)*, 2020.

[11] Susan B Barnes. A privacy paradox: Social networking in the united states. *First Monday*, 2006.

[12] Danah Boyd and Alice E Marwick. Social privacy in networked publics: Teens' attitudes, practices, and strategies. In *A decade in internet time: Symposium on the dynamics of the internet and society*, 2011.

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

[14] Ankur Chattopadhyay, David Christian, Aaron Oeder, and Ibrahim Budul. A novel visual-privacy themed experiential-learning tool for human-privacy & societal-security awareness in middle-school and high-school youth. In *2019 IEEE Frontiers in Education Conference (FIE)*, pages 1–9. IEEE, 2019.

[15] Ankur Chattopadhyay, David Christian, Adam Ulman, and Caleb Sawyer. A middle-school case study: Piloting a novel visual privacy themed module for teaching societal and human security topics using social media apps. In *2018 IEEE Frontiers in Education Conference (FIE)*, pages 1–8. IEEE, 2018.

[16] Emily Christofides, Amy Muise, and Serge Desmarais. Hey mom, what's on your facebook? comparing facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, 3(1):48–54, 2012.

[17] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 143–157, 2014.

[18] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 739–749, 2014.

[19] Diana Freed, Natalie N Bazarova, Sunny Consolvo, Eunice J Han, Patrick Gage Kelley, Kurt Thomas, and Dan Cosley. Understanding digital-safety experiences of youth in the us. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2023.

[20] Arup Kumar Ghosh, Charles E Hughes, and Pamela J Wisniewski. Circle of trust: a new approach to mobile online safety for families. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[21] Arup Kumar Ghosh and Pamela Wisniewski. Understanding User Reviews of Adolescent Mobile Safety Apps: A Thematic Analysis. In *Proceedings of the 19th International Conference on Supporting Group Work*, GROUP '16, pages 417–420, New York, NY, USA, November 2016. Association for Computing Machinery.

[22] Isha Ghosh. *Social Interventions to Reduce the Privacy Paradox*. PhD thesis, Rutgers The State University of New Jersey, School of Graduate Studies, 2020.

[23] Heidi Hartikainen, Afsaneh Razi, and Pamela Wisniewski. Safe sexting: The advice and support adolescents receive from peers regarding online sexual risks. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–31, 2021.

[24] Paul Hodkinson. Bedrooms and beyond: Youth, identity and privacy on social network sites. *New Media Society*, 19(2):272–288, 2017.

[25] Qing Hu, Chenghong Zhang, and Zhengchuan Xu. Moral beliefs, self-control, and sports: effective antidotes to the youth computer hacking epidemic. In *2012 45th Hawaii International Conference on System Sciences*, pages 3061–3070. IEEE, 2012.

[26] Snježana Stanarević Katavić, Hajdi Ivanović, and Anita Papić. Digital privacy and data protection knowledge and skills of university students in croatia: Preliminary findings. *Education for Information*, (Preprint):1–23, 2023.

[27] Jihoon Kim, Lindsay Leban, and Yeungjeom Lee. Theoretical explanations of the development of youth hacking. *Crime & Delinquency*, page 00111287221115639, 2022.

[28] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J Godfrey, Heather Lipford, and Pamela J Wisniewski. Examining collaborative support for privacy and security in the broader context of tech caregiving. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–23, 2021.

[29] Priya C Kumar, Fiona O'Connell, Lucy Li, Virginia L Byrne, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. Understanding research related to designing for children's privacy and security: A document analysis. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference*, pages 335–354, 2023.

[30] Amanda Lenhart, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr, and Lee Rainie. Teens, kindness and cruelty on social network sites: How american teens navigate the new world of" digital citizenship". *Pew Internet & American Life Project*, 2011.

[31] Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaton. Teens, social media, and privacy. *Pew Research Center*, 21(1055):2–86, 2013.

[32] Alice Marwick, Claire Fontaine, and Danah Boyd. "nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-ses youth. *Social Media+ Society*, 3(2):2056305117710455, 2017.

[33] Tamir Mendel and Eran Toch. Susceptibility to social influence of privacy behaviors: Peer versus authoritative sources. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 581–593, 2017.

[34] Israel Márquez, Debora Lanzeni, and Maria José Masanet. Teenagers as curators: digitally mediated curation of the self on instagram. *Journal of Youth Studies*, 26(7):907–924, 2023.

[35] Patricia A Norberg, Daniel R Horne, and David A Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41(1):100–126, 2007.

[36] Vilius Petkauskas. Mother of all breaches reveals 26 billion records: what we know so far, 2024.

[37] Sandra Petronio and Jeffrey T Child. Conceptualization and operationalization: Utility of communication privacy management theory. *Current opinion in psychology*, 31:76–82, 2020.

[38] Chanda Phelan, Cliff Lampe, and Paul Resnick. It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pages 5240–5251, 2016.

[39] Farzana Quayyum, Daniela S Cruzes, and Letizia Jaccheri. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30:100343, 2021.

[40] Karen Raphael. Recall bias: a proposal for assessment and control. *International journal of epidemiology*, 16(2):167–170, 1987.

[41] Afsaneh Razi, Ashwaq AlSoubai, Seunghyun Kim, Nurun Naher, Shiza Ali, Gianluca Stringhini, Munmun De Choudhury, and Pamela J Wisniewski. Instagram data donation: A case study on collecting ecologically valid social media data for the purpose of adolescent online risk detection. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–9, 2022.

[42] Wonsun Shin and Hyunjin Kang. Adolescents' privacy concerns and information disclosure online: The role of parents and the internet. *Computers in Human Behavior*, 54:114–123, 2016.

[43] Ashley R Smith, Jason Chein, and Laurence Steinberg. Peers increase adolescent risk taking even when the probabilities of negative outcomes are known. *Developmental psychology*, 50(5):1564, 2014.

[44] Valerie Steeves and Cheryl Webster. Closing the barn door: The effect of parental supervision on canadian children's online privacy. *Bulletin of Science, Technology & Society*, 28(1):4–19, 2008.

[45] Mega Subramaniam, Natalie Pang, Shandra Morehouse, and S Nisa Asgarali-Hoffman. Examining vulnerability in youth digital information practices scholarship: What are we missing or exhausting? *Children and Youth Services Review*, 116:105241, 2020.

[46] Eva H Telzer, Jorien Van Hoorn, Christina R Rogers, and Kathy T Do. Social influence on positive youth development: A developmental neuroscience perspective. *Advances in child development and behavior*, 54:215–258, 2018.

[47] Mary Theofanos, Yee-Yin Choong, and Olivia Murphy. 'passwords keep me safe'–understanding what children think about passwords. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 19–35, 2021.

[48] Emily C Weinstein, Robert L Selman, Sara Thomas, Jung-Eun Kim, Allison E White, and Karthik Dinakar. How to cope with digital stress: The recommendations adolescents offer their peers online. *Journal of Adolescent Research*, 31(4):415–441, 2016.

[49] Davey Winder. 235 million instagram, tiktok and youtube user profiles exposed in massive data leak, 2020.

[50] Pamela Wisniewski. The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience? *IEEE Security & Privacy*, 16(2):86–90, 2018.

[51] Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. Engaging children about online privacy through storytelling in an interactive comic. In *Electronic Visualisation and the Arts (EVA 2017)*. BCS Learning & Development, 2017.