"Stalking is immoral but not illegal": Understanding Security, Cyber Crimes and Threats in Pakistan

Afaq Ashraf and - Taha, *Lahore University of Management Sciences;*
Nida ul Habib Bajwa and Cornelius J. König, *Universität des Saarlandes;*
Mobin Javed and Maryam Mustafa, *Lahore University of Management Sciences*

https://www.usenix.org/conference/soups2023/presentation/ashraf

This paper is included in the Proceedings of the
Nineteenth Symposium on Usable Privacy and Security.

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

“Stalking is immoral but not illegal": Understanding Security, Cyber Crimes and Threats in Pakistan

Afaq Ashraf
Lahore University of Management Sciences

- Taha
Lahore University of Management Sciences

Nida ul Habib Bajwa
Universität des Saarlandes

Cornelius J. König
Universität des Saarlandes

Mobin Javed
Lahore University of Management Sciences

Maryam Mustafa
Lahore University of Management Sciences

Abstract

We explore the experiences, understandings and perceptions of cyber-threats and crimes amongst young adults in Pakistan, focusing on their mechanisms for protecting themselves, for reporting cyber threats and for managing their digital identities. Relying on data from a qualitative study with 34 participants in combination with a repertory grid analysis with 18 participants, we map users mental models and constructs of cyber crimes and threats, their understanding of digital vulnerabilities, their own personal boundaries and their moral compasses on what constitutes an invasion of privacy of other users in a country where there is little legal legislation governing cyberspace and cyber crimes. Our findings highlight the importance of platform adaptation to accommodate the unique context of countries with limited legal mandates and reporting outlets, the ways in which digital vulnerabilities impact diverse populations, and how security and privacy design can be more inclusive.

1 Introduction

We unpack the experiences, perceptions of cybercrimes and mechanisms for self-protection of young adults in Pakistan, focusing on their social media usage. The pandemic has accelerated the growth of the internet and resulted in a significant increase in internet traffic [14, 23]. This shift has enabled the migration of various activities such as shopping, education, work, and entertainment to online platforms. However, with the rise in internet usage, the number of reported cybercrime incidents has also increased, as noted by the FBI and Interpol in the United Kingdom and the United States [1, 4]. The FBI reported that the number of cybercrime complaints received between January and May 2020 was nearly equivalent to the total number of complaints received in the entire year of 2019 [49]. Similarly, according to the Pakistan Telecommunication Authority (PTA), the number of cybercrime complaints received by the authority has been increasing in recent years. In 2020, the PTA received over 17,000 complaints related to cybercrime, an increase of around 40% compared to the previous year [6]. Despite the increasing number of cybercrime complaints, the conviction rate for cybercriminals in Pakistan remains low [6]. This is due to a number of factors, including a lack of technical expertise among law enforcement agencies, a weak legal framework for combating cybercrime, and a lack of awareness among the general public about how to protect themselves from cybercrime.

Among internet users in Pakistan, young adults constitute a large percentage of the demographic. In 2016, 19% of all internet usage in Pakistan was attributed to individuals aged 15-24 years old [2]. This demographic is considered tech-literate, digitally savvy, and early adopters of online platforms, primarily using social media platforms like Twitter, Instagram, Tiktok and Snapchat. The Digital Rights Foundation, a non-profit operating in Pakistan, reports that approximately 69% of the calls they received reporting cybercrimes were made by individuals within the age range of 18 to 30, with 78% of those calls being made by women, indicating that younger women are disproportionately affected by cybercrimes. There are, however, few studies that explore the relationships young, tech-savvy users in contexts like Pakistan, which have limited legal frameworks governing online spaces and few mechanisms for redressal, have with privacy and security online. Pakistan is a religious, patriarchal cultural context with a strong emphasis on honor and social status, resulting in often extreme consequences of online privacy breaches and harms. This is particularly true for women, as evidenced by high-profile cases such as the honor killing of Qandeel Baloch in Pakistan [27] and the suicide of Vinupriya in India [48]. It is important to unpack *what* a cybercrime constitutes in such a

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

context. What constitutes experienced *harm* for young people and where do platforms fail to account for diverse and complex contexts with varying factors at play, such as patriarchal structures of control and religious connotations?

We gathered qualitative data from 34 interviews and utilized the repertory grid technique (RGT) to collect data from 18 interviews with literate young men and women aged 18 to 23. Our study does not specifically aim to target individuals who have experienced cybercrime. Instead, we focus on literate users at the undergraduate level who have adopted devices and started going online at an early age (some as early as 5 years old). We find their use predominantly centers around social media platforms and much of their experiences and harms are associated with these platforms. Our work makes three key contributions:

1. We unpack what constitutes a cybercrime in this context, laying out the conditions under which online behavior is considered a harm and a crime from the perspective of young people. We also visualize the experienced severity of cybercrime through a gender disaggregated spectrum.
2. We highlight the strategies and behaviors that young users employ to protect themselves on social media platforms and their source of learning for these behaviors.
3. We explore design implications to improve knowledge of privacy mechanisms and increase control over online data sharing among social media users.

2 Related work

The present study expands the existing literature on privacy perceptions by specifically focusing on the perception of *cybercrime* in Pakistan. An understanding of *what* constitutes a cybercrime is complex, and its definition varies depending on the context, user mental models, and perceptions. Prior work in privacy has explored user perceptions and experiences of cybercrimes but often in developed contexts and often with adult populations [35, 51, 53]. Our work aims to fill this gap in knowledge by investigating the perceptions of cybercrime among young adults in the complicated context of Pakistan.

2.1 Privacy Perceptions Across Cultures

Privacy perceptions are influenced by factors such as social norms, individual characteristics, and community dynamics [36]. As a result, individuals in the Global North and Global South have different privacy expectations, beliefs, and behaviours [39]. One study across eight countries reports that Japanese and German participants have higher privacy concerns on their smartphones than those from Australia, Canada, Italy, Netherlands, the UK, and the USA, even though German users rated the sensitivity of their data as lower than that of Italian and Japanese [28]. Phone locks and pins are often used to safeguard data [12, 28, 29]. In contrast, prior work reveals that in South Africa, users are more worried about *who* is viewing their data rather than the data itself or its collection by platforms. These users are unaware of finer privacy features on social media platforms and rely heavily on blocking as the main privacy mechanism [43]. Similarly, Bellman et al. conduct a survey with 534 responses to understand the differences in privacy concerns amongst users across 38 countries. They highlight the importance of cultural values, internet experiences, and desires of political institutes as key factors impacting privacy concerns [11]. Similarly, other work exploring privacy practices of women in Pakistan, India, and Bangladesh reveal five key practices for safeguarding data, including phone locks, app locks, aggregate and entity deletion, private modes, and avoidance [47].

In Pakistan, religion plays a powerful role in shaping privacy attitudes and behaviors where women often negotiate the creation of gendered spaces online as a way of protecting their information from unfamiliar individuals, as prescribed by Islamic teachings [39]. Similarly, Arabic social media users frequently establish private online accounts to uphold *ird*, an Arabic term referring to personal or familial honor, in line with social norms [7]. Muslim women in the USA also reveal how social surveillance, which refers to performing actions out of social obligations within the community, impacted their activities online [8]. Prior work also reveals low-income, low-literate women in Pakistan, India, and Bangladesh associate privacy with *Western values* [47] or with shame [39], often believing privacy is only for people who have done something that they want to hide.

2.2 Cybercrime Experiences and Perceptions

Perceptions of cybercrime vary between the Global North and Global South, with factors such as socioeconomic status, gender, customs, and religion influencing their formation.

An increase in the use of digital spaces and platforms has resulted in a subsequent increase in cybercrimes [15, 30, 37] with online shopping fraud, online banking fraud, cyberbullying like stalking and threatening, malware, and hacking the most prevalent forms of online crimes [42]. In Finland, the 5 most common forms of victimization experienced by people in the age group of 15-74 years old were malware, harassment like defamation and threat of violence, hacking, fraud, and sexual harassment. People with higher internet usage were more impacted by malware attacks [37]. The PEW Research Center conducted a survey in the USA which found that Americans have reported personally experiencing online harassment and view it as a significant issue [21]. Another study by the same research center revealed that 26% of women reported being stalked online, and 25% reported experiencing sexual harassment online [55]. In a survey conducted by Maple et al. with 353 participants, 324 reported experiencing online harassment, with women citing “fear of personal injury" as their top concern when engaging online, followed by concerns related to their reputation [34].

During the COVID-19 lockdown in the UK, incidents related to “frauds associated with online shopping and auctions, and the hacking of social media and email" saw the largest increases, being the two most common categories of cybercrime in the country [17]. Another study exploring experiences of influencers on TikTok, Facebook, Instagram, Twitter, and YouTube found that at least 95% of creators described facing some form of harassment at least once in their career [52]. The study revealed through a longitudinal study that hate and harassment have grown 4% over the last three years and now affect 48% of people globally. They found that young adults, LGBTQ+ individuals, and individuals who frequently use the internet are more at risk of privacy violations [51].

In contrast, few studies focus on unpacking privacy experiences and behaviours in the Global South. One such study exploring online privacy perceptions and practices in Ghana reveals a lack of understanding of how internet technologies operate with users relying heavily on passwords, and those who augment their security do so with a variety of ad-hoc practices learned through word of mouth [18]. Another study by Sambasivan et al. in India, Pakistan, and Bangladesh, found that a majority of the participants regularly faced online abuse, experiencing three major types: cyberstalking, impersonation, and personal content leakages [46]. Other work reveals Low Socioeconomic Arabs (LSA) experienced black hat hacking, identity theft, shoulder surfing, and defamation. High Socioeconomic Arabs (HSA) experience grey hat hacking, credit card theft, financial fraud, and identity theft. The consequences of the attacks were more severe for LSA like reputational harm while HSA reported little to no consequences from the attacks [45]. According to a 2021 Digital Rights Foundation report, the most commonly reported cyber harassment cases were blackmailing, non-consensual use of information, unsolicited contact, hacked account, financial fraud, fake profile, and defamation. Other threats like impersonation, bullying, hate speech, and cyberstalking were also reported [3].

2.3 Cybercrime among Young Adults

Young people are the most frequent users of the internet and technology, and as such, they are most likely to be exposed to cybercrimes than other demographic groups [13,56]. This is due to their new financial responsibilities, social independence, and frequent technology usage [13]. While few studies globally have focused on young people those that have report that students often receive messages that threatened, insulted, or harassed them or were pornographic in nature [24,40]. Prior work also reveals that amongst undergraduate and graduate female students, those who viewed social media as having a negative impact on their lives also reported experiencing more online harassment [54]. Another four-country (Finland, US, UK, Germany) study examining cybercrime victimization among teenagers and young adults, found that online crime victimization was relatively uncommon, with slander and the threat of violence being the most common forms of victimization, and sexual harassment the least common [38]. Crimes like malware, hacking, and phishing were more common among U.S. undergraduate students. The students reported gaining knowledge about cybercrime through prior victims and media sources [13].

Previous studies conducted on technology usage amongst adults in low-literate and low-income areas of Pakistan and other Southeast Asian nations have revealed disparities in technology utilization between men and women and variations in privacy perceptions based on cultural and religious values [39,46,47]. This study examines whether young adults with a higher level of education, technological literacy, and economic stability compared to their low-literate and low-income counterparts experience similar challenges with privacy and cybercrime. Furthermore, this study aims to explore the reasons behind these difficulties, if present, despite the higher level of technological literacy in this demographic. Additionally, this study seeks to complement existing literature on privacy and cybercrime, which primarily focuses on the female perspective, by examining the male perspective on these issues.

3 Methodology

This study explores the young adults’ mental models of cybercrime in Pakistan. Our main questions were:

- RQ1: What is considered a cybercrime from the perspective of young people, and how do they define the severity of online behavior as harmful or criminal? Are there gendered nuances in this categorization of an online behaviour as a crime or harmful?
- RQ 2: What strategies and behaviors do young users employ to protect themselves online and where do privacy affordances fail them?
- RQ 3: What are their mechanisms for reporting or seeking support in a context like Pakistan which has a limited legal framework for the digital world?

Our research consisted of Repertory Grid (RGT) interviews with 18 participants (13M, 5F) to address RQ 1 and semi-structured qualitative interviews with 34 participants (17M, 17F) to explore RQs 2 and 3. Both studies had unique participants.

3.1 Repertory Grid Study

The study employs the Repertory Grid Technique (RGT) to elicit personal constructs and to observe the perception of participants regarding cyber threats. Developed by George Kelley as part of his Personal Construct Theory, it posits that people construe reality according to their personal constructs [10], and they form these constructs by observing the contrasts between a set of examples [32]. The main components of RGT are *elements*, *constructs*, and *linking mechanisms* [50]. *Elements* represent objects of thought (people, places, ideas, or inanimate objects) that are compared methodically to discover the constructs of a person [22]. *Constructs* are the discriminations that people make between the elements. *Linking mechanisms* are the ways that show how participants interpret each element relative to each construct [50]. In our case, elements are cybercrime threats; constructs are characteristics that participants use to describe similarities and differences between cybercrime threats; and linking mechanisms are ratings of the threats made by the participants on each construct. Rating refers to the process of comparing or evaluating elements on each construct using a numerical or qualitative scale to capture individual perceptions and distinctions. A diagram explaining the methodology can be seen in Figure 1.

More precisely, we employed the Full RGT Method [44] where both the elements and the constructs were elicited from the participants. The participants were first asked about their personal experiences and the experiences of their close acquaintances with cybercrime to elicit the elements and finalize the cybercrime element list. After this element elicitation phase, the construct elicitation phase started where participants were presented with triads of elements organized in the triadic form [50] (see Table 3 in Appendix for triad order). Participants were instructed to compare and contrast any two most similar elements with the third one. To understand the underlying assumptions and reasoning behind the elicited constructs, the participants were further probed using “Why?” and “How?” questions (also called the Laddering Technique [26]) whenever needed. For instance, one of the presented triads during the study involved *hacking*, *unsolicited contact*, and *non-consensual use of information (NCUI)*. A participant mentioned that hacking and NCUI are similar, stating that they are more harmful compared to unsolicited contact. When inquired about the reason behind the choice, the participant explained that hacking and NCUI could potentially lead to the unauthorized access of personal pictures, which could then be used for blackmail. In contrast, unsolicited contact was seen as less directly harmful to the victim. The constructs were then recorded on a repertory grid (see Figure 4 in Appendix), and participants were asked to rate each element in relation to each (self-generated) construct using a five-point Likert scale (Linking Phase).

3.2 Qualitative Study Design

The study protocol consisted of 8 sections, which aimed to elicit information about the participants’ device and internet usage and their experiences and beliefs regarding cybercrime and reporting mechanisms. To validate the protocol, pilot interviews were conducted, and the protocol was revised based on the findings from these interviews. To address the linguistic diversity of the participants, the protocol was translated into both English and Urdu. The average length of the interviews was approximately 0.7 hours, ranging from 0.31 hours to 1.2 hours. Sampling continued until data saturation was achieved, at which point no new information was obtained. Interviews were conducted online through Zoom. The interviews were conducted in a mixture of English and Urdu languages.

3.3 Participant Recruitment

The participants were recruited using a snowball sampling technique through personal contacts and online forms posted on university forums. The participants were pursuing degrees in various majors including STEM, Business, and Humanities. The interviews were conducted both in person and online on Zoom.

For the RGT study, the sample consisted of undergraduate students enrolled in 8 universities in Pakistan. A pilot study was conducted with a sample of 5 participants using the Repertory Grid Technique (RGT) method to establish a definitive methodology for the final interviews. We continued to recruit participants until saturation was reached, i.e. when no new threats or experiences of privacy violations emerged. A total of 18 participants (5 females, 13 males) with ages ranging between 18-24 were recruited from 8 universities in Pakistan. The demographics of the participants are presented in Table 1.

The qualitative study sample consisted of undergraduate students enrolled in 12 universities in Pakistan. A total of 34 participants (17 females, 17 males) with ages ranging between 18-24, were recruited from 12 universities in Pakistan. The demographics of the participants are presented in Table 4 in Appendix.

Gender	Male	13
	Female	5
Age (years old)	18	1
	19	3
	20	2
	21	6
	22	2
	≥ 23	4
	Average, Median, Mode	20.94, 21, 21
Education Year-(Undergraduate)	Freshman	2
	Sophomore	4
	Junior	3
	Senior	9
University	Private	5
	Public	3

Table 1: RGT Demographics

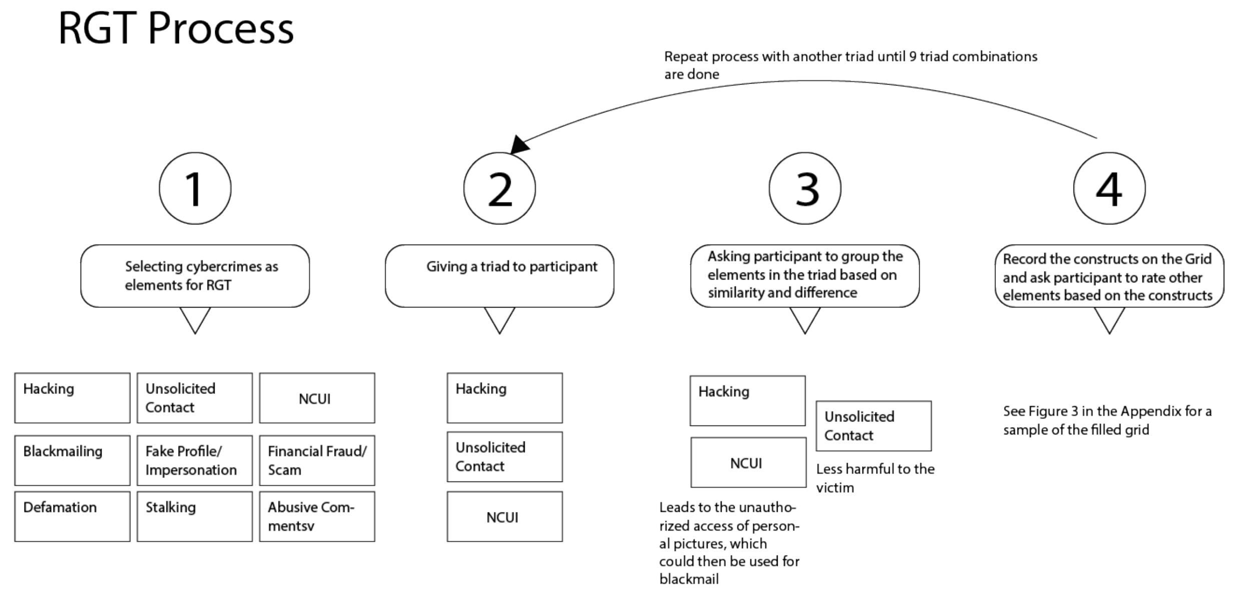

RGT Process
Repeat process with another triad until 9 triad combinations are done
1
2
3
4
Selecting cybercrimes as elements for RGT
Giving a triad to participant
Asking participant to group the elements in the triad based on similarity and difference
Record the constructs on the Grid and ask participant to rate other elements based on the constructs
Hacking
Unsolicited Contact
NCUI
Blackmailing
Fake Profile/ Impersonation
Financial Fraud/ Scam
Defamation
Stalking
Abusive Com- mentsv
Hacking
Unsolicited Contact
NCUI
Hacking
NCUI
Unsolicited Contact
Less harmful to the victim
Leads to the unautho- rized access of person- al pictures, which could then be used for blackmail
See Figure 3 in the Appendix for a sample of the filled grid

Figure 1: Methodology of the RGT process

3.4 Ethical Considerations

Both studies were approved by the IRB at the university where the study took place and informed verbal consent was obtained prior to conducting the research. The participants were informed that only audio recordings would be made and that the data would be used exclusively for research purposes. Additionally, it was communicated to the participants that the data would not be shared with any third parties and that any personally identifiable information would be removed during transcription to maintain anonymity.

At the time of the study, the minimum wage for unskilled workers and adolescent workers in Pakistan was PKR 120.2 (0.45 USD) per hour [5]. All participants were compensated for their time. The participants in RGT interviews were compensated PKR 500 (1.87 USD), while those participating in qualitative interviews were compensated PKR 1000 (3.74 USD). Participants were also informed that they could decline consent for recording without any impact on the compensation offered.

Given the sensitive nature of the subject matter and the cultural context of Pakistan, a female researcher was designated to conduct interviews with female participants, while male researchers were responsible for interviewing male participants.

3.5 Data Analysis

The recorded data was first transcribed. The data was then analysed using open-coding [31] which was conducted by a team of three researchers. To ensure consistency in the coding process, the first three interviews were collaboratively coded and an initial codebook was created. Subsequently, each researcher conducted individual coding, and recurring codes were consolidated during meetings. A total of 3,852 codes were generated from the transcripts, which were grouped into themes using Thematic Analysis, as described by Brown et al. [16]. The themes were further synthesized and organized using Affinity Mapping.

3.6 Positionality

The authors of this study are based in Pakistan and comprised of two female and two male researchers who were residing and working within the country during the time of the research. An additional 2 authors are based in Germany. Among the authors, two were considered to be young adults during the study, providing them with an advantage in their ability to relate to the experiences of the participants. This, in turn, facilitated an intuitive understanding of the social and religious context of the participants’ responses pertaining to cybercrime. Additionally, the female researchers of the study have previously lived in both the US and Europe, and have spent much of their formative years in Pakistan which allows for a unique understanding of the Paksitani context.

4 Findings

Our findings highlight the cybercrime experiences, digital safety perceptions, safety behaviours, and available support systems of educated, tech-savvy users in Pakistan. We discuss the differences in these experiences and behaviours as compared to earlier reported experiences of low-literate, low-income users [39,46] in Pakistan and broadly the experiences and behaviours of young people in the Global North [13,37].

We find, as reported in prior work, phishing, fake profiles and impersonation, financial fraud and cyber-stalking to be frequently experienced harms in our context [9,33,38]. However, we also find specific gendered nuances and differences in what is considered a harm, how harms are experienced, the effectiveness of existing privacy affordances and the barriers to reporting that have not been reported in prior work.

We structure our findings below by first presenting a cybercrime spectrum which is based on the RGT study data and the qualitative data both (Section. 4.1). The rest of the findings are based only on the data from the qualitative study.

4.1 Cybercrime Spectrum: RGT Data and Qualitative Analysis

We used data from our RGT study along with qualitative data to calculate a dis-aggregated spectrum of cyber threats from least severe to most severe (Figures 2, 3). In the Repertory Grid Technique (RGT) interviews, multiple constructs were elicited to indicate the severity of each threat, such as Emotional harm (vs. Physical harm), No direct harm (vs. Direct harm), and Potentially harmful (vs. Less harmful). Figure 4 displays a sample of a grid from our RGT study. During the categorization process, elements were assessed based on their proximity to poles indicating severity or benignity. If an element was ranked towards the pole that indicated severity (i.e. More Severity, Potentially Harmful, Exploitation of the Victim), it was considered a severe threat. A similar process was applied for the poles (i.e. Mildly Threatening, Less Harmful, The Victim is not Exploited) that implied benignity. Similarly, during the qualitative interviews, participants were asked which online threats they considered severe and benign. We measured the frequency of each threat they rated severe or benign by grouping the responses. The total frequency of each threat was calculated by summing the frequencies of benign and severe threats obtained from both the qualitative and RGT interviews. Finally, the final severity rating for each threat was determined by subtracting the total benign frequency from the total severity frequency. Threats with higher scores were considered more severe, while those with lower scores were categorized as benign.

We see notable differences between male and female spectrums. Male participants considered Hacking, Blackmailing, NCUI, and Financial Fraud to be more severe while female participants considered Defamation, Hacking, NCUI, and Fake Profile to be more severe. Male and Female Participants both considered Stalking, Abusive Comments, and Unsolicited Contact to be less severe. Female participants also considered Financial Fraud to be less severe, which is in contrast to the male spectrum. In the subsections below we unpack and contextualize the spectrum based on the experiences and concerns expressed by the participants along with the prevalent socio-cultural norms based on our qualitative study.

4.2 Cybercrime Experiences and Concerns

Threat	Total (%)	Males (%)	Females (%)
Unsolicited Contact	20	2.5	17.5
NCUI	17.5	0	17.5
Hacking	15	7.5	7.5
Fake Profile & Impersonation	15	2.5	12.5
Financial Fraud/ ScamCalls	15	7.5	7.5
Blackmailing	7.5	0	7.5
Defamation	7.5	0	7.5
Stalking	2.5	0	2.5

Table 2: Frequency of threats reported by male and female participants

Participants in our qualitative study reported 40 personal cybercrime experiences, and 35 experiences of other people (family, friends, media coverage). Table 2 displays the frequency of each reported threat experienced by participants. The types of cybercrimes experienced by the participants, along with their definitions, can be found in Table 5 in Appendix. The definitions were supplemented from the Digital Rights Foundation [25], which is a Pakistani research-based advocacy NGO focusing on technologies to support human rights, democratic processes, and digital governance.

In the following subsections, we discuss the cybercrime experiences of five cyberthreats: unsolicited contact, cyberstalking, fake profile/ impersonation, financial fraud/ scam calls and non-consensual use of information. We highlight the concerns, the platform level affordances and participants own mitigation strategies for each crime. For each we also detail the reality of participants experiences. The following sections are based on data from our qualitative study.

4.2.1 Unsolicited contact

Unsolicited contact was the most frequently reported cybercrime across all female participants.

Concerns: Male and female participants considered unsolicited contact benign (relatively harmless crime). Female participants reported being contacted on various platforms without their consent, revealing that the privacy affordances provided by social media platforms were ineffective against unsolicited contact. Female participants would persistently receive message requests and calls despite blocking the accounts on social media and the contact numbers multiple times.

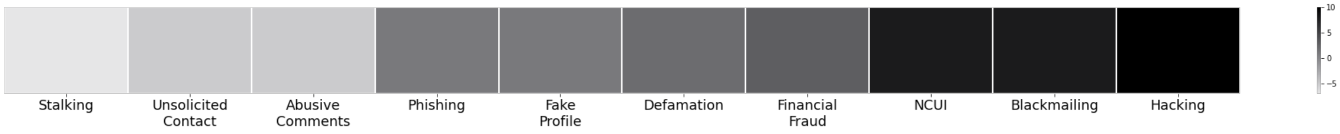


Figure 2: Male Spectrum about Cyberthreats

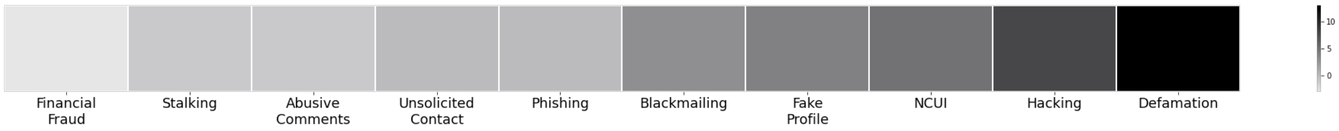


Figure 3: Female Spectrum about Cyberthreats

The perpetrators were always male, and their motive was to establish friendships with female users. One female participant highlighted: *"This [unsolicited contact] is such a common occurrence; I mean, people don't even call this [unsolicited contact] a cybercrime because it's that common. A random person texts you on Instagram and forces you to be friends; like, it's so common now that you don't even pay attention to it. You're just like this happens and stuff." - PIFT-F1.*

We found that users misuse the disappearing messages and one-time picture view feature of Snapchat to perpetrate unsolicited contact. Snapchat servers are designed to delete all Snaps (pictures) after all recipients have viewed them. Since the chats get deleted automatically, perpetrators send offensive content to users with the affirmation that the evidence of harassment will be erased permanently: *"Recently, in some harassment cases, we got to know that the harassers harass [others] on such platforms like Snapchat where all the chats are deleted... they don't want the chat to stay." - PF1.*

In another incident, one participant reported an instance of misuse of the Airdrop feature on an iPhone smartphone. The participant explained that their friend was traveling on a bus and forgot to turn off her Airdrop, which allowed a stranger to connect to her device and send unsolicited images.

Sambasivan et al.'s work in India, Pakistan, and Bangladesh highlights that 65% of the women in their sample reported friendship requests and unwanted phone calls from strangers as a common form of online abuse [46]. In contrast, unsolicited contact has not been reported as a frequent threat in the Global North [13, 15, 38]. Cultural norms around the segregation of genders and the importance placed on the modesty of women also impact the severity of some privacy violations as more traumatic in our context than others.

Affordances and Mitigation: Social media platforms, such as Instagram and Facebook, allow users to make their profiles private and block or report the abuser's profile. Participants take additional precautionary measures to ensure their privacy by not sharing their contact details with strangers and restricting the requesting profiles.

Reality: Despite platform level affordances, participants were unable to effectively navigate unwanted contact. Instagram's feature to allow users to create multiple accounts from a single profile was a contributing factor to the high prevalence of unsolicited contact on the platform. To address this issue, Instagram introduced a feature that allows users to block an account and any future accounts created using the same email address or contact number. This allows users to block contact with an individual's current account and any future accounts that the person may create in order to contact them again. However, participants found this feature to be ineffective in blocking unsolicited contact as users make new accounts with new email addresses: *"I even tried the option on Instagram to report all future accounts made by this person [the perpetrator], but maybe he made an account from a different email [that I kept receiving his messages]." - PU-F1.*

Participants also reported that the perpetrator often created a new account or phone number to contact them despite being blocked. This led to a sense of hopelessness among female participants, who had come to accept this type of cybercrime as a normal part of their online experience. On the other hand, unsolicited contact was not common among male participants, as evident from the Table 2, which may have contributed to their perception of it as benign. However, male participants were aware of its prevalence in society:*"The most frequent cyber-crimes you tend to hear about are messages to women, pictures of genitalia, or posts or texts mentioning lewd activities that they would like to do to the said women." - LM1.*

4.2.2 Cyberstalking

Our findings reveal that while both male and female participants found cyberstalking a benign threat, it was reported only by female participants.

Concerns: Cyberstalking was viewed as normal amongst our participants who did not consider it as *illegal* since social media platforms do not prevent users from accessing other users' profiles. Participants understood public profiles as fair game for abusive comments and stalking without fear of legal repercussions. They believed it was perfectly legal to interact with profiles (in any way) as long as they were public. The participants being stalked considered it to be less severe as they were not *aware* of the fact they were being stalked: *"I would say stalking is immoral but not illegal since you are putting the information out there in public yourself" - LM4.*

We found male participants were relatively less concerned about cyberstalking than female participants. They believed they could ward off the stalkers through their physical strength. However, male participants were more concerned with online tracking and stalking by social media companies. They expressed concern about the platforms themselves spying on their digital activities. They explained that they were worried about being shown ads for something they only verbally discussed with their friends: *"Cyberstalking is also quite a threat, but only if the companies conduct it; stalking happens through [online] platforms." - LM2.*

Female participants believed they could be stalked through their laptop cameras and were concerned about hacking of their cameras and capturing of their photos in compromising positions. They strongly believed that cyberstalking often leads to crimes in the real world which include physical stalking and harassment:*"They [stalkers] get their [female victims] address and phone number, and they get into more detail about how they get their address and phone numbers. And then they follow her, making her extremely uncomfortable." - GF3.*

Studies in the region have not previously reported cyberstalking [39,46] as most studies have worked with low-literate populations. In contrast, our participants were young and tech-savvy, with much more engagement with online spaces and platforms.

Affordances and Mitigation: Mobile applications ask users before accessing multimedia, contacts, and camera of the user's device. Whatsapp allows its users to limit access to their profile picture and statuses to specific contacts. In addition, our study participants reported taping their front-view laptop cameras in fear of stalking by hackers. They avoided posting personal content, such as pictures and contact details, to the public.

Reality: We found that default privacy settings of social media platforms can significantly impact users' experience and the potential for unwanted or harmful interactions. Participants perceived Instagram to be more secure as compared to Facebook because when creating an account on Instagram, the default profile picture settings are set to private, while on Facebook, users are required to enable it manually. However, participants mentioned third-party external websites that can be used to enlarge and view anyone's profile pictures on Instagram. Originally, Instagram restricts users from enlarging the profile picture of any other user. These third-party links are easily accessible through online search engines. As far as we know, Instagram has failed to address this issue.

4.2.3 Fake profile & Impersonation

Concerns: Perpetrators created fake profiles using false information to exploit contacts and tarnish reputations. They frequently posed as women to gain access to women's accounts and then sent victims inappropriate content, such as explicit images and texts. In certain instances, they utilized real details of other individuals to impersonate them online. The motivation behind these impersonations often involved defaming the real individuals or establishing trust by pretending to be someone close to them.

A female participant reported: *"There was this guy who liked me. I didn't wanna get involved with him, so he got angry and sent me a friend request [through a fake account]. I thought it was my friend's and I accepted his request. He stole all my pictures with screenshots. Then he created another account and uploaded those pictures with captions that were not very pleasant." - FJMUF1*

Participants expressed deep concerns about the potential damage to their reputation caused by fake profiles. They emphasized the harm associated with a counterfeit profile impersonating them and sharing inappropriate or questionable content, leading others to mistakenly hold them responsible for it.

Affordances and Mitigation: Social media platforms allow users to create unique usernames, protecting against profile impersonation. Each profile is linked to a separate email address and mobile number, strengthening security measures. Moreover, users can report impersonating profiles and request the platform delete the profile.

To further protect themselves from fake profiles our study participants reported that they checked the requesting profile's activity (when a friend request is made) to verify its authenticity. To prevent the misuse of their display pictures, female participants in our study frequently blurred them.

Reality: Our research uncovered a contrasting reality. Perpetrators in our study possessed multiple SIM cards registered under their names, enabling them to create numerous profiles on social media platforms such as Instagram. In Pakistan, individuals can register up to five SIM cards using a single ID card. Similarly, Instagram permits users to create up to five profiles linked to a single email address.

Participants' lack of trust in official reporting mechanisms and cybercrime agencies compelled them to take matters into their own hands. Female participants, for instance, formed online groups to collectively report and flag fake accounts engaged in harassment. This approach proved effective as submitting a large number of reports within a short time frame increased the chances of the social media platform suspending the offending account. Additionally, they employed call-out posts to publicly shame perpetrators, recognizing that male wrongdoers were concerned about their social image and damaging their reputation significantly. By publicly defaming the perpetrators on social media platforms, female participants effectively discouraged their harassing behavior and instilled fear among other men, deterring them from engaging in similar activities. : *"I just now put it in my friend's group and tell them to mass report it (the account), and their (perpetrator's) account gets disabled. You do name-shaming or call out a person (on social media). Tweet about them. Now people are scared to do such stuff because they know that if you tweeted about it and other people saw it, people are gonna suspend your account." - GCU-F2.*

4.2.4 Financial Fraud/ Scam Calls

Concerns: Scammers frequently targeted victims by assuming authoritative roles, such as bank employees or members of reputable community organizations. They utilized tactics like account-blocking threats or enticing cash rewards to obtain personal information. This information was then exploited for fraudulent transactions or to deceive victims into believing they had won lottery prizes, often requiring a small registration fee. However, our participants displayed a high level of awareness about prevalent scams in Pakistan and demonstrated the ability to recognize and avoid them easily.

Participants tended to blame the victims of scam calls and financial fraud, perceiving it as their own fault. Since the participants had never fallen victim to a scam, they only recounted scenarios they had observed. The victim in such scenarios was usually elderly, low-literate, and tech-illiterate: *"If a person is going to random sites and not verifying their authenticity, then it is their fault too. People should be careful themselves; you can't just blame the person committing the crime." - NUSTM1*

Affordances and Mitigation: Recent smartphone updates have introduced features that flag incoming calls from unknown numbers, aiding participants in our study in identifying potential scam calls. Through community-based reporting, if a phone number receives multiple spam reports, it can be labeled as a potential scam number, and new users will be notified accordingly. In addition, we observed that our participants employed various strategies to assess the authenticity of websites before engaging in transactions. For instance, they relied on indicators such as the site's popularity, product reviews, and visual aesthetics to establish a level of trust and convince themselves of the site's legitimacy.

Reality: No personal experiences of this cybercrime were reported, hence no vulnerabilities were identified.

4.2.5 Non-Consensual Use of Information

Concerns: NCUI (Non-consensual Use of Intimate Images) was exclusively reported by female participants in our study. Our findings established a clear connection between NCUI, fake profiles, and blackmail. Perpetrators gained unauthorized access to victims' personal data, which they then utilized to either blackmail the victims or create fraudulent profiles. *"There was some guy having my photos, he was basically blackmailing me into meeting him or else he'll get my photos and post them" - LCWU-F1*

The personal information was obtained either through the victims' social media accounts or, in one instance, through non-consensual dissemination by their friends. The perpetrators, predominantly males, would approach female participants under the pretext of initiating a relationship. *"She [the friend] gave my pictures to some person and then he texted me and is like I have your pictures, I know who you travel with in the school van; all you have to do is talk to me everyday. Otherwise, I will create a fake account using your pictures. GCU-F4*

Affordances and Mitigation: Snapchat's screenshot notification feature prevents the unauthorized use of personal photographs by alerting users when their snaps are captured. Our findings indicate that features providing more control over content visibility and lifespan enhance user experience and foster greater trust in the platform. Participants responded positively to Snapchat's timed snap feature, which allows users to set a viewing timer on their snaps, making them accessible for a specific period. This feature instills a sense of security, enabling users to share pictures without worrying about misuse, as recipients can only view them within a limited timeframe.

Reality: Despite some platform affordances, participants highlighted the ineffectiveness of Snapchat's screenshot notification feature when a user takes a screenshot by activating airplane mode on their mobile device, as it does not trigger a notification: *"If someone takes a screenshot [of the chat], you are notified, but even that has loopholes where people use it with airplane mode and stuff." - PIFT-M1*

Participants expressed concern about the limitations of the timed snap feature, as it was possible for users to capture and distribute the content using a different smartphone, discouraging them from sharing personal content through snaps. Similarly, on WhatsApp, blocking or deleting a contact does not delete the chat history between users, causing serious concerns among participants regarding potential chat leakage and the potential for their chats to be used against them: *"For instance, your conversation with someone comes to a close; even if you delete the stuff [chats], they will still have all the pictures downloaded in their phone. That is the only issue in Whatsapp." - LM2*

4.3 Barriers to Reporting Cybercrime

We found three major barriers when participants reported cybercrime to concerned authorities. These included the ineffectiveness of reporting platforms, lack of awareness regarding reporting mechanisms, and concerns about families.

4.3.1 Effectiveness of Reporting Platforms

Participants were skeptical of the effectiveness of social media platforms in resolving their reports of cybercrime. Additionally, they expressed a lack of trust in reporting such crimes to legal authorities. This contrasts with the experiences reported by US undergraduate students, as previously documented in the literature, where a greater level of comfort was reported in relation to reporting cybercrime to appropriate authorities [13].

The participants in our study revealed a lack of trust in the ability of legal agencies to effectively and efficiently resolve their reports of cybercrime. This sentiment was further reinforced by concerns about the potential for excessive information-gathering and the dissemination of sensitive personal information to third parties. Additionally, participants were concerned about legal agencies contacting their parents or gaining access to other personal information in the process of reporting cybercrimes. Overall, these concerns regarding privacy and the handling of sensitive personal information contributed to a reluctance to report cybercrime to legal agencies: *"If my email account is hacked, there is much more [information]. If that email account is connected to several other accounts, they [cybercrime agencies] will know which platforms and accounts I am using. They can access my data from those accounts." - LM2*.

Participants were also reluctant to report cybercrimes to social media platforms, citing the inefficiency of the platforms in taking timely action on complaints. They explained that the damage had already been inflicted on the victims by the time social media platforms took appropriate action toward the complaint. This is one of the reasons that people took matters into their hands: *"I have had my pictures used in contexts where I did not want them to be used. Someone started uploading my photos with crude captions wherein my response was to search online how to remove them through reporting systems on Instagram. And what I learnt from that was that by the time Instagram would sift through and decide it was worth removing, the damage would have been done. It would take less than twenty-four hours for me to become a laughingstock." - LM1*

In Pakistan, there is a general mistrust of government institutions, as individuals often encounter issues such as delayed or unresponsive responses, complex procedures, and uncooperative staff when interacting with these departments. This mistrust extends to Pakistan's Federal Investigation Agency (FIA) specifically when it comes to reporting cybercrime. Participants noted that the FIA does not provide statistics on the number of crimes resolved, making it difficult for them to assess the agency's efficiency. There is also little transparency about the process of lodging a complaint or what happens once a complaint has been made.

However, a few male participants told us that the agencies working against cybercrime in Pakistan were doing a satisfactory job. They explained that once a crime is reported to FIA, they resolve it effectively and promptly: *"Yes, FIA is doing a good job because once you complain to them, they take two days max to reply to you." - LM3*.

It is important to note that the participant only mentions the time taken to receive a reply from FIA. Resolving a complaint takes an even longer time. In contrast, female participants mentioned that FIA is not helpful in the majority of the cases. Most female participants did not report cybercrimes they faced to any legal agency, citing a lack of knowledge about whom to contact and how to report such crimes. One participant provided an example of a case of blackmail on Facebook involving another girl, in which her pictures were leaked, and she was being blackmailed for a large sum of money. She explains that the FIA was not helpful in resolving this crime.

Similarly, social media platforms do not take contextualized action against the reported cybercrimes. One participant reported that a fake account was made using her name on Facebook. The perpetrator blocked the participant from the fake profile. Despite consistent requests to Facebook and cybercrime agencies, the participant could not get the fake account deleted. Expressing concern over the non-consensual use of her pictures on a fake account, the participant mentioned: *"In what I experienced, the [fake] account was not disabled and it had about 500 people in the friend list. Using my pictures, I did not know whom they were talking to or what they were talking about. My concern is that somebody is using my identity, that is why I am very concerned about my pictures that they do not get leaked anywhere." - GCU-F4*. In contrast to formal pathways, participants often preferred utilizing their personal contacts in cybercrime agencies so their reports could be heard and appropriate action could be taken against the perpetrators. Similarly, perpetrators from influential families often use their political connections to intimidate the victim to not report cyber-crimes. Participants also expressed concern that if they report the cybercrime and the perpetrator finds out, they could make their life more difficult if they had such connections.

These concerns and the general lack of transparency in the procedures and mechanisms for how platforms and local agencies handle complaints leads to an absence and vacuum of support mechanisms for users in Pakistan.

4.3.2 Lack of Awareness Regarding Reporting Mechanisms

Along with distrust in cybercrime agencies, another important barrier when reporting cybercrime for our participants was the lack of awareness and education regarding reporting mechanisms. The participants were unaware of agencies working to curb cybercrime. Participants mentioned that they would only contact agencies if they could not solve the problems themselves or with the help of their friends. Only a few participants were aware of the Federal Investigation Agency (FIA) as a possibility for reporting crimes. In general, female participants were not aware of where to report. This lack of awareness was also cited as a reason why women in Pakistan do not report cybercrimes. When asked how they would report a cybercrime, participants believed the reporting procedure to be complicated and beyond their expertise: *"I don't think I'll take any steps to report cybercrime because it's quite complicated, and I do not know where to report it and what the procedure is. I have no idea." - FJMU-F1.*

Our participants were aware of the reporting features of the social media platforms they used, which contrasts with what Sambasivan reported [46]. However, they did not find the response from the platforms to be appropriate enough to deal with the cybercrime (more in Section 5.4).

We also found the sources of awareness regarding cybercrimes and privacy among young adults in Pakistan, which differed from the sources previously reported amongst low-literate populations in Pakistan as reported by Naveed et al. [39] but are more similar to the sources reported amongst US populations [41]. These sources were:

1. Friends: Participants, both male and female, reported that they mainly learned about cybercrimes and privacy features of applications from their friends.

2. Social Media Groups: Participants, primarily female, reported that they learned about cybercrimes prevalent in Pakistan through social media posts. They explained that they had joined groups on Instagram or Facebook where posts about such topics were made.

4.3.3 Concerns about Families while Reporting

Participants expressed concerns regarding family reactions when it came to reporting. They preferred not to inform their family about experienced cybercrime. They explained that if the family got aware of the cybercrime situation, they would start worrying, and it would cause them mental stress. One participant mentioned that if someone has not done anything wrong, they should tell their family about the cybercrime. However, what constitutes as wrong varies from family to family. Since the burden of maintaining family's honor often falls on women in Pakistan [39], even talking to men online could be considered a wrongful act by women. Noting this, female participants expressed concerns about being victim blamed if they informed their family members about the cybercrime violation. They believed their parents would not be supportive of their actions and would point out faults in their actions. Victim blaming is also common in Pakistan, especially regarding women. Participants expressed that they do not have enough space to talk about these issues safely: *"Because the females are being affected by cybercrime so much that we cannot even talk about it. And whoever does, gets victim blamed that it's your own fault. That's the main problem that we don't get enough space to talk about it or be heard." - GF3.*

Additionally, family members discourage female participants from reporting cybercrime to concerned authorities and ask them to instead block the perpetrator and ignore it. This is typically done to preserve family honour and reputation within their social circles. Due to this, participants preferred resolving cybercrime situations personally to contain its spread to family members or the public. Such familial concerns have not previously reported as barriers in the Global North [13, 15, 19, 37].

5 Discussion

Our work examines experienced and perceived online harms and cybercrimes within Pakistan's educated and technologically proficient young adult population. The security gaps discussed in section 4.2 have serious implications in a complex context like Pakistan, particularly for young people who navigate religious values, family honour, peer pressure, a lack of legal support and gendered expectations in online spaces.

We highlight key insights from our findings below:

- We find distinct gendered differences in the experiences of and types of harm from cyber-crimes, with female users predominantly harmed through violations negatively impacting their reputations or those of their families like defamation, fake profiles or NCUI. In contrast, male users are often more concerned with financial frauds often because in Pakistan they are responsible for finances and actively conduct financial transactions.
- Significant emphasis is placed on social standing within the community in this context and so users are reluctant to report cyber-crimes or seek help from authorities. There are also few legal frameworks tackling cybercrimes, leaving young people with little support.
- Users are very aware of platform level vulnerabilities, but often not of platform affordances. This coupled with an inadequate response from reporting to platforms means they often rely on non-technical (social) mechanisms to protect themselves. For example, female users engage in collective, mass reporting of accounts used for harassing other female users (within a short period of time) to shut down the account.

It is important to highlight here that most often the focus in South Asia is on privacy *literacy* as most prior work in the region has focused on low-literate or low-income populations [15, 19, 39, 45–47]. In contrast, we find even with tech-savvy, literate and early adopters of technologies, platform privacy features fail to provide contextualized privacy affordances.

Our findings in particular highlight the gendered differences in how cybercrimes are experienced and perceived. While this is also reported in studies in the US and UK [34,55], we find in the Global South context (India, Bangladesh and

Pakistan), female users report a higher incidence of cybercrimes like unsolicited contact, non-consensual use of information (NCUI), fake profiles and impersonation [46]. These similarities suggest a shared cybercrime landscape among these countries. In contrast, identity theft was a greater concern for individuals in the USA, while hidden costs in services, frauds, and scams were more worrisome for Germans [29]. Shoulder surfing, a threat not found in our target demographic, raised concerns among individuals in Germany and Saudi Arabia [45]. Our work in addition to prior work in Pakistan, India and Bangladesh [18, 20, 39, 46, 47] suggests some shared experiences, concerns, harms and mitigation strategies across all these countries, highlighting the need for culture, context specific privacy design.

5.1 Design Implications

Based on our data we identify several design opportunities for addressing the concerns of our population. Despite their technical proficiency, our participants demonstrated a lack of knowledge about the privacy features provided by social media applications. The results of our study indicate that multiple participants were not aware of the privacy affordances provided by social media platforms that made them vulnerable to cybercrimes. One possible way to address this issue is to use geo-location tagging to identify users in contexts where they might be vulnerable to specific privacy violations. Using this context based on geo-location, platforms could customise on-boarding procedures. Platforms should also consider switching from an opt-out mechanism for privacy settings to an opt-in default approach, whereby privacy preservation is the default setting. Below we propose mechanisms to counter the cybercrimes discussed in Section 4.2:

1. **Unsolicited contact**: One possible mechanism to tackle this is for social media platforms to consider implementing default settings that disable contact by strangers or provide users with the option to make these choices during an context-specific on-boarding process.

2. **Cyberstalking**: We propose that social media platforms notify users when their profiles are repeatedly visited by another user within a short timeframe. We also recommend that profiles should be locked by default or locked during privacy on-boarding.

3. **Fake profile**: Our participants identified a significant concern when reporting incidents to social media platforms, specifically their lack of visibility into the progress and outcome of their reports. This lack of transparency, particularly in cases where the reported incident was time-sensitive, such as defamation, led to participants attempting to resolve the issue on their own. To address this issue, we propose that social media platforms should implement a feature that provides users with a timeline of the progress of their reports. This would enable users to have greater visibility into the actions taken in response to their reports, and to make more informed decisions about their next steps. It is also vital that platforms create context aware, culturally appropriate guidelines to address reports. Geo-locations of the users reporting can be used to send the reports to specific channels to handle them with the relevant cultural context.

4. **Financial Fraud**: To enhance awareness and protect users from financial fraud, we recommend that social platforms implement a nudging strategy by regularly providing information about common scams in the user's country. By utilizing geolocation data, platforms can tailor the information to be specific and relevant to each user's location, helping them stay informed and vigilant against prevalent scam patterns in their area.

6 Conclusion

Our study employs the repertory grid technique and qualitative interviews to unpack users' mental models of cybercrimes, their experiences with cybercrime, and their privacy-preserving behaviors. We highlight the importance of understanding and incorporating specific cultural and religious values into the design to allow diverse users to freely use online spaces. We also underscore the challenges of designing in such nuanced and complex contexts where religious, familial, and cultural values often clash with user desires and online behaviours. Despite these challenges, it is important for designers and platforms to consider potential mechanisms to address the safety of young online users in contexts like Pakistan, where there is little legal support from local agencies.

Acknowledgments

This research was funded by the German Academic Exchange Service‘s (DAAD) “Deutsch-Pakistanische Forschungskooperationen“ program under project ID: 57609539.

References

[1] Covid-19 exploited by malicious cyber actors-2020. https://www.cisa.gov/uscert/ncas/alerts/aa20-099a (02/05/2023).

[2] Digital development dashboard. https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx (02/05/2023).

[3] Digital rights foundation, annual report 2021. https://digitalrightsfoundation.pk/wp-content/uploads/2022/05/helpline-annual-report-2021-1.pdf (02/15/2023).

[4] Interpol report shows alarming rate of cyberattacks during covid-19.

[5] Minimum wage notifications. https://efp.org.pk/minimum-notifications/.

[6] Ayaz Hussain Abbasi. Pandemic effect: Cybercrime on the rise. *T-Magazine*, 2022.

[7] Norah Abokhodair and Sarah Vieweg. Privacy & social media in the context of the Arab Gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, pages 672–683, 2016.

[8] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. Aunties, strangers, and the FBI: Online privacy concerns and experiences of Muslim-American women. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 387–406, 2022.

[9] Ahmed Aleroud and Lina Zhou. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68:160–196, 2017.

[10] Antonia Bauman. The use of the repertory grid technique in online trust research. *Qualitative Market Research*, 18(3):362–382, 2015.

[11] Steven Bellman, Eric J Johnson, Stephen J Kobrin, and Gerald L Lohse. International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5):313–324, 2004.

[12] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. On the need for different security methods on mobile phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, pages 465–473, 2011.

[13] Morvareed Bidgoli, Bart P Knijnenburg, and Jens Grossklags. When cybercrimes strike undergraduates. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–10, 2016.

[14] Timm Böttger, Ghida Ibrahim, and Ben Vallis. How the internet reacted to COVID-19: A perspective from Facebook's edge network. In *Proceedings of the ACM Internet Measurement Conference (IMC '20)*, pages 34–41, 2020.

[15] Casey Breen, Cormac Herley, and Elissa M Redmiles. A large-scale measurement of cybercrime against individuals. In *CHI Conference on Human Factors in Computing Systems*, pages 1–41, 2022.

[16] Nela Brown and Tony Stockman. Examining the use of thematic analysis as a tool for informing design of new family communication technologies. In *27th International BCS Human Computer Interaction Conference (HCI 2013)*, pages 1–6, 2013.

[17] David Buil-Gil, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, and Nacho Díaz-Castaño. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, 23(sup1):S47–S59, 2021.

[18] Jay Chen, Michael Paik, and Kelly McCabe. Exploring internet security perceptions and practices in urban Ghana. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 129–142, 2014.

[19] Cassandra Cross. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2):187–204, 2015.

[20] Jayati Dev, Sanchari Das, and L Jean Camp. Understanding privacy concerns of whatsapp users in india: poster. In *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security*, pages 1–1, 2018.

[21] Maeve Duggan. Online harassment 2017. 2017.

[22] Mark Easterby-Smith. The design, analysis and interpretation of repertory grids. *International Journal of Man-Machine Studies*, 13(1):3–24, 1980.

[23] Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, et al. A year in lockdown: How the waves of COVID-19 impact internet traffic. *Communications of the ACM*, 64(7):101–108, 2021.

[24] Jerry Finn. A survey of online harassment at a university campus. *Journal of Interpersonal Violence*, 19(4):468–483, 2004.

[25] Digital Rights Foundation. Helpline annual report 2021, 2022.

[26] Bannister Fransella, Bell. *A Manual for Repertory Grid Technique*. John Wiley, New York, 2004.

[27] Imran Gabol and Taser Subhani. Qandeel baloch murdered by brother in Multan: police. *DAWN.COM*, Jul 2016.

[28] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. Keep on lockin' in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4823–4827, 2016.

[29] Marian Harbach, Sascha Fahl, and Matthew Smith. Who's afraid of which bad wolf? A survey of it security risk awareness. In *2014 IEEE 27th Computer Security Foundations Symposium*, pages 97–110, 2014.

[30] Julio Hernandez-Castro and Eerke Boiten. Cybercrime prevalence and impact in the UK. *Computer Fraud & Security*, 2014(2):5–8, 2014.

[31] Judith A Holton. The coding process and its challenges. In Kathy Charmaz and Antony Bryant, editors, *The Sage handbook of grounded theory*, volume 3, pages 265–289. Sage, Los Angeles, 2007.

[32] Devi Jankowicz. *The Easy Guide to Repertory Grids*. John Wiley, New York, NY, USA, 2003.

[33] Katharina Krombholz, Dieter Merkl, and Edgar Weippl. Fake identities in social media: A case study on the sustainability of the Facebook business model. *Journal of Service Science Research*, 4:175–212, 2012.

[34] Carsten Maple, Emma Short, and Antony Brown. Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey. Technical report, University of Bedfordshire, 2011.

[35] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, pages 2189–2201, 2017.

[36] Nora McDonald and Andrea Forte. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[37] Matti Näsi, Petri Danielsson, and Markus Kaakinen. Cybercrime victimisation and polyvictimisation in Finland—Prevalence and risk factors. *European Journal on Criminal Policy and Research*, pages 1–19, 2021.

[38] Matti Näsi, Atte Oksanen, Teo Keipi, and Pekka Räsänen. Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16(2):203–210, 2015.

[39] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. "Ask this from the person who has private stuff": Privacy perceptions, behaviours and beliefs beyond weird. In *CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2022.

[40] Kaja Prislan, Igor Bernik, Gorazd Meško, Rok Hacin, Blaž Markelj, and Simon LR Vrhovec. Cybercrime victimization and seeking help: A survey of students in Slovenia. In *Proceedings of the Third Central European Cybersecurity Conference*, pages 1–2, 2019.

[41] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How I learned to be secure: A census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677, 2016.

[42] Carin MM Reep-van den Bergh and Marianne Junger. Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, 7(1):art. 5, 2018.

[43] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 'I have too much respect for my elders' understanding South African mobile users': Perceptions of privacy and current behaviors on Facebook and WhatsApp. In *Proceedings of the 29th USENIX Conference on Security Symposium*, pages 1949–1966, 2020.

[44] Ronit Rozenszajn, Galia Zer Kavod, and Yossy Machluf. What do they really think? the repertory grid technique as an educational research tool for revealing tacit cognitive structures. *International Journal of Science Education*, 43(6):906–927, 2021.

[45] Mennatallah Saleh, Mohamed Khamis, and Christian Sturm. What about my privacy, Habibi? Understanding privacy concerns and perceptions of users from different socioeconomic groups in the Arab World. In *IFIP Conference on Human-Computer Interaction (INTERACT 2019)*, pages 67–87. Springer, 2019.

[46] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, page 2, 2019.

[47] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 127–142, 2018.

[48] Express News Service. Girl commits suicide after morphed pics appear on Facebook... *The New Indian Express*, Jun 2016.

[49] Calvin Shivers. Covid-19 fraud: Law enforcement's response to those exploiting the pandemic. *Federal Bureau of Investigation*.

[50] Felix B. Tan and M. Gordon Hunter. The repertory grid technique: A method for the study of cognition in information systems. *MIS Quarterly*, 26:39–57, 2002.

[51] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, et al. Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 247–267. IEEE, 2021.

[52] Kurt Thomas, Patrick Gage Kelley, Sunny Consolvo, Patrawat Samermit, and Elie Bursztein. "It's common and a part of being a content creator": Understanding how creators experience and cope with hate and harassment online. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, page art. 121, 2022.

[53] Steve van de Weijer, Rutger Leukfeldt, and Sophie Van der Zee. Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, 43(1):17–34, 2020.

[54] Jessica Vitak, Kalyani Chadha, Linda Steiner, and Zahra Ashktorab. Identifying women's experiences with and strategies for mitigating negative effects of online harassment. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 1231–1245, 2017.

[55] Emily A Vogels. The state of online harassment. *Pew Research Center*, 13, 2021.

[56] S Elizabeth Wick, Craig Nagoshi, Randy Basham, Catheleen Jordan, Youn Kyoung Kim, Anh Phuong Nguyen, and Peter Lehmann. Patterns of cyber harassment and perpetration among college students in the united states: A test of routine activities theory. *International Journal of Cyber Criminology*, 11(1):24–38, 2017.

A RGT Protocol

Hello, thank you so much for agreeing to this interview! I am from <institution name>, and I'm working with my fellow researchers to understand the cybercrime experiences, perceptions, and understandings of young adults in Pakistan. In this interview, we hope to learn more about your digital activity and your experiences with cybercrime, if any. To accomplish this task, we will use an interesting interview technique called Repertory Grid Technique. I will explain the specifics of the methodology as we proceed.

Here are a couple of pointers before we start:

- We will compensate you PKR 500 for your time. Kindly share your account details at the end of the interview.
- I would ideally want to record this interview so I can later analyze your responses. Do you give me consent for the audio recording of this interview?
- We will keep your data anonymous and secure. It would not be shared with anyone apart from our research team. If your quotes are used in the final report, we will label the quote with a dummy label that cannot be traced back to you.
- The interview will take approximately 1 hour of your time. If you want to stop the interview at any point during this session, please let me know. You will still be fully compensated for your time.

If you have questions, then do let me know. I am going to start recording now. I would like you to reconfirm that you have given me consent to record this interview.

A.0.1 Focus: Demographics

- What is your age?
- What is your gender?
- What is your current education?
- What is your current occupation, if any?

A.0.2 Focus: Electronic usage

- How many electronic devices do you own?
- How many of the electronic devices you mentioned are shared among your friends or family?
- What are your most frequently used applications?

A.0.3 Focus: Opening questions

- Have you ever been the victim of a cybercrime? If so, can you tell me about your experience?
- Have you ever had to report a cybercrime to law enforcement? How did that experience go?

A.0.4 Focus: Methodology familiarization

Thank you for sharing your experiences. I will now introduce you to the Repertory Grid Technique. Let me walk you through an example, so it is easier for you to understand the process.

- Tell me the names of any three Professors you have had the opportunity to work or study with.
- Can you tell me a way in which any two of these Professors are different from the third? Why is that?

I will write down your comparison on the grid now. On the left is the ’similarity pole,’ meaning the property you found similar in two Professors. On the right is the ’contrast pole,’ the property you found contrasting in the third Professor. [Details: A sample of the grid is shown in Figure 4]

- On a scale from 1 to 5, rate each Professor based on his/her closeness to the similarity or contrast pole. 1 means the Professor strongly lies in the similarity pole category; 5 means the Professor strongly lies in the contrast pole category. The middle value of 3 means the Professor cannot be classified in either of the categories or can be equally classified in both of them.
- Please justify your ratings for each Professor.

A.0.5 Focus: Element familiarization

Let’s move on to the main part of the interview. Here is the list of 9 cybercrimes. In addition to these, I am adding cybercrimes you have personally experienced but are not on this list.

- Give me a definition of each of these cybercrimes. If I feel you are missing any crucial point, I will correct you.

A.0.6 Focus: Main Repertory Grid study

Great! We are all set. I will be presenting you with a random set of three cybercrime names one by one. You are required to compare and contrast any two of them with the third one. The process will be the same as the example we went through about the Professors. [Details: The triads were presented in the order shown in Table 3]

Triad No	Element 1	Element 2	Element 3
1	Hacking	NCUI	Unsolicited Contact/ Inappropriate Contact
2	NCUI	Unsolicited Contact/ Inappropriate Contact	Blackmailing
3	Unsolicited Contact/ Inappropriate Contact	Blackmailing	Fake Profile/ Impersonation
4	Blackmailing	Fake Profile/ Impersonation	Scam/ Financial Fraud
5	Fake Profile/ Impersonation	Scam/ Financial Fraud	Defamation
6	Scam/ Financial Fraud	Defamation	Stalking
7	Defamation	Stalking	Abusive Comments
8	Stalking	Abusive Comments	Hacking
9	Abusive Comments	Hacking	Scam/ Financial Fraud

Table 3: Triads

B Qualitative Study Protocol

B.0.1 Focus: Demographics

- What is your age?
- What is your gender?
- What is your current education?
- What is your current occupation, if any?
- What is your marital status?

B.0.2 Focus: Electronic usage

- How many electronic devices do you own? Name them.
- How long have you owned a device and have been using internet services?
- How many of the electronic devices you mentioned are shared among your friends or family? What purpose do they use your device for?
- What do you usually use your devices for? How many applications do you use? What are your most frequently used applications?

B.0.3 Focus: Internet consumption

- What do you think is the greatest privacy risks on the online platforms that you use?
- Do you share different information on different online platforms [including social media sites and e-commerce]? Why is it so?
- What kind of information (that you share online) is riskier and needs to be protected more securely?

B.0.4 Focus: Privacy-preserving mechanisms

- On a scale of 1 to 10 (1 being the lowest and 10 being the highest), how concerned are you about privacy violations?

- Which threats do you fear the most? Why is that? What measures do you take to protect yourself against them?
- Do you use any security measures to protect the data on your phone, device, and applications? If yes, what measures do you take?

B.0.5 Focus: Understanding of and experiences with cybercrime

- How would you define cyberspace?
- What do you think is a privacy violation in the digital space? What types of these violations are included in your interpretation of cybercrime?
- What demographics/ groups are more vulnerable to cyber threats you have mentioned? How can these demographics better protect themselves from these threats?
- Have you ever experienced a privacy infringement? If yes, what exactly happened? If not, do you know of anyone else who has experienced one? Explain.
- Do you think all cybercrimes are strictly punishable? Are there any threats that you think are unethical but not a crime?

B.0.6 Focus: Awareness of cybercrime

- Do you think cybercrime is increasing? If yes, what might be the reasons?
- What do you think can be done to control (handle) privacy violations/ cybercrime? [follow up on the answer; ask how and why?]
- Where do you educate yourself about (a) cybercrime, (b) Online ethics, (c) Privacy violations?
- What barriers have you faced in educating yourself regarding (a) cybercrime, (b) Online ethics, and (c) Privacy violations?

B.0.7 Focus: Cybercrime reporting

- If a cybercrime incident were to happen to you (being hacked/unauthorized data access), what would be your first step?
- Would you be comfortable reporting a cyber threat? If so, how and where would you report? and what would your expectation be (in terms of resolution)?
- Do you think that government organizations are playing their role actively in apprehending the perpetrators of cybercrime?

B.0.8 Questions related to individual threats [From RGT data]

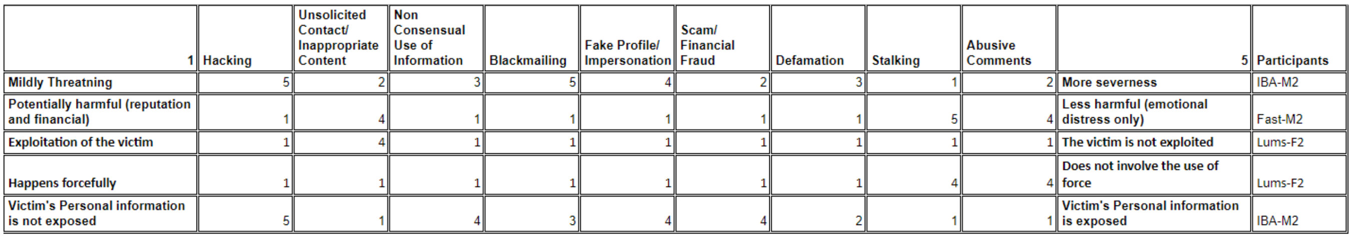
- Which threats are more frequent in cyberspace, and what factors make them more frequent? Discuss the features of the threat which make them easy to perform.
- What factors make the identification (and reporting) of a threat difficult for the victim?
- Do you think cyber threats lead to threats in the physical space? How so?
- Why do you think someone would carry out a cybersecurity breach?
- Do you think there are threats where the victim is at fault for falling victim? Could they have been avoided by taking better precautionary measures?

C Qualitative Demographics

Gender	Male Female	17 17
Age (years old)	18 19 20 21 22 ≥ 23 Average, Median, Mode	3 2 5 14 7 3 20.85, 21, 21
Education Year (Undergraduate)	Freshman Sophomore Junior Senior	4 6 3 17
University	Private Public	5 7
Owned Devices	Smartphone Laptop Tablets Tv, PC, Console	34 32 5 5
Internet Usage (years)	1-5 6-10 11-15 16-20 Average, Median, Mode	9 7 7 3 9.48, 10, 5

Table 4: Qualitative Demographics

D Repertory Grid



1	Hacking	Unsolicited Contact/ Inappropriate Content	Non Consensual Use of Information	Blackmailing	Fake Profile/ Impersonation	Scam/ Financial Fraud	Defamation	Stalking	Abusive Comments	5	Participants
Mildly Threatning	5	2	3	5	4	2	3	1	2	More severness	IBA-M2
Potentially harmful (reputation and financial)	1	4	1	1	1	1	1	5	4	Less harmful (emotional distress only)	Fast-M2
Exploitation of the victim	1	4	1	1	1	1	1	1	1	The victim is not exploited	Lums-F2
Happens forcefully	1	1	1	1	1	1	1	4	4	Does not involve the use of force	Lums-F2
Victim's Personal information is not exposed	5	1	4	3	4	4	2	1	1	Victim's Personal information is exposed	IBA-M2

Figure 4: Repertory Grid - A sample of 5 constructs elicited from 4 different participants. The left column represents the similarity pole, and the second-last right column represents the contrast pole. The middle columns represent the various cybercrimes that the participants rated on a scale of 1 to 5

E Cybercrime Definitions

Cybercrime	Description
Hacking	Gaining unauthorized access to someone's electronic system, data, account, and devices, which can result in loss of data, loss of identity, and blackmailing.
Unsolicited contact	Unsolicited contact involves unwanted and repeated calls and messages by the accused/abuser, which may include spam, repeated requests for contact, personalized threats, blackmail, or any unwanted contact that makes the receiver feel uncomfortable.
Non-Consensual Use of Information (NCUI)	NCUI occurs when an abuser uses the victim's information without their consent and usually, without their knowledge
Blackmailing	Blackmailing involves using personal information or psychological manipulation to make threats and demands from the victim.
Fake Profile	Fake profile on a social media platform is an account pretending to be someone that does not exist.
Impersonation	When someone is using someone else's identity online and is acting as them online. It manifests in profiles purporting to belong to someone on social media websites and contacting people through texts or calls pretending to be someone else
Scam Calls/ Messages	Fraudulent calls that pretend to be an individual or from an authority to make a quick profit. Mostly such scam calls lead to potential financial fraud being committed.
Defamation	Defamation involves any intentional, false communication purporting to be a fact that harms or causes injury to the reputation of a person
Stalking	Stalking is keeping track of someone's online activity, without their knowledge, in a way that it makes the subject of the stalking uncomfortable.
Abusive Comments	Abusive comments involve the usage of harsh, hurtful, explicit, or insulting language to attack another person.

Table 5: Cybercrime definitions - The definitions were supplemented from the Digital Rights Foundation's 2021 Annual Report [25].

F Codebook of Qualitative Study

Top-level category	Description	Codes
Cybercrime perceptions	Subjective experiences, beliefs, and personal definitions of cybercrime.	1. Privacy violations 2. Associated risks
Privacy risks	Cybercrime threats through technology and their consequences.	1. Fears 2. Concerns 3. Online activities 4. Vulnerable demographics 5. Device sharing 6. Avoidance
Privacy control	Management of privacy on online tools.	1. Privacy affordances 2. Privacy-preserving practices 3. Private profiles 4. Two-factor authentication 5. Encryption 6. Screenshot notifications 7. Limiting account access
Reporting	Underlying challenges to reporting cybercrime incidents.	1. Hurdles 2. Family support/ resistance 3. Reporting venues 4. Nepotism 5. Control over the situation 6. Awareness 7. Expectations on report resolution 8. Victim blaming

Table 6: Codebook