Understanding the Security Advice Mechanisms of Low Socioeconomic Pakistanis

Sumair Ijaz Hashmi*
sumair.hashmi@cispa.de
CISPA Helmholtz Center for Information Security, *and* Saarland University
Germany

Rimsha Sarfaraz*
24100234@lums.edu.pk
Lahore University of Management Sciences
Pakistan

Lea Gröber
lea.groeber@cispa.de
CISPA Helmholtz Center for Information Security, *and* Saarland University
Germany

Mobin Javed
mobin.javed@lums.edu.pk
Lahore University of Management Sciences
Pakistan

Katharina Krombholz
krombholz@cispa.de
CISPA Helmholtz Center for Information Security
Germany

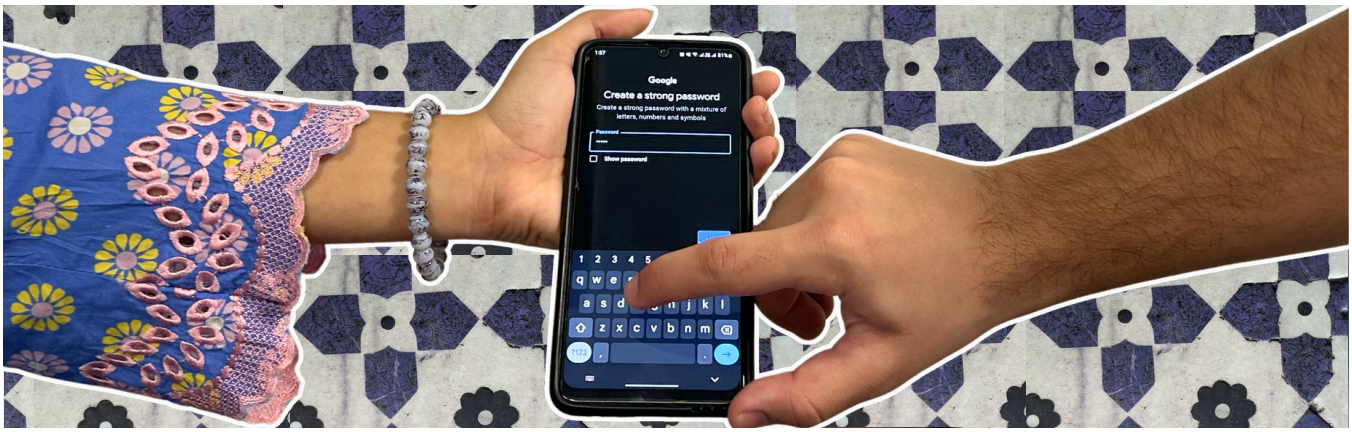

Figure 1: The helper (on the right) sets up a password for the user's new Android phone.

ABSTRACT

Low socioeconomic populations face severe security challenges while being unable to access traditional written advice resources. We present the first study to explore the security advice landscape of low socioeconomic people in Pakistan. With 20 semi-structured interviews, we uncover how they learn and share security advice and what factors enable or limit their advice sharing. Our findings highlight that they heavily rely on community advice and intermediation to establish and maintain security-related practices (such as passwords). We uncover how shifting social environments shape advice dissemination, e.g., across different workplaces. Participants leverage their social structures to protect each other against threats that exploit their financial vulnerability and lack of digital literacy. However, we uncover barriers to social advice mechanisms, limiting their effectiveness, which may lead to increased security and privacy risks. Our results lay the foundation for rethinking security paradigms and advice for this vulnerable population.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Social aspects of security and privacy**;

KEYWORDS

Security Advice, Intermediation, Passwords, Threats, Global South, Low Socioeconomic

ACM Reference Format:
Sumair Ijaz Hashmi, Rimsha Sarfaraz, Lea Gröber, Mobin Javed, and Katharina Krombholz. 2025. Understanding the Security Advice Mechanisms of Low Socioeconomic Pakistanis. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26-May 1, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 25 pages. https://doi.org/10.1145/3706598.3713297

*Both authors contributed equally to this research.

CHI '25, April 26-May 1, 2025, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713297

1 INTRODUCTION

Smartphone users from low socioeconomic backgrounds, especially those who are illiterate, face severe security challenges when navigating the online world [46, 47, 65, 76, 87, 90, 95, 96, 106, 107]. Attackers often exploit their lack of literacy, e.g., the 2023 loan scam that affected roughly 25 million users in Pakistan [15]. Pakistan is a suitable test bed to study low socioeconomic populations, as 39% of all citizens are uneducated [79], and most socioeconomically disadvantaged people are financially constrained and have limited access to technology [1, 78, 81, 102].

Security advice has been studied for W.E.I.R.D.[1] populations [37, 63, 64, 85, 89, 91, 109, 115]. However, security advice may be inaccessible to socioeconomically disadvantaged people, as it is usually in English and requires literacy [92, 93]. Furthermore, any advice obtained from the Western context may be inapplicable due to a different threat landscape in the Global South [25, 43, 103]. Prior work in the non-WEIRD context has uncovered a high reliance on informal support networks for using technology [7, 11, 97, 100]. However, how these informal support networks help navigate security-specific challenges is understudied. Similarly, it is not thoroughly mapped how the social embeddedness impacts security advice mechanisms and security-related practices in the context of the Global South.

A fuller understanding of the security advice mechanisms of low socioeconomic people is essential to identify challenges in existing advice mechanisms and to design context-sensitive and usable advice. We fill this gap with a qualitative study with 20 (10M, 10F) users from low socioeconomic communities in Pakistan that are partially or fully illiterate.

Our research examines how and why these individuals learn and share this advice and whether variations exist in their behaviors. In particular, we answer the following research questions:

RQ1: What are the security advice mechanisms of low socioeconomic Pakistanis? Uncovering their advice sources, usage, and sharing practices is important to understand their existing advice landscape to identify avenues for intervention.

RQ2: What factors influence why these people share and disseminate security advice? Uncovering motivations and barriers in advice-sharing is important to understand the potential of this social activity as a countermeasure against security and privacy threats.

Among other things, we find that our participants utilized their social structures to obtain advice and enact intermediation in security related practices, such as setting up passwords (see Figure 1) and staying safe from scams. These mechanisms helped them navigate threats that exploited their financial vulnerability and digital illiteracy. Social environments tend to influence the advice sources and lessons participants learn: we interviewed a mix of factory, domestic, and janitorial workers and found stark variances in advice mechanisms. Participants shared advice when they wished to help other vulnerable peers, promoting community belonging and trust. However, participants also encountered barriers in advice sharing, e.g., victim blaming, that limited the effectiveness of these advice mechanisms. These results call for rethinking the design of existing security mechanisms to tie them to the needs and socioeconomic context of this vulnerable population. Such efforts are essential to provide accessible technology, security, and safety for low socioeconomic populations in South Asia, one of the next decade's most prominent emerging mobile phone market [44].

[1]W.E.I.R.D refers to users in Western, Educated, Industrialized, Rich, and Democratic contexts [53].

2 RELATED WORK

Prior work relevant to our study falls into two categories: (i) security advice and collective approaches to handling security and privacy in the Global North, and (ii) studies focusing on informal support networks in the Global South to manage technology, privacy, and security.

2.1 Security Advice and Collective Approaches to Handling Security and Privacy

Security Advice. A large body of prior work uncovers security advice mechanisms in the Global North. Wu et al. systematize prior research on social cybersecurity and discuss security advice sharing under the broader domain of influencing others' security and privacy behaviors, highlighting people's reliance on each other for aid and assistance in security and privacy knowledge [112]. Studies in the US found that people learn and share security advice via various information sources such as websites, media, and the people around them, such as family, friends, and colleagues [40, 84, 85, 89, 91]. A study on security advice disseminated on online discussion forums in Japan found that, apart from cyber incidents, advice may be about password management, security software, privacy abuse, and account/device management [48]. Several studies have shown that advice sharing is prevalent because it leverages psychological principles of peer influence and social proof, which influence the adoption of secure behaviors [29–31]. Studies have uncovered that the negative experiences of other people may also influence the adoption of security practices [84, 85, 89–91].

Prior work identified challenges to adopting and disseminating security advice. Security advice on the Web may be difficult to comprehend [92, 111], and even experts fail to agree on advice prioritization, leaving end-users on their own [93]. Advice is rejected by people (i) if it is perceived to be inconvenient or difficult to implement, (ii) if the advice contains too much marketing material, or (iii) if the individual has not yet faced a negative experience [37, 89, 91, 115].

Sociodemographic factors have been found to influence security advice mechanisms [27, 58, 89, 90, 106]. Low socioeconomic Americans tend to take advice from family, friends, and service providers, while high socioeconomic Americans are more likely to take advice from their workplace [89, 90]. Low-income Americans are at high risk of privacy and security threats when navigating online services and choose to rely on informal advice sources, such as librarians or community networks [58, 106]. Coopamootoo et al. found that gender differences exist in the UK in advice sources and intake: advice from intimate and social connections is more prevalent among women, while online content is preferred by men [27]. Women approach these connections due to their perceptions of the advisor's experience and trustworthiness, while men approach social connections to evaluate options and seek second opinions [27].

Collaborative Approaches. People take collaborative approaches to make security and privacy decisions [77]. Prior research in the Western context has uncovered how people in groups, such as family members, friends, and acquaintances, may assume the roles of 'tech caregivers' and 'caregivees' while collectively handling and communicating issues with technology [64]. Such groups demonstrate "community collective efficacy", defined as a community's capacity to perform a task in a collaborative environment [23, 63]. Watson et al. found that people working in groups may share and secure digital resources, e.g., accounts, collaboratively by having collective mental models regarding threat actors and holding accountability at the individual level [109].

However, prior work has uncovered limitations in these collaborative mechanisms. There is little group coordination to safeguard digital resources, leading to many missed opportunities in collaboratively managing security and privacy [109]. Several studies find that group interactions and discussions around security and privacy are rare, often avoided, and not substantial [63, 64, 109]. When these interactions do occur, they tend to focus only on large data breaches and news events or primarily discuss security and privacy in passing without conveying constructive information [19, 109]. Individuals rarely discuss their own experiences as they find them personal and irrelevant to the group, and when they do, it is mostly with only certain individuals rather than the entire group [109]. Instead, people often prefer passive participation in security and privacy discussions as they are more inclined to seek information about others' experiences and less inclined to share their own [26]. A few reasons, uncovered by prior work, on why these challenges may occur are (i) a lack of incentive to participate due to unequal responsibilities, (ii) tech savviness causing a power imbalance in existing power hierarchies, or (iii) a lack of individual-level privacy when engaged in group-level activities [8–10, 63, 64].

2.2 Advice Mechanisms Beyond W.E.I.R.D.

Security behaviors in developing regions differ due to cultural differences, knowledge gaps, context, technology use, usability, and cost considerations [103]. Warford et al. systematize how at-risk people, such as those from low socioeconomic backgrounds (e.g., those in developing contexts [4–6, 68, 94, 103], developed contexts [61, 89, 90, 98, 106, 108, 110], non-Western women [13, 33, 95, 96, 104], and older adults in developing regions [59]), suffer from risks, such as (i) time and resource constraints due to a lack of income, education, and digital literacy, (ii) societal constraints due to their marginalization, and (iii) relationships with potential attackers in their social circles [107]. To mitigate these risks, at-risk users may adopt social protective practices, such as taking (i) informal help from trusted family and peers or (ii) formal help from trusted organizations, like libraries [107]. We find that these factors motivate low socioeconomic Pakistanis to leverage their existing social structures to disseminate security advice and intermediate in security-related technology use, such as setting up passwords and avoiding negative experiences.

Examples of Advice Sharing Beyond W.E.I.R.D. Several examples in the Global South context show how people adopt more social and collective approaches to advice sharing. Redmiles et al. found that users from collectivist-focused countries, such as Brazil, Vietnam, and India, seek information from others at higher rates as compared to individuals from more individualistic-focused countries, such as the US [88]. Das et al. found that MTurk users from India were much more likely to report changing their security or privacy behavior in response to a social trigger than MTurk users from the US [29]. Sambasivan et al.'s work shows that community networks in urban slums in India intermediate and direct the mobile phone usage of those around them, leading to a high level of trust in the community for phone and camera sharing [97]. Extreme examples of reliance on others can be taken from studies in Bangladesh, where researchers found that people may ask for help from others while using the phone for anything other than making and receiving phone calls [11, 100], such as local rickshaw drivers depending on their more literate peers to access basic mobile phone operations [7]. Phone sharing in families in Bangladesh also opens up avenues for intermediation from family members to help stay safe from online threats, such as harassment and unsolicited contact [4]. Research in urban India has examined how the collaborative behaviors enacted in families for protection from threats involve self-appointed family technology managers who make decisions for their elderly to protect them from perceived threats [73]. Similarly, research on cybercafes in Kenya found a huge reliance on the support and advice of cybercafe managers, such as to setup user passwords, who often may adopt unsafe practices that compromise the digital safety of their customers [72]. Furthermore, Reichel et al. found that privacy knowledge about social media apps in middle-to-low income South African communities is learned via word of mouth and from friends [94]. South Asian women across socioeconomic strata also rely on family members for emotional support and advice when harassed online [95, 96].

Advice Sharing in Pakistan. As explained by Gröber et al. in their work on Pakistani content creators [43], Pakistan, in particular, is an interesting landscape to study because of its highly gendered, Islamic, and class-based society where patriarchy and religious norms define the landscape of the country. Prior work has uncovered how such patriarchal norms, religious and family values, and social standing in society influence the security and privacy perceptions and behaviors of Pakistani citizens (a few examples are [16, 43, 76, 87, 95, 96]). In the context of advice sharing, a study on security advice sources and adoption of urbanized and educated stay-at-home Pakistani women found many similarities with prior work done in the Western context [37], where they rely on informal advice sources such as family and friends and adopt/reject advice due to similar reasons related to convenience and effort [12]. Similarly, Ashraf et al. found that young Pakistani adults rely on friends and online social media groups to gain awareness about cybercrime [16]. Prior research on a broader sample has shown how Pakistani women lack the agency to make decisions about purchasing and using phones [56]. Instead, male family members enforce these decisions on their women [56]. Work done on privacy knowledge sources of low-income and low-literate Pakistanis found that men learn about privacy settings and knowledge from each other in social gatherings, and women (who are largely excluded from such gatherings) learn from their men [76]. As a countermeasure to social exclusion, several studies investigate Pakistani women-only digital safe spaces, such as Facebook groups, where

women can anonymously discuss advice on socially taboo topics, such as domestic abuse [14, 74, 113]. Regarding security-related threats, Razaq et al. highlight how Pakistanis collaboratively navigate the landscape of mobile-based scams by uncovering limiters and enablers within victims' social circles who (mis)guide others on how to react to scams [87].

However, the advice disseminated concerning such threats among low socioeconomic Pakistanis, along with the factors enabling or inhibiting advice-sharing, are understudied. Our work provides another facet to prior literature in the Global South as we study how low socioeconomic Pakistanis enact security advice mechanisms and collaborative behaviors mentioned in Section 2.1. In particular, we explore how and why the social support networks of these people influence how they disseminate and use security advice to help configure secure behavior and navigate their threat landscape, which we also uncover.

3 METHODOLOGY

We conducted qualitative semi-structured interviews with n=20 participants (10M, 10F) to understand low socioeconomic Pakistanis' security advice sources, usage, and sharing mechanisms. Figure 2 provides an overview of the study procedure and we offer further details in the following sections.

3.1 Target Population

Our target population was Pakistanis from a low socioeconomic background, with a special emphasis on illiteracy. We defined low socioeconomic background as: (1) Income level close to or below the country's monthly minimum wage of 32,000 PKR (≈ 115 USD [2]) [35], and (2) Literacy level below higher secondary education, which is approximately 12 years of education[3] (similar to [76]), where the education's medium of instruction was not in English[4], as an understanding of English text was required to operate mobile phones effectively [66, 67]. We did not explicitly assess their digital literacy.

3.2 Study Design

Prior work has outlined how disadvantaged people, such as low socioeconomic populations, are challenging to research [21, 39, 41, 60, 70]. For example, they may lack the incentive to participate due to a lack of interest, trust, and rapport with the researcher [41], or they may find it challenging to comprehend the contents of a study [70].

Field Work. To address these challenges upfront, we visited a factory in Pakistan to familiarize with the environment and the working conditions. While being there, we talked to four factory workers (3 men, 1 woman) in 30 min same-sex 1-on-1 sessions. The goal of the session was to explore the feasibility of different research methods (e.g. running a face-to-face survey vs. conducting interviews) and the intelligibility of the necessary terminology and technical concepts. We found that people lacked the vocabulary to articulate the concepts we were interested in and that even seemingly simple technical terms such as *"smartphone"* could lead to confusion and false answers. We found that a conversational style of data gathering was more successful, as it left room to adapt closely to the participant's needs and offer clarifications when needed. Following the field work, we decided for semi-structured interviews to answer our research questions.

Development of Interview Guideline and Pre-tests. We iteratively developed and pre-tested the interview guideline with seven janitorial workers from our university (3M, 4F). After each interview, we debriefed them on our motivation to conduct in-depth interviews with other blue-collar workers to understand how they face and deal with online threats. We obtained and incorporated their feedback into the question style and topics. The pre-tests alternated between male and female participants to ensure comprehension and inclusion across genders.

We observed the following challenges from pre-testing, which informed subsequent changes to the protocol:

- **Comprehension**: A major challenge was ensuring participants understood our questions and gave meaningful and relevant responses, especially regarding complex and abstract topics such as "security". Similarly, our pilot participants struggled discussing security advice on an abstract level. This led to the following changes: (1) We designed the interview guideline around concrete technology use, focusing on phones since those are relatively accessible to low socioeconomic populations [56, 97]. To elicit security threats, we then asked about any negative experiences they, or someone they knew, had encountered when using the phone or apps on the phone. (2) If needed, we provided contextualized and local examples of security threats, such as by talking about concrete Pakistani scam narratives instead of discussing scam calls abstractly. These examples were taken from the Digital Rights Foundation's annual Pakistani cyber harassment helpline report [34]. (3) We removed technical terms, such as "phishing", which our participants expressed difficulty comprehending, and replaced them with easy-to-understand and hands-on definitions. See Appendix Section A.6 for threat definitions.
- **Trust and Rapport**: We uncovered that our participants were generally uncomfortable discussing threats and negative experiences. Their reservations were understandable as they may have felt it was unwise to discuss their incidents with apparent strangers. To establish rapport and trust with our participants (1) We thoroughly explained the study's contents and purpose, assuring them of their safety and anonymity (see Ethics 3.5), (2) We assured them we would not judge their knowledge, actions, or responses to our questions and that our interviews would not affect their jobs, and (3) We started the interview with phone usage behavior to get participants comfortable talking.

Using our observations and their feedback, we then crafted the final interview protocol, explained next. We stopped pre-testing after seven participants, as the last two participants gave relevant and meaningful responses and did not suggest further recommendations. The data of the pre-test is not included in the final analysis.

[2]For reference, 1 USD was equivalent to 278.88 PKR and 1 EUR was equivalent to 309.4 PKR at the time of writing in September 2024.

[3]In Pakistan, schools are commonly divided into Kindergarten, Primary (1-5 years of education), Middle (6-8 years of education), Secondary (9-10 years of education), and Higher Secondary (11-12 years of education) [2].

[4]In Pakistan, public schools generally use Urdu as the medium of instruction [69].

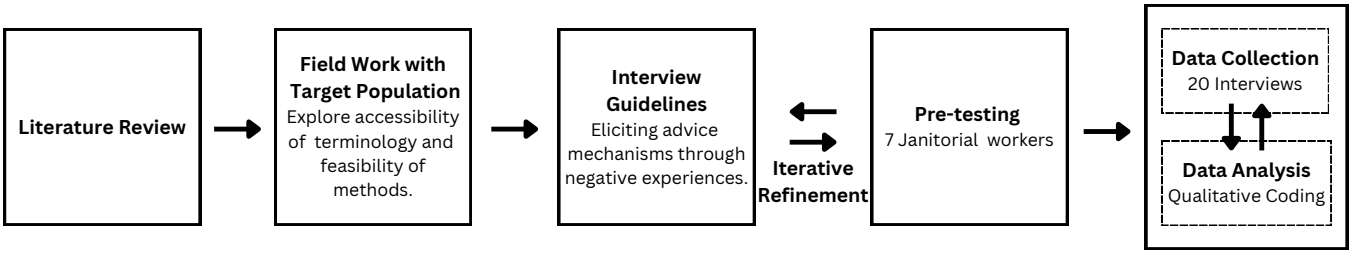

Figure 2: Overview of the Study Procedure to Elicit Security Advice Mechanisms.

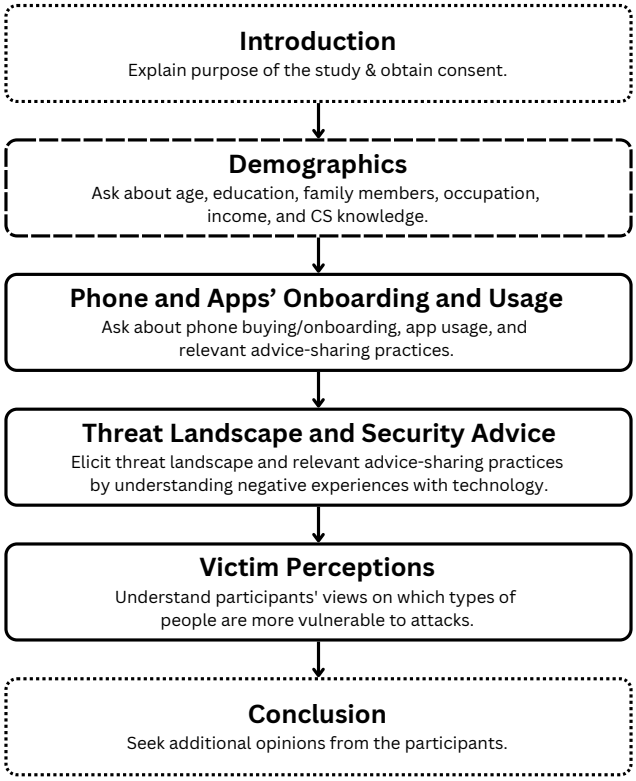

Figure 3: Interview Protocol

3.2.1 Final Interview Protocol. Figure 3 provides an overview of the interview flow and contents. We describe the interview sections below, and the complete protocol is attached in Appendix A. We conducted the interviews in a mix of Urdu and Punjabi, depending on the participant's preference. Each interview started with an introduction that described the purpose of the study as understanding informal advice sources of technology and its threats among Pakistani citizens (see 3.5 for ethical considerations). After obtaining consent for audio recording, we began the interview. The interviews were structured as follows:

Demographics. We started with questions about their age, job description, income level, educational background, who they lived with, and computer science knowledge (whether they had completed any additional certification or training in IT, Computer Science, or related fields). These questions served as ice-breakers to get participants talking.

Phone and Apps' Onboarding and Usage. This section established how participants used technology. We asked about their digital devices, phone buying and onboarding practices, app usage patterns, and whether they share these devices with anyone else and why. We especially focused on who they took advice and help from while setting up and using their phone and apps, asking questions on how and why they took this help.

Threat Landscape and Security Advice. We then moved on to understand the threats experienced by our participants. For this purpose, we asked them to recall any negative experiences they or someone they know may have experienced while using their phones. We inquired about details regarding the incident, such as the victim, threat description, defensive mechanisms deployed, consequences suffered, and reasons for facing the threat and complying with the attacker. Here, we again focused on advice by eliciting their sources of information, including who they took help from during and/or after facing this threat, and asking questions on how and why they took this help. We asked how our participants further shared these incidents with anyone else and why. If our participants did not mention any threat incidents, we probed them with explanations and examples of known threats in Pakistan [34].

Victim Perceptions. We concluded by exploring participants' perceptions of who could be vulnerable to these attacks. This section complemented our analysis by eliciting further motivations and practices from our participants to help those around them.

3.3 Recruitment and Participants

We obtained a convenience sample through snowball recruitment in different workplaces. We reached out to workers personally or through social connections. All participants came from urban slums near Lahore, Pakistan, where the data collection occurred. After each interview, we asked participants if they knew anyone from their social circles whom we could interview. Owing to the sociocultural norms of the country, we conducted interviews in a same-sex setup. Each interview lasted between 20 - 30 minutes. Participants were given 500 PKR (≈ 1.79 USD) as monetary compensation for their participation. We calculated the compensation based on the average completion time of the pretests. It is greater than the mean hourly salary of our target population and corresponds to

Demographic	Category	Count
Gender	Male	10
	Female	10
Age (years)	20-29	7
	30-39	9
	40-49	4
Income (PKR)	15,000-20,000	2
	25,000-30,000	3
	30,000-35,000	9
	35,000-40,000	6
Education (years)	None	7
	Primary (1-5)	3
	Middle (6-8)	3
	Secondary (9-10)	7
Occupation	Janitorial Worker	8
	Factory Worker	6
	Driver	1
	Cook	3
	Housekeeper	2
Workplace	University	8
	Factory	6
	Domestic	6

Table 1: Demographics of Participants.

Gender	Monthly Income (PKR)
Male	Average: 33.4k, Median: 32k
Female	Average: 27.2k, Median: 30k
Work Environment	**Monthly Income (PKR)**
University	Average: 32.2k, Median: 32k
Factory	Average: 29.6k, Median: 31k
Domestic	Average: 28.3k, Median: 30k

Table 2: Average and Median Monthly Incomes of Participants Across Gender and Work Environments.

the Pakistani minimum wage [35]. This compensation rate is also consistent with prior Pakistan-centric user studies [16, 49, 76]. All interviews were conducted between March and July 2024.

We recruited a total of 20 (10M, 10F) participants, with 8 (4M, 4F) from the janitorial staff at a Pakistani university, 6 (3M, 3F) factory workers, and 6 (3M, 3F) domestic workers such as house helps, drivers, and cooks. All of our participants had less than or equal to secondary education (9-10 years) with Urdu as the medium of instruction. Furthermore, our participants said they could not read and write in English and self-identified as low-literate. Seven participants were illiterate. The average monthly salary of 30,500 PKR (≈ 109 USD) is slightly lower than the minimum wage. See Table 1 for the aggregated sociodemographics of our sample. Table 2 shows participants' average and median monthly incomes across gender and work environments.

3.4 Data Analysis

We transcribed the audio recordings of the interviews in the interview language (Urdu and/or Punjabi) and then translated them into English. Two native Urdu and Punjabi speaking researchers fluent in English conducted the translations. The researchers took turns translating, with one researcher translating the transcriptions into English and the second verifying by back translating the English versions into the native language. The researchers reviewed and resolved any inconsistencies between the original transcription and the back translation. Back translations have been used in prior work as a method to ensure translation accuracy [54].

We followed a bottom-up "open-coding" approach to code the interviews to obtain grounded insights from the data [24, 28, 99]. Two Pakistani researchers (one male and one female) conducted the qualitative analysis. The researchers independently coded the first eight interviews with the university staff (4M, 4F). After coding each interview, they discussed their codes and code assignments with each other to resolve disagreements and iteratively developed an initial codebook.

The researchers analyzed the initial codebook and derived high-level themes, which we used to target further recruitment of domestic and factory workers. Coding for these additional interviews was divided between the authors, where the male author coded the female interviews and vice versa. The researchers consistently discussed if new concepts emerged or if any changes were needed. We stopped data collection with an additional six interviews from the factory workers (3M, 3F) and six domestic workers (3M, 3F) as we reached thematic saturation [51, 52] in their responses concerning advice-sharing patterns. After open-coding all interviews, the researchers jointly discussed the emerging themes by grouping codes in the codebook and conducting axial coding to identify additional insights. Our codebook is attached in Appendix B.

3.5 Ethics

Our study is approved by our university's ethical review board. We adopted the following best research practices to ensure our at-risk population does not face any risks from our research [18]. Participants gave informed consent before conducting the interview. To obtain this consent, the interviewers thoroughly explained the contents of the study and answered any questions participants had. In our consent debriefing, we allowed them to stop the interview at any time or skip any question if they felt uncomfortable. All participants agreed to have their interviews audio-recorded. The collected data was treated confidentially and stored according to GDPR principles. Only anonymized participant quotes and aggregated demographics have been published.

We also acknowledge that we, as researchers, need to build reciprocity and promote community engagement with at-risk users to help them achieve their goals [18]. Our initial field work mentioned in Section 3.2 helped us understand our target population's context: by talking to them in 1-on-1 sessions, we understood their challenges on a personal level and designed a relevant interview protocol that corresponded to the issues people had. In our pre-tests we obtained feedback from our participants after each interview on how to improve the interview protocol to make it relevant to the target population and incorporated their feedback as mentioned in Section 3.2. At the end of each interview, we also asked our participants (both pre-test and final sample) about how they felt after giving the interview. Overall, our participants had a positive

sentiment towards our study and reported that they found the interviews to be quite informative, especially when we prompted them about different security-related threats, about which they had not thought about/experienced before. After the interview, the interviewers allowed participants to contact them to answer any questions regarding their mobile phone usage and security behavior.

3.6 Limitations

Despite our deliberate recruitment strategy of interviewing people from different work environments, our qualitative interview study with blue-collar workers living in urban slums may not give generalizable results for the low socioeconomic population at large. We miss out on unemployed people, gender and religious minorities, people who stay at home or live in rural areas, and people not located near Lahore, Pakistan, where our data collection occurred.

Regarding the interview protocol, we prompted our participants with specific examples from the Digital Rights Foundation's cyber harassment helpline report [34]. These examples were necessary as our pre-tests concluded that it was difficult to elicit meaningful data without giving the interviewees some example threats to jog their memory. However, we acknowledge the limitation that using such examples may bias our participants to discuss only a narrow range of incidents. We still may lack a complete picture of the spread of their negative experiences. This limitation does not invalidate our analysis, as we focus on their advice and social support mechanisms that complement their threat landscape. Regardless, future work should validate and measure the true distribution of threat incidents among underprivileged Pakistanis.

We acknowledge these limitations of our study and call for future quantitative work in this space to validate our findings.

4 RESULTS

Findings are illustrated with participants' quotes as (Gx_W), where x denotes the participant's assigned ID within the gender group G (**M**ale, **F**emale), and W represents the work environment (**F**actory, **U**niversity, **D**omestic).

4.1 Background on Technology Use & Threat Landscape

We uncover our participants' advice mechanisms by understanding two use cases of advice: (i) phone onboarding and usage patterns and (ii) threat landscape. These use cases provide background information for understanding the advice landscape explained in the following sections.

4.1.1 *Phone Onboarding and Usage Patterns.*

Phone Usage. Nineteen participants used an Android smartphone, either through personal ownership (15) or by using a shared smartphone owned by their family or friends (4). One participant used a feature phone[5]. Thirteen of our smartphone users relied on voice-based controls to navigate their phones and apps, such as using speech-to-text on YouTube to search for content and voice messages to communicate over WhatsApp. The remaining six smartphone users (younger and relatively more educated) could type in Roman Urdu. University and domestic workers used WhatsApp to communicate with their supervisors/employers. However, the factory workers were not allowed to use phones at work. Non-work-related use cases of WhatsApp involved making phone calls to family members at home. Participants also used Facebook, YouTube, and TikTok for video-based entertainment. Other commonly used apps included government-sponsored relief applications, such as the Benazir Income Support Programme application [42].

Phone Buying. Our participants cannot afford to make one-time purchases of expensive items. In urban slums, mobile shopkeepers offer customers to pay in installments instead of one-time payments. To buy phones in installments, our participants must first formally establish trust with shopkeepers by having someone else, a friend or family member that the shopkeeper(s) already trust, vouch for them and guarantee they can make the monthly payments on time. Seven participants purchased their Android phones via such installments and guarantees. These participants reported that their Android phones cost between 15-35k PKR; hence, they cannot afford to pay a large portion (approximately 50%) of their monthly salary for a phone purchase. Instead, they adopt this practice of monthly payments, paying an average monthly installment of 3-4k PKR. These were second-hand phones from Chinese-based brands, such as Xiaomi, Tecno, and Oppo. Gender differences exist in who partakes in this activity, as all female participants relied on a male family member, such as a brother or a husband, to make this purchase on their behalf [56]. Breadwinners are in charge of making these monthly payments for their families.

Phone Onboarding. All participants relied on more literate peers to help set up user accounts for their phones and applications. The onboarding process of most user accounts, such as WhatsApp, Google, and Facebook, was in English and required setting up and remembering passwords and understanding how to fill out online signup forms. However, our participants' lack of literacy inhibits their understanding of this onboarding process. Hence, they needed help setting up the Google account required for the initial onboarding of their Android phones. They also required assistance to set up accounts and/or passwords for various applications, such as WhatsApp, Facebook, and TikTok. This approach required our participants to rely on their peers/helpers to input personal details and set up passwords/PINs. These helpers included more educated family members, neighbors, shopkeepers, co-workers, and employers. Our participants did not report issues sharing such personal information with these helpers as they trusted them. The helpers did not just guide the initial phone and apps' onboarding process but also served as long-term support for our participants by helping them reset forgotten passwords, log in to the same (or set up new) accounts when they change phones, and resolve generic phone-related issues such as accidental misclicks.

Phone Sharing. Although phone sharing has already been explored in the Global South [3, 4, 56, 76, 96, 97], we briefly mention similar practices adopted by our participants as it opens up avenues for sharing advice with phone-sharers. People who owned feature

[5]A feature phone is an earlier generation mobile phone that contains only basic functionalities, such as making and receiving phone calls and SMS via a mobile SIM. A feature phone usually lacks a touchscreen and has physical buttons instead of virtual ones.

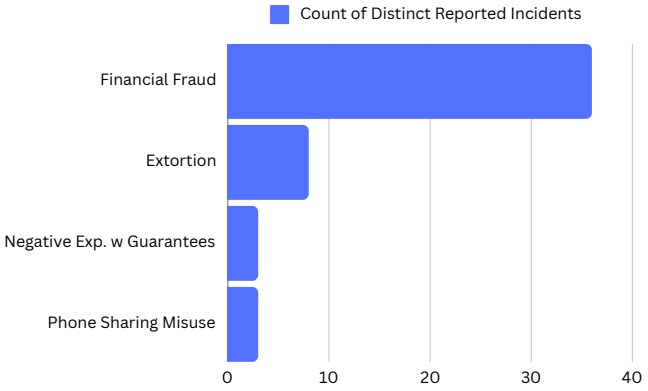

Figure 4: Frequency of Threats Based on Reported Interview Data.

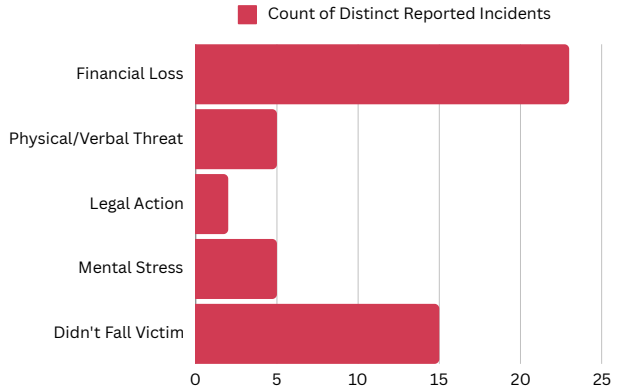

Figure 5: Distribution of Types of Harms Based on Reported Interview Data.

phones used other people's smartphones. People who go to work during the day shared their smartphones with their family members when they returned home. They participated in this phone-sharing activity primarily because they could only afford one or two smartphones in their house. Hence, everyone must use the same limited set of phones for leisure or work.

4.1.2 Threat Landscape. We uncover the following threats our participants have experienced or heard about through their advice sources. For each type of threat, we specify the total number of participants from our qualitative study who reported this threat (**T**) and further categorize them based on whether participants shared their incident(s) after being prompted by the interviewer (**P**) or actively without prompting (**A**), using the notation **[T = m + n | P: m | A: n]**. Figure 4 presents the frequency of incidents with *Financial Fraud* being the most prevalent in our qualitative sample, followed by *Extortion*, *Negative Experiences with Guarantees and Installments*, and *Phone Sharing Misuse*.

As a consequence, participants reported different types of harms: (i) financial losses of up to 350,000 PKR, (ii) physical and verbal harassment where attackers verbally abused victims and threatened them with house visits, (iii) legal action where victims were framed and arrested by the police, and (iv) mental distress. Figure 5 provides the counts for each type of harm based on reported interview data. Table 3 provides an overview of the harms of each threat uncovered.

Financial Fraud. **[T = 18 | P: 12 | A: 6]** Attackers conduct social engineering attacks by either incentivizing targets with monetary rewards or threatening them with negative consequences, such as a loss of money or legal action [49, 62, 83, 87, 101]. Based on incidents reported by our participants, attackers may conduct these attacks over a phone call, text message, or in person. Participants reported receiving scam calls that mimic government-sponsored relief programs and offer prize money or rewards in exchange for a small transaction fee. Another type of scam call involves the attackers impersonating the police, informing the target that their male younger relative, such as a son or a nephew, has been caught clubbing or drinking (socially taboo activities in Pakistan); the scammer demands bail-out money to let the relative go. Many such calls lead to monetary losses; for example, F1_U's male cousin lost 40k PKR in a scam call he faced. Thus, we uncover similar findings on scam calls as prior work on mobile-based fraud in Pakistan [83, 87], re-emphasizing this attack vector.

Extortion. **[T = 6 | P: 2 | A: 4]** Our participants reported facing extortion incidents where strangers or distant relatives would make unsolicited phone calls to harass women in their social circles, asking them to meet in person (F3_U's colleague), or trying to create a rift with their spouses (M8_D's wife), threatening with negative consequences if they don't comply. Another example of extortion involves leveraging the poor financial situation of our participants, where online unverified third-party loan apps initially offer easy loan plans but start harassing them with phone calls and house visits as the loan repayment deadline approaches. One such loan app is the "Barwaqt Loan" app, which has gained controversy in the country for its illegal extortion practices [15, 38]. An example is M3_U, who took a loan of 3000 Rupees from such a loan app. However, five days before the loan payback was due, the loan sharks started calling the participant, harassing him to repay his loan immediately, and threatening to misuse his personal information and visit his house if he wouldn't comply. When signing up on such apps, people fill out forms which ask for their personal information, such as their national ID number, full name, house address, emergency contacts, and phone number [17], which can be used as leverage to harass them.

Negative Experiences with Installments and Guarantees. **[T = 3 | P: 0 | A: 3]** Several risks are associated with the social activity of buying phones in installments, as described earlier. One risk is that participants who vouch for others need to be careful who they vouch for. While participants try to only vouch for their trusted friends and family members, these people may, deliberately or otherwise, be unable to make their payments on time. In such cases, the shopkeeper blames the voucher for the delay in the payment, as the voucher was responsible for ensuring timely payments. In extreme cases, shopkeepers may conduct house visits to demand their dues. Such house visits cause financial loss as well as mental distress for

	Monetary Loss	Physical/Verbal Threat	Legal Action	Mental Stress	Didn't Fall Victim
Negative Experience with Installments & Guarantees	•	•	•	•	
Extortion	•	•		•	•
Phone Sharing Misuse	•	•	•	•	
Financial Fraud	•			•	•

Table 3: An overview of the harms for each threat uncovered. The dot (•) represents the presence of a specific consequence corresponding to each threat type.

the voucher. The voucher must comply with the shopkeepers' demands to maintain their reputation and avoid escalating unwanted troubles with the shopkeepers during these house visits. Hence, vouchers must remain careful when deciding to whom they give a guarantee, opting to avoid the activity altogether despite pleas from their relatives and friends for assistance: *"Now when someone asks us to help them, we say, 'No, we can't.' We say this because we must care for our own pockets first, as we have seen that the one who gives the guarantee always gets in trouble"* (M5_F, whose family had to pay 20k PKR to a shopkeeper on behalf of their vouchee, a neighborhood friend, who ran away and shifted cities as he could not pay his installments).

Phone Sharing Misuse. **[T = 2 | P: 0 | A: 2]** Phone sharing may lead to fraud, reputational harm, and legal action against phone sharers. A man in F9_D's previous neighborhood allowed a stranger girl to use his phone to make a phone call when she requested it. However, after she made the phone call, the girl ran away and disappeared, and the man started getting calls from the girl's family, who accused him that he had kidnapped her and stolen her possessions. The girl's family pressed charges against him, leading to further consequences: *"That poor boy lost everything; he had to spend two years in jail"* (F9_D). Similarly, a man in M3_U's old neighborhood used his friends' phones to make phone calls to his girlfriend. He used his friends' phones to prevent his family from finding out (engaging in romantic relationships without family approval is a socially taboo activity in Pakistan). One day, the couple decided to run away together. However, the woman's family perceived that the man had kidnapped her and filed a police complaint against him. The police used the woman's phone, which she left behind when she ran away, to track all the calls made to her phone. The police then continued to arrest and interrogate all the man's friends, who had shared their phones with him, to ask for his whereabouts. In Pakistan, the police is able to trace phone numbers by various methods, such as by working together with the Pakistan Telecommunication Authority [80] to check SIM ownership records and connect them with the other government databases that contain residence-related information, such as NADRA records [75].

4.2 Methods of Giving Help (RQ 1)

We categorize *"helpers"* (mentioned in Section 4.3) as people who provide their peers with support, advice, and guidance. These helpers provide support in the following methods: *Intermediation* and *Security Advice*.

Intermediation. Helpers may provide support by directly managing the security and privacy of their help receivers. In this case, they mediate the mobile phone interaction of their helpees by resolving their issues for them. This finding is similar to prior work in the Global South that has uncovered how their more tech-literate peers intermediate mobile usage for low-literate people [7, 97, 100]. We specifically uncover how intermediate interactions are enacted in the context of security and privacy.

In the context of security threats, participants enact intermediation by handing over their phones to their helpers, who then analyze and resolve the issue their helpees face. For example, F2_U and F10_D hand over their phones to their brother and husband, respectively, whenever they get a call from an unknown number and do not respond to such calls by themselves. Similarly, M2_U intermediated the scam call his co-worker received by directly checking the caller's phone number and later on blocking that number.

Phone usage and authentication issues are resolved by directly handing over the phone to the helper. The helper then resolves the problem by acting as tech support for the intended party. This method creates a sense of convenience for our participants, who would otherwise not be able to configure accounts themselves owing to their lack of literacy: *"If I don't understand anything on the phone, I ask them, 'Son, is it like this? How do I fix this, or what do I do with this?' [pointing to her phone] - actually, I don't do anything. I make them do it for me"* (F4_U). However, we also find that in some cases, the advisee may learn from the helper by observing their behavior, such as M4_U, who initially got his passwords set up by a friend in the IT staff but has slowly tried to learn how to set the password for Facebook up himself.

Security Advice. Regarding threats, helpers may provide security advice by describing incidents and recommending specific behaviors. This advice is shared through anecdotal stories of others' experiences [84, 85, 89, 90]. These stories contain negative experiences where the victim complied with the attacker and suffered a negative consequence, such as a loss of money or reputation. For example, when M3_U saw his co-worker downloading and entering his details on a similar third-party loan app he suffered from, he told him what he faced. He told his colleague that: *"They cause many problems, so you should not take any loans from them. Instead, ask for a loan from someone else. For example, from someone over here [at the university] that you would know of. So I told my colleague, 'Don't take help from the app; those people annoy you a lot.' I made him delete this app from his phone"* (M3_U). Advisors share these stories with advisees in person, either in one-to-one or social gatherings, or

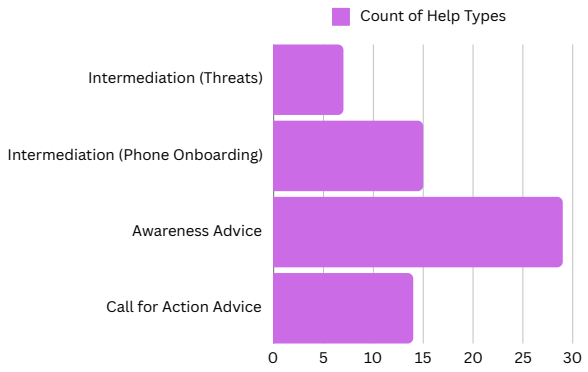

Figure 6: Frequency of Instances where Each Help Category was Used by Helpers.

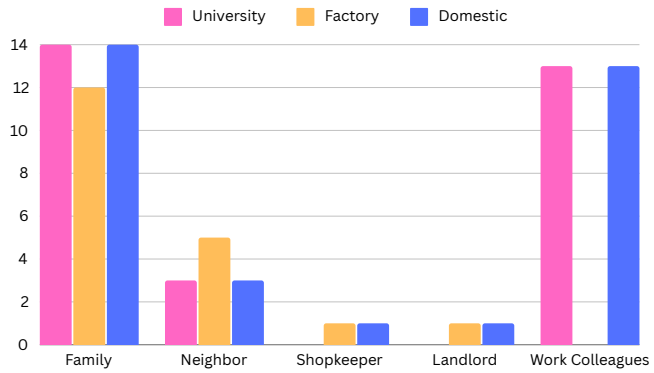

Figure 7: Frequency of Types of Helpers Across Work Environments Based on the Reported Interview Data.

through videos containing people's anecdotes shared on WhatsApp and social media.

We further categorize the security advice they shared into two sub-types based on when this advice was shared:

- **Call for Action Advice**: Advice is used as a defense mechanism during ongoing incidents or issues to help react to and resolve their ongoing challenges. For example, they may ask for help to identify whether the incoming unsolicited phone call is a fraud (F6_F from her mother and cousin) or to help reset their Facebook account's forgotten password (M5_F from his shopkeeper friend). Hence, advice is shared by helpers as a call for action, motivating help receivers to enact specific security behavior. For example, when M2_U's wife listened in on her husband's incoming scam call, she pleaded to her husband to immediately cut the call and block the number as she knew such calls were scams. This finding is similar to Razaq et al.'s work on mobile-based money fraud in Pakistan, where they find limiters (and enablers) within victims' social circles who guide people in reacting to ongoing scam calls [87].
- **Awareness Advice**: Helpers may share advice with family members, neighbors, and co-workers as they become aware of incidents in their immediate surroundings and learn secure behavior by witnessing/hearing others' stories. Sometimes, help receivers may also not seek support from their helpers and only reach out to them after it is too late when they have realized something has gone wrong. For example, M5_F's sister sent money to a scam caller without verifying the call with her brother and told her brother about the issue only after she realized that the scammer had blocked her number. In such cases, helpers shared advice retroactively after an incident had already occurred with the victims. Helpers may explain their personal experiences with such scammers and extortionists or discuss others' experiences they have witnessed or heard about in their social circles. The purpose of this advice is not to resolve any ongoing challenge; instead, it serves as a reminder to avoid similar incidents in the future. For example, F1_U learned how to stay alert for scam calls because her male cousin had faced a similar experience and shared it with his family at a gathering. Individuals may also instruct family members to follow particular behavior to avoid perceived threats. For example, M7_F has seemingly *"forbidden"* his wife and daughter from picking up calls from unknown numbers to avoid unwanted risks.

Figure 6 presents the frequency of each sub-type of help provided by helpers to illustrate the prevalence of each help category in our sample.

4.3 Helpers and Advice Sources (RQ 1)

Participants leveraged their existing social structures to obtain help and advice from their peers. They took help and advice from their family members, co-workers, neighborhood friends, shopkeepers, and landlords. Participants also got help from IT staff, employers, professors, and students at the workplace. Figure 7 presents the frequency of helpers based on their social relationships with their help receivers. Family members were the primary resource for seeking help and advice in threats and phone onboarding, followed by work colleagues (such as co-workers, employers, IT staff, professors, and students), neighborhood friends, shopkeepers, and landlords.

Family Members and Close Friends. All participants share advice with and from their family members. Women mostly obtain advice from male family members, such as brothers and husbands, and their children, both sons and daughters. Women may also discuss advice with other male or female relatives in family gatherings. Men obtain advice from other men in their family, such as younger brothers, nephews, and sons. Men also receive help from their neighborhood friends and trusted shopkeepers whom they meet in social settings. In some cases, men also obtain advice from their wives. These advice sources have (i) either faced similar incidents or (ii) have had a few years of formal education and are comfortable using technology.

Work Colleagues. We find intra-group differences among our participants based on their work environment. While all participants rely on family members as a baseline, they may or may not choose to discuss advice with their work colleagues, too. This decision is

Advice Category	Description	Example Quote
Avoid and Block	Do not pick up and/or block calls and texts received from unknown numbers.	*"If they [his wife and mother] get a call from an unknown number, I have forbidden them from picking it up." (M7_F).*
Cross-check and Verify	Investigate and verify the narratives of unsolicited callers to inquire about their validity. This also includes verifying the caller's phone number by other people.	*"First, look and see if the caller is legit or not. If he's asking money from you, try to check what he is doing with that money" (M1_U).*
Don't Share Personal Assets	Do not share phones, passwords, PIN codes, and other personal assets with strangers.	*"Don't give your phone to anyone. Even if a friend says, 'Can you give me your phone for a bit? I need to make a call,' don't give it to him" (M3_U).*
Online World is Unsafe	There is a lot of fake and vulgar content on the Internet. So, avoid complying with strangers incentivizing or threatening you.	*"If someone tries to take advantage of you, first of all, you should stay confident and know that you haven't done anything wrong. There is a lot of fake stuff out there. So don't focus on what the other person [on the call] is saying" (F3_U).*
Contact The Helper	Immediately reach out to the advisor/helper if you feel confused or scared when facing a negative incident.	*"I told my friend that she should ask me or reach out to someone else she trusts whenever she faces such calls" (F9_D).*

Table 4: Security advice regarding threat incidents disseminated and implemented by participants.

based on the affordances provided by the work environment to allow such discussions.

- **University Workers**: The university workers among our participants heavily rely on other members employed at the university, such as IT staff, students, professors, and other janitorial workers, to discuss phone-related issues. The university work environment allows janitorial workers to use phones at work, and eat and work together. Such a collaborative environment enables them to quickly discuss any unsolicited phone calls they receive at work and resolve such calls collectively. For example, M2_U helped another janitorial worker identify that his unsolicited phone call was a scam, as our participant had already received a similar call a few weeks prior. These janitorial workers also connect with the university IT staff, who, in their free time, help them onboard their phones by setting up passwords and accounts. These workers are also surrounded by students and professors who are generally approachable. For example, M4_U mentions having a trusted connection with a professor from the Computer Science department with whom he frequently shares family matters, financial troubles, and phone-related issues, including the scam call he had faced: *"He [the professor] keeps asking me if everything is okay in my life. So I am very close to him. So I thought if I hid from him what I faced, then I would be lying"* (M4_U). The advice they learn from the workplace is then shared amongst their family members and relatives.
- **Factory Workers**: In contrast, our factory workers do not rely on other work colleagues for help as they are not allowed to use phones at work, with many workers often leaving their phones at home for their families to use. Furthermore, the demanding job at the factory prevents them from having much free time to talk about non-work-related discussions and make friends: *"I don't have such friends here that are working with me, that I would go to their houses a lot... this does not happen"* (F7_F). Hence, they only rely solely on family members.
- **Domestic Workers**: Domestic workers get help from their employers, employers' families, and other workers in the same household. For example, M8_D, a driver for a family, took advice from his employer's sons for onboarding his Facebook account and then helped M9_D, a cleaner in the same house, set up his WhatsApp account. However, this reliance on employers and other employees depends on how comfortable they feel asking for help. For example, househelps F8_D and F10_D do not take advice from their workplace as they are new to the city and job, respectively, and have yet to make good connections with their employers and other nearby househelps. Instead, they fall back to relying solely on family members.

4.4 Advice Content (RQ 1)

Regarding threat incidents, we elicit the advice our participants learn and share with others. We categorized the security advice learned and disseminated by our participants into the following five categories: (i) *Avoid and Block*, (ii) *Cross-check and Verify*, (iii) *Don't Share Personal Assets*, (iv) *Online World is Unsafe*, and (v) *Contact The Helper*. Table 4 describes each category along with examples

	Work Environments		
Advice Category	University	Factory	Domestic
Avoid and Block	6	2	1
Cross-check and Verify	4	0	1
Don't Share Personal Assets	2	0	0
Online World is Unsafe	4	0	0
Contact The Helper	2	0	1

Table 5: Advice categories and the number of participants who shared that advice across work environments.

of participant quotes. Appendix C contains a complete list of all advice pieces uncovered in our qualitative study. Table 5 presents the participants who disseminated advice for each uncovered advice category. From this table, we found that the work environments in which participants were employed influenced which pieces of advice they learned and shared:

Work-environment Differences. We find that the work environment of our participants impacts what advice they learn and share. Primarily, university workers shared more nuanced and diverse advice than factory workers. All participants from all three work environments mentioned to *Avoid* and *Block* strangers as base measures to protect themselves from unsolicited contact: blocking or cutting calls from unknown numbers and not responding to unsolicited text messages. However, only the university and domestic workers mentioned further probing to *Cross-check* and *Verify* the pre-texts, narratives, and phone numbers of these unsolicited calls to inquire about their integrity. University workers also perceive the online world as unsafe for other people in their socioeconomic strata due to the prevalence of *"fake"* and *"vulgar"* content, causing them to stay apprehensive of unwanted, unsolicited contact. Hence, they advise others to remain cautious, not falter when threatened with allegations or incentivized with rewards, and stay confident in the face of adversaries: *"If someone runs away with your ear, you don't run after them; you first check your ear"* (F3_U using an analogy to advise on how to deal with allegations put forth by extortionists). Similarly, only university workers endorsed the practice of *Not Sharing Personal Assets*, such as passwords and phones, with strangers. University and domestic workers also offer to serve as long-term helpers for their advisees, allowing their advisees to contact them whenever they experience a threat: *"I told my brothers that they should never talk to these scammers and immediately cut the call. And if they can't understand what's happening [if they cannot determine whether the call is legit or fake], then I've told them to call me immediately"* (M4_U). Therefore, the variety and diversity of advice may depend on the work environment's affordances to allow technological discussions and collaboration among co-workers.

4.5 Motivations for Sharing Advice (RQ 2)

Our participants choose to participate in security advice dissemination (both giving and receiving advice) for the following reasons:

Perceived Group Competence and Sense of Goodwill. Participants share advice with others when they perceive them to be vulnerable in the face of threats due to their lack of education, income, experience with technology, or social support. Our participants believe that poor socioeconomic backgrounds may entice those around them to comply with scammers as they may fall for greed. Hence, they feel they must protect those around them and help them avoid the empty promises of attackers: *"So I told my friend that she should have asked me for advice. Because we folks [people in her socioeconomic strata] earn money after a lot of hard work, we can't give it to any scammers just like this"* (F9_D). However, attackers may also leverage participants' desire to help others to conduct attacks related to phone-sharing misuse and scams. Hence, participants advise others as they think victims may be too trusting of others due to a lack of digital experience and education. They believe education and digital experience are essential in understanding how technology operates as attackers may misuse their lack of knowledge to conduct fraud.

Similarly, participants believe that victims lack monetary or technological support from their families and friends, forcing them to rely on untrusted parties, including loan sharks and potential scammers, to try their luck. Hence, participants share advice with others as they believe that potential victims in participants' social circles have no one else to turn to: *"I think people need to have support systems to get help from their friends and family during hard times. Everyone needs such a support system when they need money or anything else. People should get [monetary and/or emotional] help from people they know, such as their relatives or friends, rather than from strangers and scammers. This way, they won't suffer from such scams and will avoid being victims. So we should use our connections to get help from our relatives or siblings. It's a better thing [than relying on strangers], in my opinion"* (M9_D). This lack of monetary support and technological experience makes people feel less confident when using phones due to the unknown nature of the digital landscape. This lack of confidence makes them highly vulnerable to threats that imply negative consequences, such as extortion, as they may not feel confident enough to know they haven't done anything wrong on their phones. For these reasons, our participants share advice with others as they wish to help others so they don't fall victim: *"I think we should share such incidents with others. Because if, God forbid, suppose something happens to you, then everyone else should know that 'Man, such kinds of things happen.' So, we should share stuff like this so that people can learn; there is nothing wrong with this"* (M3_U). Hence, our participants recognize that they are vulnerable due to their underprivileged background. As a result, they are motivated to share advice out of goodwill to help those around them alleviate their challenges.

Trust between Advisees and Advisors. Our participants share and receive help from others as they feel a sense of trust with their peers. For example, M8_D relies on his employers as he finds them to be respectful, welcoming, and comforting: *"Firstly, I can go and sit wherever I want in their house; no one forbids anything. Secondly, I am not rude to anyone, nor is anyone over here rude to me. Everyone will call me 'a brother', and I will address everyone as 'Sir or Ma'am.' So we give and get respect from these people"* (M8_D). Hence, they feel comfortable asking for help as they know their advisors would understand and empathize with their situation: *"Our helpers take it seriously and regret it if something bad happens to someone, like if he gets robbed or cheated. They say: 'Let's encourage him, brother, it's okay, but be careful from now on.'"* (M9_D).

4.6 Barriers for Sharing Advice (RQ 2)

We uncover the following barriers preventing our participants from disseminating advice to others.

Ridicule and Victim Blaming. Victim blaming is a major hurdle in advice-sharing as it prevents victims from sharing advice out of fear of being ridiculed, demotivated, and put to blame for what they have suffered. This reason is in contrast to the trust between peers mentioned in Section 4.5, as participants express that certain others make fun of their plight instead of showing empathy and support: *"They make fun of you if something bad happens to you. They talk about it happily and behave rudely with you"* (M9_D). Furthermore, others may often downplay victims' helplessness in the face of tragedy and instead criticize them by dictating what they should have done or how they should have behaved: *"They tell me, 'It is your fault for what you have faced.' They ask me [rhetorically], 'Who allowed you to follow along with the caller?' They say that 'If someone [from your family/friends] had allowed you [to comply with the attacker], only then you should have done this [send money to the caller]'"* (M9_D). Hence, they avoid sharing personal incidents with others as they have experienced sharing stories and being disappointed with the outcome of unwanted gossip and ridicule: *"For example, we [the interviewer and the participant] are very politely and respectfully talking to each other right now. But if, as soon as you go, I start talking bad stuff about you and gossiping about you. This sort of stuff happens to us"* (F4_U).

Work-Induced Challenges. Another major hurdle in advice sharing is the poor socioeconomic situation of our participants, which forces them to focus on sustaining a living and hence provides them with only minimal time to be socially involved with other people and, therefore, share advice. A participant shared, *"There is no time to share stuff, we have so much work. We don't even get time to straighten our backs."* (M7_F). The work environment contributes to limiting their social activity: We reiterate our factory workers' mode of operation where they are not allowed to use phones, collaborate with others, and have limited avenues to share advice in the workplace. Similarly, participants new to the city or the work environment do not feel comfortable discussing their personal/family incidents with others. Hence, advice sharing may not be prevalent with those outside their family as some participants exhibit a sense of privacy when it comes to family matters: *"You know, there are a 100 things that happen at home that one cannot tell to anyone so simply like this"* (M1_U).

Family Dynamics. We uncover that advice sharing may be limited between family members as well; breadwinners of households, such as M4_U, have a notion of being the head of the household and hence do not wish to share actual negative experiences they have faced to avoid their family members from being demotivated: *"I am the oldest brother. I don't want my younger brothers to get worried and think negatively, that 'If he [the participant] can experience something so bad, then what will happen to us.' So, I try to keep my brothers positive"* (M4_U).

4.7 Effectiveness of Advice Sharing

Finally, we explore the effectiveness of community advice sharing and intermediation by understanding when these mechanisms work or fail to deliver help.

4.7.1 Failed Advice Mechanisms. Advice sharing cannot deliver help promptly and effectively due to the following reasons:

Incorrect Advice and Intermediation. Attackers' narratives may delude the potential advisors in our victims' social circles [87]. Similarly, helpers may fail to provide correct intermediation and support during security-related incidents. As a result, people who could help intervene in threats may fall for the scammers' narratives and allow their advisees to comply with attackers [87]. Hence, they may provide incorrect advice, leading to negative consequences. For example, when F3_U got a scam call offering her prize money in exchange for a small transaction fee, she asked her mother, whom she usually contacted for advice regarding her matters, about the call's legitimacy. However, her mother also fell for the scam narrative and allowed her daughter to send the transaction fee money to the scammer.

Advice Rejection. Sometimes, advice is shared but not implemented as victims' poor socioeconomic situation forces them to decide that the reward scammers promise is worth the potential risks. For example, M8_D's friend complied with the scammer despite his advisor, an educated colleague, warning him not to comply with the caller: *"Our senior [colleague] told my work friend that such calls are usually fraud, so he advised my friend not to comply with the unknown caller. But my friend ignored the senior colleague's words and transferred the money to the caller. After that, the caller cut the call and blocked my friend's number. My friend tried calling the number again, but the caller's number was switched off; that's how I think the caller blocked him. My friend went back to the senior colleague and pleaded to him, saying 'Sir, his number has been switched off, please try calling him.' The senior said, 'My friend, I already told you that this is a fraud. But you didn't listen. Now I can't do anything.'"* (M8_D). In extreme cases, we uncover that victims may not utilize advice sources as they may hide their issues from potential advisors, who could have otherwise intervened on behalf of victims. For example, M9_D's father hid the scam call he was facing from the shopkeeper who queried about the unusual nature of his transaction: *"Masha'Allah, everyone in the market knew my father. So the shopkeeper at the mobile shop asked my father, 'Uncle, why are you taking these cards? Like, you always get load credit from me.' The shopkeeper knew my dad and realized something was off. The shopkeeper was literate and had a mobile phone shop, so he understood such things. But my father hid it from him and said, 'No, son, we need the cards right now; therefore, I am taking it'"* (M9_D).

4.7.2 Positive Outcomes. When the above-mentioned challenges do not interplay, advice-sharing shows the potential for working in favor of our participants, as we uncover examples where targets of threats implemented the advice/help from their advisors during the ongoing incident and did not suffer any negative consequences. For example, F8_D did not fall for a fraud message she received as her husband, who had experienced a similar scam a few weeks ago, advised her to stay vigilant. Fifteen reported incidents in our

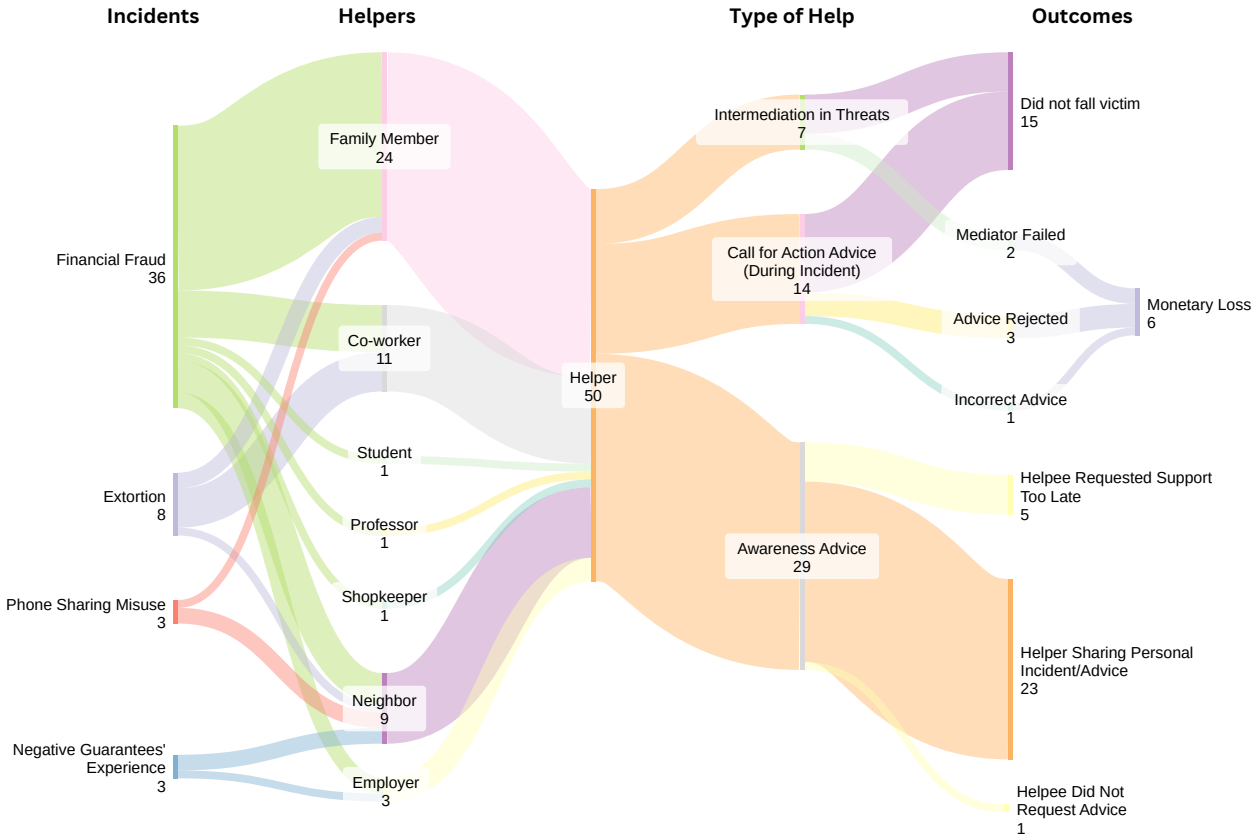

Figure 8: Overview of Participants' Help Mechanisms in Security-Related Threats.

data concluded with this positive outcome, where help receivers (i) recalled and/or obtained and (ii) implemented correct advice and support from their helpers.

4.8 Key Takeaways

Our results highlight the extreme social embeddedness of security-related practices of low socioeconomic Pakistanis. In particular, we uncover how intermediated interactions and community advice sharing shape how participants enact and deal with security. Figure 8 summarizes these findings for the uncovered security-related threats, and Figure 9 presents analogous findings for the uncovered phone onboarding and usage practices. The figures show how helpers from participants' various social circles, such as family, friends, and co-workers, provided support through intermediated interactions and security advice. Participants then used this help to (i) onboard and use technology and (ii) raise awareness and safeguard against security-related threats. While participants were motivated to leverage these help mechanisms, sometimes, the effectiveness of this help was challenged, leading to negative experiences.

5 DISCUSSION

5.1 Reflections on Advice

We uncovered five categories of security advice learned and disseminated by our participants (see Table 4). Similar to other at-risk populations [107], our participants shared and adopted social protective strategies and distancing behaviors to protect themselves from digital threats. We uncovered how such protective strategies are disseminated and employed in the low socioeconomic Pakistani context. This advice differs from the advice discussed in more Western and educated contexts that also discuss technical behaviors such as stronger passwords, multi-factor authentication, software updates, privacy controls, and more [22, 48, 57, 89, 93].

We found that the threat landscape for our participants relied more on exploiting human weaknesses rather than technological vulnerabilities. For example, similar to prior work on financially stressed loan app users in Kenya and India [71, 86], we found that participants may sign up for highly exploitative loan payment plans and later suffer from unwanted extortion by loan sharks. While social engineering and financial fraud exist in Western contexts, their citizens also discuss other cyber incidents, such as hacking, malware, and data breaches [84, 85, 109]. However, such incidents are not of concern to our participants, as they did not mention them despite our interview protocol being open to diverse threats and negative experiences. For example, we explicitly prompted them on threats related to *"hacking"*, but we did not uncover any concrete instances.

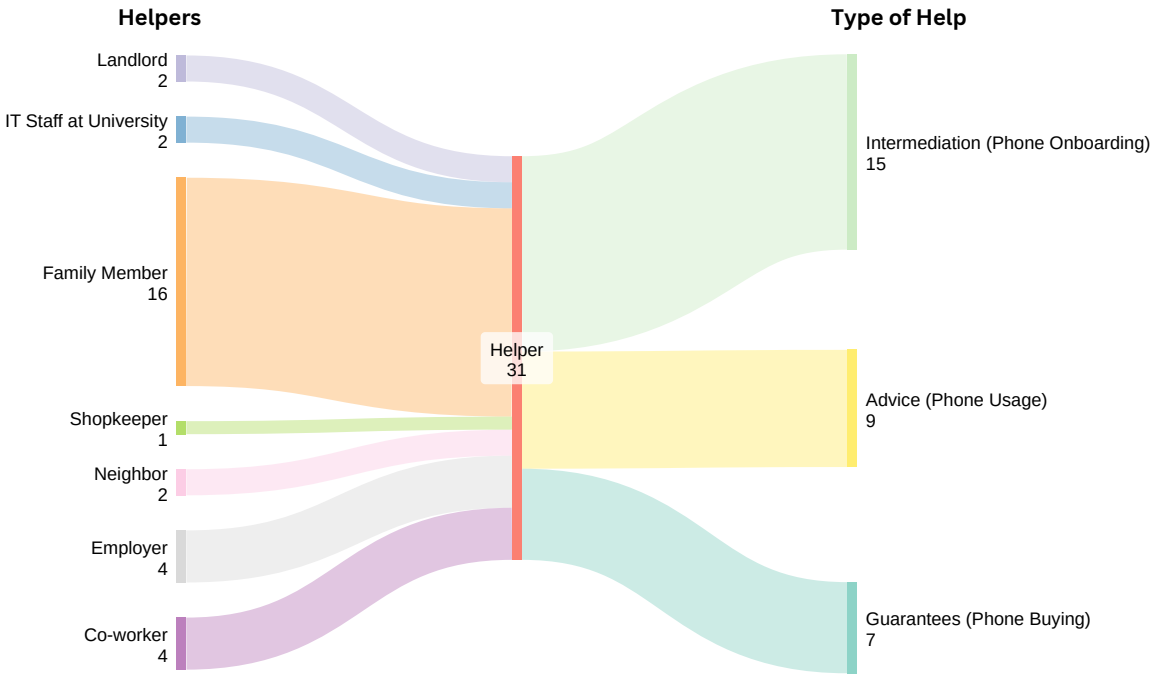

Figure 9: Overview of Participants' Help Mechanisms in Phone Onboarding.

These differences in perceived and experienced threats raise the question on the effectiveness of standardized protection mechanisms. We argue that security advice disseminated in other contexts may not yet be relevant and transferrable to our participants' threat landscape. Protecting this low socioeconomic population with solely technical security solutions is hard, which is what security advice in prior literature primarily focuses on. For example, participants may give in to demands from scammers despite having enabled secure practices, such as One-Time-Passwords (OTP), as these technical solutions do not prevent participants from consciously making insecure decisions, such as deliberately giving their OTP to a scammer over a phone call. Therefore, while participants may benefit from the technical behaviors recommended by security experts, future work must first focus on (i) understanding participants' mental models on how they assess threats and risks and (ii) helping raise participants' awareness on how attackers operate by curating context-specific security advice. Such efforts are a necessary first step to help participants adopt social and technical protective strategies that are relevant and applicable.

5.2 Factors Influencing the Advice Landscape

We discuss the following factors that help explain how and why low socioeconomic people take part in security advice sharing. We also discuss how these factors interact to create additional challenges in advice sharing for the target population. Future work must validate these factors.

5.2.1 Socioeconomic Status.

Poor Financial Situation. The poor socioeconomic situation of our participants negatively impacts how they are embedded in the digital landscape as it inhibits them from accessing basic mobile services and makes them vulnerable in the face of threats. Lacking financial stability means most participants work minimum-wage jobs and live paycheck to paycheck. Their situation contrasts those populations that prior literature in the Pakistani context has studied, such as younger adults [16], stay-at-home women [12], or content creators [43], who are relatively financially stable. Hence, our low socioeconomic participants are especially vulnerable to threats that rely on leveraging their poor financial situation by enticing them with easy-return loans or lottery prizes. Similarly, risks threatening their economic security, such as demanding immediate payback on loans or extorting vouchers to pay back installments of other people, are perceived as highly dangerous by participants. Hence, our participants focused more on financial challenges and the associated risks with their poor economic situation. Therefore, a primary motivation in obtaining advice was not just staying safe or secure in the digital world; rather, they sought help to alleviate their economic situation. However, their financial situation caused more harm than good. The main reason for compliance with attackers was that when it came to financial matters, our participants were so worried about losing their money or so invested in earning a few extra bucks that they ignored the potential consequences of complying with strangers. This issue made them amenable to taking risks, which made them prone to falling for scam calls and extortion schemes that played on their financial vulnerability. Their financial situation also caused them to reject advice or not utilize their advice sources; for example, M8_D's friend and M9_D's father rejected the advice obtained by their educated colleague and hid their issue from their helper, respectively. They did this as the apparent reward their callers promised seemed worth the risk of complying with

a stranger, not knowing they were being scammed until it was too late. This finding provides another facet to prior work on why advice is rejected, as victims in our socioeconomic context, owing to their poor financial situation, may not accurately determine the risk of complying with attackers when it comes to matters related to money [12, 37, 89, 91, 115].

Lack of Education and Literacy. A lack of formal education makes most existing applications and user interfaces unusable for our participants, as they are primarily designed as text-based interfaces requiring basic abilities to read and write in English, preventing them from gaining technological experience [66, 67]. In the context of security and privacy, our participants fail to understand and navigate authentication mechanisms integrated into applications, causing them to rely on intermediated interactions with more literate helpers to make and manage user accounts.

Their lack of technological experience makes them vulnerable to threats as they lack the skills to identify potential risks. Instead, our participants trusted the advice obtained by their helpers as they perceived them to be competent (their helpers either had higher levels of literacy or had faced similar threats [77]). However, participants did not self-report to judge the quality or utility of the advice they received and implemented, which we attribute to a lack of digital education and experience. We believe this is an important limitation in their advice mechanisms as these helpers may provide incorrect advice. For example, in line with prior work [87], we uncovered that helpers in our participants' social circles might also fall for scammers' narratives, allowing their advisees to comply with attackers' demands.

Fraudsters may exploit the lack of awareness among illiterate users to conduct fraud by leveraging mechanisms designed to help them; for example, Over-The-Counter (OTC) transactions at shops, which were designed to help illiterate people make financial payments and pay bills, are also misused to defraud these people [87]. Prior work on socioeconomically disadvantaged Americans uncovers how they struggle to protect themselves from scams when navigating the online world, forcing them to resign, fear, and avoid technology, and have perceived low self-efficacy when navigating the online world [106]. Hence, technological interventions may not be adequate to help reduce their risks, as they may only add fuel to the fire. As a countermeasure, our our participants implement social protective strategies through support, advice, and intermediation from their more experienced helpers to navigate their mobile phones and associated risks.

5.2.2 Social Embeddedness. We discuss the following aspects as facets of social advice mechanisms:

Class-based Society. Pakistanis with low socioeconomic status lack access to education, income, healthcare, and social and political participation [45]. Anecdotally, they may not even eat the same food as upper-class citizens [105]. Pakistan is a highly class-based society, where groups from different socioeconomic backgrounds live very different lives and often do not intermingle, leaving less privileged people socially excluded and highly marginalized as they may not interact with upper-class citizens and lack access to basic resources [1, 36, 45, 78, 81, 102]. This income inequality and divide may bring people in the lower socioeconomic strata closer together when dealing with security and privacy, leading to high interpersonal trust and community belonging as they have no one to help them except themselves: *"Us small people think more about this [helping others in their neighborhood]. Since we are small people, we think more about the poor. But the richer folks don't think like this for us. They say, 'yeah, okay, we'll do something for them, not a big deal.'"* (M1_U). Prior work has uncovered how such community belonging, shared identity, and interpersonal trust foster information sharing and emotional support in security and privacy [58, 64].

However, we uncover how attackers conduct social engineering attacks [49, 62, 83, 87, 101] in the low socioeconomic Pakistani context by misusing people's trust to conduct scam calls and phone-sharing misuse. Malicious actors within victims' social circles may also abuse their social connections to deceive victims into paying installments on their behalf and extort female relatives. Such threats lead to mental distress, financial losses, and reputational harm for victims. Hence, these issues may decrease confidence, trust, and motivation in utilizing existing social structures for advice sharing.

Culture. Family, religious, and patriarchal values in male dominated societies like Pakistan impact women's agency in public and digital spaces, forcing their online safety, privacy behaviors, and technological decisions to depend on what men decide for them [56, 76, 95, 97]. This concept of paternalism leads to potential risks and privacy concerns with sharing personal information, threat experiences, and phones with (mostly male) family members, shopkeepers, and peers [4, 5, 103]. One such risk that we uncover is victim blaming and ridicule, where victims of threats were demotivated to share advice about their negative incidents out of fear of being blamed or ridiculed for their experiences. Victim blaming may be a consequence of paternalism, as people may choose to ignore the complexity of the problems victims face and instead blame them for not behaving as expected to the norm, leading to their suffering [82]. Victim blaming has also previously been explored in the Global South, especially how it limits seeking both formal and informal help in cybercrime, harassment, and gender-based violence as victims (mostly women) fear a lack of support from their social circles and associate a social stigma against official reporting mechanisms [16, 43, 74, 95]. We complement prior work by highlighting how it inhibits advice sharing with advisees. However, victim blaming can have more serious consequences. The Pakistani sociocultural norms value the honor and piety of women; however, when this honor is questioned, women themselves are often at the receiving end of negative consequences [16, 43, 55, 95]. In some cases, these negative consequences may even lead to harassment and death, see the case of Qandeel Baloch's "honor-killing" as an example [32]. Such factors are highly relevant to security advice mechanisms as they may lead to limited use of existing social structures for advice sharing.

Prior work has endorsed an interesting countermeasure against paternalism that involves utilizing women-only digital safe spaces, where at-risk users can anonymously and safely discuss socially taboo topics, such as negative threat experiences [14, 74, 113]. However, we argue that such digital safe spaces may be inaccessible for our target population, who face additional challenges of having a high culture of phone sharing and requiring considerable intermediation from helpers in accessing and using technology, potentially

rendering their anonymity and privacy ineffective in any digital solution.

Work Environments. We identify that the work environment brings low socioeconomic people together in the Pakistani context. This finding was not reflected in prior work by Redmiles et al. [89, 90], who found that low socioeconomic Americans tended to take advice from family, friends, and service providers, while high socioeconomic Americans took advice from the workplace. University workers, both men and women, were allowed more avenues to collaborate and were allowed to use phones at the workplace. Our university and domestic workers interacted with more literate peers, showing how their unique environment helped bridge the gap between two disparate socioeconomic groups (employers, IT staff, professors, students, and blue-collar workers). Such affordances allowed them to help each other during security incidents and intermediate phone authentication. Being in the company of more educated people helped alleviate their situation as they could always ask them for advice. In contrast, these benefits were unavailable for factory workers who had to rely solely on family members and peers outside their work environment. Owing to limited advice avenues and the low technological experience of their social circles, the advice shared and learned by factory workers was less diverse than that of other workers.

5.3 Recommendations and Solutions

We place our work in the context of low socioeconomic populations in the Global South, where prior work (in addition to our study) has uncovered re-emerging patterns of phone sharing and a reliance on peers to intermediate and guide phone usage (a few examples are studies in Pakistan, Bangladesh, and India [3, 4, 56, 76, 96, 97]). Together with prior work, we find that threat landscape in these developing contexts is unique as it exploits people's financial vulnerability, societal expectations, and sociocultural norms [25, 43, 71, 86, 103]. Context-specific advice and technology must be designed to help alleviate the security and privacy challenges of low socioeconomic populations. We present the following actionable recommendations as a starting point for the community. These recommendations address how (i) advice content, (ii) advice dissemination, and (iii) security-related technology should be designed for our target population.

5.3.1 Advice Content. Prior work has argued for rethinking how privacy-preserving technology should be designed for the Global South context [4, 16, 76, 96]. We make an analogous argument for security advice: advice needs to be carefully designed and delivered in a manner that respects the sociocultural norms of the country, is accessible to the low literate context, and is sensitive to the shifting threat landscape. Due to the reasons explained in Section 5.1, mere translation of security advice from Western contexts [22, 57, 84, 85, 93] into native languages is not the way forward. For example, a woman in the low socioeconomic Pakistani context, who is forced to share phones with her family members, either due to the patriarchal norms or merely because she cannot afford a personal phone, cannot be expected to challenge the status quo and implement the behavior of not sharing personal information and devices with others. Instead, advice should be more nuanced to effectively and appropriately navigate the societal challenges low socioeconomic citizens face. For this purpose, we call for collaborating with local security experts and end-users to systematically generate security advice for this context. We suggest considering the sociocultural context, such as gender, religion, literacy, and financial constraints and expectations, when curating advice.

5.3.2 Advice Dissemination.

Leveraging Work Environments. Considering how much the workplace environment shapes employees' phone use and knowledge-sharing habits, we suggest that organizations make it easier for blue-collar employees to share advice and incidents. As Razaq et al. have suggested, raising awareness about social engineering attacks through formal means is crucial [87]. We build on this idea by recommending workplaces host workshops or similar events to educate employees about security threats and update them on the latest security issues. These sessions should focus on building a sense of community and empathy among employees, which can help reduce barriers to sharing security advice, such as victim-blaming. These sessions should also be gender-segregated, discouraging paternalism and encouraging women to discuss their issues freely without fear of being victimized [14, 74, 113]. The advice disseminated must be regularly evaluated and updated to address new threats and challenges. Otherwise, their advice may be rendered obsolete as threats become more complex. Such initiatives can provide an avenue for interaction between employees of different social classes and bring them together, leveraging social structures to improve the dissemination of security advice.

Leveraging Short Form Video Content. Video-based content, such as on TikTok, Facebook, and YouTube, was accessible to our participants as they did not require specific literacy skills to understand the content. Searching for these videos was also made easy, either by the speech-to-text functionality on YouTube or the automated recommendation system on TikTok and Facebook. We recommend utilizing this existing channel to disseminate security advice. This can be achieved by collaborating with local content creators to generate short-form videos to guide users on secure digital behaviors. Such videos would be appropriate for the local context as the micro-influencers would already be well-integrated with their followers, speaking in the native language and communicating in a culturally-appropriate manner. Prior work has explored the impactful potential of TikTok's short-form videos on user engagement [114], and we suggest utilizing this as a mechanism to disseminate security advice.

5.3.3 Digital Recommendations. Like many previous security and privacy studies in the Global South [76, 94, 96, 103], we recommend focusing on making security technology more accessible for low socioeconomic users. However, breaking down barriers to phone usage for low socioeconomic users will expose them to more threats, such as hacking and account compromise, which are not common currently, so we need to be careful when designing for this vulnerable population. Hence, we advocate for more profound, comprehensive changes, as making only one feature accessible won't address the deeply rooted accessibility challenges. A more holistic approach in context-sensitive design is needed to effectively address these issues for low socioeconomic populations. We present two

avenues where technology can be redesigned as a starting point for the community.

Device Onboarding. Our findings showed that many participants struggled with the phone and app onboarding process, often relying on others due to its lack of accessibility. Such device onboarding can be made more accessible by having a conversational mode of interaction that emulates the current *"intermediation"* mechanism that participants employ to onboard their phones. Similarly, voice-based elements and native language should be supported by default for this context. We recommend future co-design studies to leverage our findings, including incorporating lessons in design by prior work in the HCI and ICT4D domains on similar populations (such as [66–68]), to make such authentication mechanisms more accessible.

Scam Call Content Warnings. In 2024, Google launched device-level protection to automatically determine a call's legitimacy by analyzing the content using generative AI [20]. The algorithm analyzes the caller's narrative and displays warnings as visual elements in English during the suspicious call, similar to phishing email content warnings on Gmail [20, 50]. While this mechanism is still not fully deployed on all devices, it is a step in the right direction to mitigate the rising threat of telephone scams. However, the usability of this mechanism in the low socioeconomic context is questionable, where users may have difficulty understanding these warnings. Similarly, empirical testing needs to be conducted to determine how well-suited these warnings are for localized scam calls such as in Pakistan, where less training data may be available to make accurate judgements on the call's legitimacy. Future work needs to evaluate the usability and design of automated content warnings for scam calls in the Global South. Future work also needs to assess the privacy implications of such AI-enabled detection mechanisms.

6 CONCLUSION

Low socioeconomic people are at high risk of security and privacy threats as attackers leverage their financial vulnerability and the trust they have with other community members. As a countermeasure, low socioeconomic Pakistanis utilize their existing social structures to obtain advice and intermediation in onboarding their phones, navigating threats, and staying safe. While these advice mechanisms are limited in their efficacy owing to the poor social standing and sociocultural norms of low socioeconomic citizens, they may be the only support these people have. Hence, future research and design must study how to utilize the uncovered potential of security advice mechanisms for the most vulnerable in Pakistani society for more inclusive security design.

ACKNOWLEDGMENTS

We thank the reviewers for their invaluable feedback, which helped us improve our paper. We thank our friends Shafay Kashif and Ushna Saeed for helping us recruit participants. We thank Carolyn Guthoff for her input. Lastly, we thank our participants for taking part in our study.

REFERENCES

[1] Sayyed Khawar Abbas, Hafiz Ali Hassan, Jawad Asif, and Faiqa Zainab. 2018. How income level distribution responds to poverty: Empirical evidence from Pakistan. *Global Scientific Journals* 6, 3 (2018), 131–142.

[2] Abu Dhabi Department of Education and Knowledge. [n. d.]. Pakistani Curriculum. https://www.adek.gov.ae/en/Education-System/Private-Schools/Curriculum/Pakistani-Curriculum Accessed: 2024-08-11.

[3] Syed Ishtiaque Ahmed, Shion Guha, Md Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. 2016. Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*. 1–10.

[4] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital privacy challenges with shared mobile phone use in Bangladesh. *Proceedings of the ACM on Human-computer Interaction* 1, CSCW (2017), 1–20.

[5] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 906–918.

[6] Syed Ishtiaque Ahmed, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. " Everyone Has Some Personal Stuff" Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[7] Syed Ishtiaque Ahmed, Maruf Hasan Zaber, Mehrab Bin Morshed, Md Habibullah Bin Ismail, Dan Cosley, and Steven J Jackson. 2015. Suhrid: A collaborative mobile phone interface for low literate people. In *Proceedings of the 2015 Annual Symposium on Computing for Development*. 95–103.

[8] Mamtaj Akter, Leena Alghamdi, Jess Kropczynski, Heather Richter Lipford, and Pamela J Wisniewski. 2023. 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*. 1–7.

[9] Mamtaj Akter, Amy J Godfrey, Jess Kropczynski, Heather R Lipford, and Pamela J Wisniewski. 2022. From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals? *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (2022), 1–28.

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

[11] Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, MA Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. 2020. We don't give a second thought before providing our information: understanding users' perceptions of information collection by apps in Urban Bangladesh. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies*. 32–43.

[12] Elham Al Qahtani, Yousra Javed, Heather Lipford, and Mohamed Shehab. 2020. Do women in conservative societies (not) follow smartphone security advice? a case study of saudi arabia and pakistan. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 150–159.

[13] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. 2015. Security practices for households bank customers in the Kingdom of Saudi Arabia. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 297–308.

[14] Tawfiq Ammari, Momina Nofal, Mustafa Naseem, and Maryam Mustafa. 2022. Moderation as empowerment: Creating and managing women-only digital safe spaces. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–36.

[15] ARY News. 2024. *Online Loan Apps: Here's How Citizens Are Blackmailed.* https://arynews.tv/online-loan-apps-heres-how-citizens-are-blackmailed/ Accessed: 2024-08-08.

[16] Afaq Ashraf, Cornelius J König, Mobin Javed, Maryam Mustafa, et al. 2023. " Stalking is immoral but not illegal": Understanding Security, Cyber Crimes and Threats in Pakistan. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 37–56.

[17] Barwaqt Fintec. 2024. Barwaqt Fintec Application Process. https://www.barwaqtfintec.com/ApplicationProcess/ Accessed: 2024-11-18.

[18] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. 2024. Sok: Safer digital-safety research involving at-risk users. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 635–654.

[19] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. 2022. " Adulthood is trying each of the same six passwords that you use for everything": The Scarcity and Ambiguity of Security Advice on Social Media. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–27.

[20] Google Security Blog. 2024. Safer with Google: New intelligent, real-time protections on Android to keep you safe. https://security.googleblog.com/2024/11/new-real-time-protections-on-Android.html Accessed: 2024-11-18.

[21] Billie Bonevski, Madeleine Randell, Chris Paul, Kathy Chapman, Laura Twyman, Jamie Bryant, Irena Brozek, and Clare Hughes. 2014. Reaching the hard-to-reach: a systematic review of strategies for improving health and medical research with socially disadvantaged groups. *BMC medical research methodology* 14 (2014), 1–29.

[22] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No one can hack my mind revisiting a study on expert and {Non-Expert} security practices and advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 117–136.

[23] John M Carroll, Mary Beth Rosson, and Jingying Zhou. 2005. Collective efficacy as a measure of community. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1–10.

[24] Kathy Charmaz. 2006. *Constructing grounded theory: A practical guide through qualitative analysis*. sage.

[25] Yan Chen and Fatemeh Mariam Zahedi. 2016. Individuals' internet security perceptions and behaviors. *Mis Quarterly* 40, 1 (2016), 205–222.

[26] Chhaya Chouhan, Christy M LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J Wisniewski. 2019. Co-designing for community oversight: Helping people make privacy and security decisions together. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–31.

[27] Kovila PL Coopamootoo and Magdalene Ng. 2023. "{Un-Equal} Online Safety?" A Gender Analysis of Security and Privacy Protection Advice and Behaviour Patterns. In *32nd USENIX Security Symposium (USENIX Security 23)*. 5611–5628.

[28] Juliet M Corbin and Anselm Strauss. 1990. Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology* 13, 1 (1990), 3–21.

[29] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A typology of perceived triggers for {End-User} security and privacy behaviors. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 97–115.

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

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

[32] Dawn News. 2016. Qandeel Baloch murdered by brother in Multan: police. https://www.dawn.com/news/1271213 Accessed: 2024-08-25.

[33] Jayati Dev, Pablo Moriano, and L Jean Camp. 2020. Lessons learnt from comparing {WhatsApp} privacy concerns across saudi and indian populations. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 81–97.

[34] Digital Rights Foundation. 2021. *DRF Cyber Harassment Helpline Annual Report 2021*. Technical Report. Digital Rights Foundation, Lahore, Pakistan. https://digitalrightsfoundation.pk/wp-content/uploads/2022/05/helpline-annual-report-2021-1.pdf

[35] Employers Federation of Pakistan. 2023. Punjab Minimum Wages Notification 2023. https://efp.org.pk/punjab-minimum-wages-notification-2023/ Accessed: 2024-07-16.

[36] Express Tribune. 2019. Pakistan's Rich and Poor Live in Different Countries. https://tribune.com.pk/story/2114456/pakistans-rich-poor-live-different-countries Accessed: 2024-08-23.

[37] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 59–75.

[38] Federal Board of Revenue. 2022. Fraudulent Apps Gathering Personal Data (Advisory No. 18). https://download1.fbr.gov.pk/Docs/2022526135150333FraudulentAppsgatheringpersonaldata(advisoryno.18).pdf Accessed: 2024-08-14.

[39] Vicki S Freimuth and Wendy Mettger. 1990. Is there a hard-to-reach audience? *Public health reports* 105, 3 (1990), 232.

[40] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. 2019. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 79–95.

[41] Tricia K Gatlin and Michael J Johnson. 2017. Two case examples of reaching the hard-to-reach: Low income minority and LGBT individuals. *Journal of Health Disparities Research and Practice* 10, 3 (2017), 11.

[42] Government of Pakistan. [n. d.]. Benazir Income Support Programme. https://bisp.gov.pk/ Accessed: 2024-08-03.

[43] Lea Gröber, Waleed Arshad, Angelica Goetzen, Elissa M Redmiles, Maryam Mustafa, Katharina Krombholz, et al. 2024. "I chose to fight, be brave, and to deal with it": Threat Experiences and Security Practices of Pakistani Content Creators. (2024).

[44] GSMA. 2024. The Mobile Economy Asia Pacific 2024. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/07/240724-Mobile-Economy-Asia-Pacific-2024-FINAL.pdf Accessed: 2024-08-08.

[45] Abdul Hameed and Zara Qaiser. 2019. Estimating social exclusion in rural Pakistan: A contribution to social development policies. *Business & Economic Review* 11, 1 (2019), 103–122.

[46] Eszter Hargittai. 2001. Second-level digital divide: Mapping differences in people's online skills. *arXiv preprint cs/0109068* (2001).

[47] Eszter Hargittai. 2003. The digital divide and what to do about it. *New economy handbook* 2003 (2003), 821–839.

[48] Ayako A Hasegawa, Naomi Yamashita, Tatsuya Mori, Daisuke Inoue, and Mitsuaki Akiyama. 2022. Understanding {Non-Experts'} Security-and {Privacy-Related} Questions on a {Q&A} Site. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 39–56.

[49] Sumair Ijaz Hashmi, Niklas George, Eimaan Saqib, Fatima Ali, Nawaal Siddique, Shafay Kashif, Shahzaib Ali, Nida Ul Habib Bajwa, and Mobin Javed. 2023. Training Users to Recognize Persuasion Techniques in Vishing Calls. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–8.

[50] Google Pixel Phone Help. 2024. Learn more about the new Scam Detection beta. https://support.google.com/pixelphone/thread/307725284/learn-more-about-the-new-scam-detection-beta?hl=en Accessed: 2024-11-18.

[51] Monique Hennink and Bonnie N Kaiser. 2022. Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social science & medicine* 292 (2022), 114523.

[52] Monique M Hennink, Bonnie N Kaiser, and Vincent C Marconi. 2017. Code saturation versus meaning saturation: how many interviews are enough? *Qualitative health research* 27, 4 (2017), 591–608.

[53] Joseph Henrich, Steven J Heine, and Ara Norenzayan. 2010. The weirdest people in the world? *Behavioral and brain sciences* 33, 2-3 (2010), 61–83.

[54] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. 2023. A world full of privacy and security (mis) conceptions? Findings of a representative survey in 12 countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–23.

[55] Qian Hongdao, Muhammad Bilawal Khaskheli, Hafiz Abdul Rehman Saleem, Jonathan Gsell Mapa, and Sughra Bibi. 2018. Honor killing phenomena in Pakistan. *JL Pol'y & Globalization* 73 (2018), 169.

[56] Samia Ibtasam, Lubna Razaq, Maryam Ayub, Jennifer R Webster, Syed Ishtiaque Ahmed, and Richard Anderson. 2019. " My cousin bought the phone for me. I never go to mobile shops." The Role of Family in Women's Technological Inclusion in Islamic Culture. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–33.

[57] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. {"... No} one Can Hack My {Mind"}: Comparing Expert and {Non-Expert} Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 327–346.

[58] Aarti Israni, Nicole B Ellison, and Tawanna R Dillahunt. 2021. 'A Library of People' Online Resource-Seeking in Low-Income Communities. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–28.

[59] Margaret C Jack, Pang Sovannaroth, and Nicola Dell. 2019. " Privacy is not a concept, but a way of dealing with life" Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–19.

[60] George P Knight, Mark W Roosa, and Adriana J Umaña-Taylor. 2009. *Studying ethnic minority and economically disadvantaged populations: Methodological challenges and best practices*. American Psychological Association.

[61] Sandjar Kozubaev, Fernando Rochaix, Carl DiSalvo, and Christopher A Le Dantec. 2019. Spaces and traces: Implications of smart technology in public housing. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[62] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and applications* 22 (2015), 113–122.

[63] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J Wisniewski. 2021. Towards building community collective efficacy for managing digital privacy and security within older adult communities. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–27.

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

[65] Mary Madden. 2017. Privacy, Security, and Digital Inequality. *Data & Society* (2017).

[66] Indrani Medhi, Somani Patnaik, Emma Brunskill, SN Nagasena Gautama, William Thies, and Kentaro Toyama. 2011. Designing mobile interfaces for novice and low-literacy users. *ACM Transactions on Computer-Human Interaction (TOCHI)* 18, 1 (2011), 1–28.

[67] Indrani Medhi, Aman Sagar, and Kentaro Toyama. 2006. Text-free user interfaces for illiterate and semi-literate users. In *2006 international conference on information and communication technologies and development*. IEEE, 72–82.

[68] Hamid Mehmood, Tallal Ahmad, Lubna Razaq, Shrirang Mare, Maryem Zafar Usmani, Richard Anderson, and Agha Ali Raza. 2019. Towards digitization of collaborative savings among low-income groups. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–30.

[69] Ministry of Federal Education and Professional Training, Pakistan. 2018. National Education Policy Framework 2018. https://www.mofept.gov.pk/SiteImage/Policy/National%20Eductaion%20Policy%20Framework%202018%20Final.pdf Accessed: 2024-08-11.

[70] Wanda Montalvo and Elaine Larson. 2014. Participant comprehension of research for which they volunteer: a systematic review. *Journal of Nursing Scholarship* 46, 6 (2014), 423–431.

[71] Collins W Munyendo, Yasemin Acar, and Adam J Aviv. 2022. "desperate times call for desperate measures": User concerns with mobile loan apps in kenya. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2304–2319.

[72] Collins W Munyendo, Yasemin Acar, and Adam J Aviv. 2023. " In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 570–587.

[73] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–24.

[74] Mustafa Naseem, Fouzia Younas, and Maryam Mustafa. 2020. Designing digital safe spaces for peer support and connectivity in patriarchal contexts. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–24.

[75] National Database and Registration Authority, Pakistan. 2024. National Database and Registration Authority (NADRA). https://www.nadra.gov.pk Accessed: 2024-11-18.

[76] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. 2022. " Ask this from the person who has private stuff": Privacy Perceptions, Behaviours and Beliefs Beyond WEIRD. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–17.

[77] Norbert Nthala and Ivan Flechais. 2018. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 63–82.

[78] Pakistan Bureau of Statistics, Government of Pakistan. [n. d.]. Pakistan Labour Force Survey 2020-21. https://www.pbs.gov.pk/sites/default/files/labour_force/publications/lfs2020_21/LFS_2020-21_Report.pdf. Accessed: 2023-09-20.

[79] Pakistan Bureau of Statistics, Government of Pakistan. 2023. 7th Population and Housing Census - Detailed Results. https://www.pbs.gov.pk/digital-census/detailed-results. Accessed: 2024-08-31.

[80] Pakistan Telecommunication Authority. 2024. Pakistan Telecommunication Authority Website. https://www.pta.gov.pk Accessed: 2024-11-18.

[81] Pakistan Today. 2024. *Income Disparity in Pakistan.* https://www.pakistantoday.com.pk/2024/02/20/income-disparity-in-pakistan/ Accessed: 2024-08-08.

[82] Sven H Pedersen and Leif A Strömwall. 2013. Victim blame, sexism and just-world beliefs: A cross-cultural comparison. *Psychiatry, Psychology and Law* 20, 6 (2013), 932–941.

[83] Fahad Pervaiz, Rai Shah Nawaz, Muhammad Umer Ramzan, Maryem Zafar Usmani, Shrirang Mare, Kurtis Heimerl, Faisal Kamiran, Richard Anderson, and Lubna Razaq. 2019. An assessment of SMS fraud in Pakistan. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*. 195–205.

[84] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. 2022. Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 1–18.

[85] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. 1–17.

[86] Divya Ramesh, Vaishnav Kameswaran, Ding Wang, and Nithya Sambasivan. 2022. How platform-user power relations shape algorithmic accountability: A case study of instant loan platforms and financially stressed users in India. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. 1917–1928.

[87] Lubna Razaq, Tallal Ahmad, Samia Ibtasam, Umer Ramzan, and Shrirang Mare. 2021. " We Even Borrowed Money From Our Neighbor" Understanding Mobile-based Frauds Through Victims' Experiences. *Proceedings of the ACM on human-computer interaction* 5, CSCW1 (2021), 1–30.

[88] Elissa M Redmiles. 2019. " Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 920–934.

[89] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. 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*. 666–677.

[90] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2017. Where is the digital divide? a survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 931–936.

[91] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 272–288.

[92] Elissa M Redmiles, Miraida Morales, Lisa Maszkiewicz, Rock Stevens, Everest Liu, Dhruv Kuchhal, and Michelle L Mazurek. 2018. First steps toward measuring the readability of security advice. In *The 2018 IEEE Security & Privacy Workshop on Technology and Consumer Protection (ConPro)*.

[93] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*. 89–108.

[94] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 2020. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and {WhatsApp}. In *29th USENIX Security Symposium (USENIX Security 20)*. 1949–1966.

[95] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. " 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*. 1–14.

[96] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. " 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)*. 127–142.

[97] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. Intermediated technology use in developing communities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2583–2592.

[98] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. 2019. Tough times at transitional homeless shelters: Considering the impact of financial insecurity on digital security and privacy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[99] Anselm L Strauss and Juliet M Corbin. 1997. *Grounded theory in practice*. Sage.

[100] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. 2018. Design within a patriarchal society: Opportunities and challenges in designing for rural women in bangladesh. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.

[101] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. 2019. Users really do answer telephone scams. In *28th USENIX Security Symposium (USENIX Security 19)*. 1327–1340.

[102] United Nations Development Programme (UNDP). 2020. Income Inequality in Pakistan. https://www.undp.org/sites/g/files/zskgke326/files/migration/pk/UNDP-PK-Poverty-2-Income-Inequality-in-Pakistan.pdf Accessed: 2024-08-23.

[103] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. 1–14.

[104] Aditya Vashistha, Abhinav Garg, Richard Anderson, and Agha Ali Raza. 2019. Threats, abuses, flirting, and blackmail: Gender inequity in social media voice forums. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.

[105] VICE. 2014. The Kitchen Divides Pakistan's Rich and Poor. https://www.vice.com/en/article/the-kitchen-divides-pakistans-rich-and-poor Accessed: 2024-08-23.

[106] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–25.

[107] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. 2022. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2344–2360.

[108] Jeffrey Warshaw, Nina Taft, and Allison Woodruff. 2016. Intuitions, analytics, and killing ants: inference literacy of high school-educated adults in the {US}. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 271–285.

[109] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. " We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[110] Nicola Wendt, Rikke Bjerg Jensen, and Lizzie Coles-Kemp. 2020. Civic empowerment through digitalisation: The case of Greenlandic women. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[111] Tingmin Wu, Rongjunchen Zhang, Wanlun Ma, Sheng Wen, Xin Xia, Cecile Paris, Surya Nepal, and Yang Xiang. 2020. What risk? i don't understand. an empirical study on users' understanding of the terms used in security texts. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. 248–262.

[112] Yuxi Wu, W Keith Edwards, and Sauvik Das. 2022. SoK: Social Cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1863–1879.

[113] Fouzia Younas, Mustafa Naseem, and Maryam Mustafa. 2020. Patriarchy and social media: Women only facebook groups as safe spaces for support seeking in Pakistan. In *Proceedings of the 2020 international conference on information and communication technologies and development*. 1–11.

[114] Savvas Zannettou, Olivia Nemes-Nemeth, Oshrat Ayalon, Angelica Goetzen, Krishna P Gummadi, Elissa M Redmiles, and Franziska Roesner. 2024. Analyzing

User Engagement with TikTok's Short Format Video Recommendations using Data Donations. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–16.

[115] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–15.

A INTERVIEW PROTOCOL

Note: The actual protocol was in Urdu. An English version is attached here for readability. Also note that our interviews were semi-structured, hence, slight variation in the ordering/phrasing of the questions was allowed.

A.1 Introduction

Hi, My name is [], and I am a student at [] researching on how people use and learn about technology. I wanted to have a short chat with you on how you use your mobile device and from where do you learn about its different features and the risks associated with it. If you agree, then I'll give you 500 PKR as compensation for your time. ***Notes for the interviewer: (i) Follow ethical protocol and Get consent form signed, (ii) Reassure them of their rights, anonymity, and safety, (iii) Get consent for audio recording, and (iv) Answer any questions they have.***

A.2 Sociodemographics

Firstly, can you tell me a little bit about yourself, like:

- What kind of work do you do here?
- What is your age?
- Which region in Pakistan do you belong to?
- What is your mother tongue?
- What is your highest completed level of education?
- Have you taken any courses or training in Computer Science / IT?
- Who do you live with?
- What is your monthly income?

A.3 Phone Onboarding, Usage, and Advice / Rapport-Building Questions

Great! I have a couple of questions regarding how you interact with technology, for example, through your mobile phone or your computer etc.

- Do you have any of these in your house? (phone / computer / laptop / radio / TV / telephone / newspaper)
- What kind of mobile phone do you have?
- Is this a feature phone or a smartphone?
- Is this your personal phone or do you share it with anyone else?
- How did you start using this phone?
- Did you create an account on this phone yourself? ***Notes for the interviewer: If no, then:***
  - Who set this up for you?
  - How did they help you setup your phone?
  - Do you often ask them for help in setting up phones? Why/why not?
- Who do you share it with?
- Why do you share it with them?
- Who got you this phone?
- How do you use this phone?
- Do you have a PIN/Password on this phone?
- Who else knows this password?
- Did you set this PIN/Password on this phone yourself? ***Notes for the interviewer: If no, then:***
  - Who set this up for you?
  - How did they help you setup this?
  - Do you often ask them for help in setting up passwords? Why/why not?
- What kinds of apps do you use on this phone?

Notes for the interviewer: In case they use someone else's phone or use a shared phone, ask similar questions about their + others' usage of the phone.

A.4 App Onboarding, Usage, and Advice / Rapport-Building Questions

Okay, you talked about some apps you use on your phone. Let's dive into a couple of them. For X app ***Notes for the interviewer: ask these questions for WhatsApp, phone calls, social media apps like Facebook and Tiktok, and any other apps they mention***:

- Can you talk more about how exactly you use this app / feature?
- From where did you learn about this app?
- If someone else told you about it, why did they share it with you?
- Did you create an account on this app yourself? ***Notes for the interviewer: If no, then:***
  - Who set this app up for you?
  - How did they help you setup this app?
  - Do you often ask them for help in setting up such apps? Why/why not?
- How long ago did you start using this app?
- Does this app involve interacting with someone else?
- How do you interact with someone else using this app / feature?
- Did you tell anyone else about this app?
- With whom did you share this app with?
- Why did you share it with them?
- Are you folks often telling each other about such new things on your mobile phones? ***Notes for the interviewer: If yes, then:***
  - What kinds of apps have they shared with you?
  - Why do you folks often share such information with each other?

A.5 Threat Incidents and Security Advice

Have you faced any kind of problem with these apps or mobile phones in general? ***Notes for the interviewer: If they ask what sort of problems? then say, "perhaps someone tried to take advantage of you or caused you some form of harm while using this app?". If they don't understand, prompt them with examples given here: A.6. If they still don't understand, end the interview.***

- What problem have you faced?

- Why was this a problem?
- What or who caused the problem?
- How long ago did you face this problem?
- How did you try to navigate this problem?
- Can you recall an incident that you may have heard about of someone else who faced some kind of problem with this app (maybe you heard from someone you know or you read it somewhere)?
  - Can you tell who faced these problems?
  - What problem did they face?
  - How long ago did they face this problem?
  - How did you come to know about this problem that they faced?
  - Why did they tell you about this?
  - Are you folks often telling each other about such new things on your mobile phones? Why?
  - How did they try to navigate the situation?
  - How knowledgeable do you think they are about IT / mobile phone etc. in general?
  - What did you learn from this problem?
  - Did the person who told you about this issue give you any advice on how to solve such issues?
  - What advice did they give?
  - Have you followed this advice? Why or why not?
- Did you start to do anything differently after learning about this problem?
- Can you explain what you started to do differently?
- Did you ever tell anyone else about this problem?
  - With whom did you share this problem with?
  - When did you share it with them?
  - How did you share it with them?
  - Why did you share it with them?
  - Are you folks often telling each other about such new things on your mobile phones? Why?
  - What other kinds of problems have you discussed?
  - Why do you have such a relationship with them?
  - Is there anyone else with whom who shared this problem? Who / Why?

A.6 Example Threats

Notes for the interviewer: If they say nothing, prompt them with these - stop as soon as they agree to something: **Note**: Examples directly taken from [34].
I mean, in which someone tried to harm you or take advantage of you. For example, there can be:

- Hacking where someone tries to get unauthorized access to someone's phone, data, and account, which can result in loss of money or extortion.
- Unsolicited contact where you get unwanted and repeated calls and messages by someone, which may include spam, repeated requests for contact, personalized threats, extortion, or any unwanted contact that makes the receiver feel uncomfortable.
- Non-Consensual Use of Information (NCUI) where someone uses your information, such as your phone number, address, or pictures, without your consent and usually, without your knowledge.
- Extortion where someone uses your personal information or psychological manipulation to make threats and demands.
- Impersonation where someone uses your or someone else's identity online and is acting as them online. They may start posting stuff online or start contacting people through texts or calls pretending to be someone else.
- Scam Calls/Messages that pretend to be an individual or from an authority that tell you that you have won a reward, like perhaps from Benazir Income Support Programme or Jeeto Pakistan. They ask you to send some money or enter a code to obtain your reward. Mostly such scam calls lead to a loss of money.
- Defamation where any intentional, false information is disseminated that harms or causes injury to the reputation of a person.
- Stalking which involves keeping track of someone's online activity, without their knowledge, in a way that makes the subject of the stalking uncomfortable.
- Abusive Comments that involve the usage of harsh, hurtful, explicit, or insulting language to attack another person.

A.7 Attacker & Victim Perceptions

This is such insightful information. And I am really glad that you (or the person who faced the problem) have come this far. We are just about to wrap up this interview, I just had a couple of other generic questions related to who you interact with regarding your device and its issues.

- Do you think there are certain kinds of people who are more vulnerable to such issues?
- Why do you think such people are vulnerable?
- Can you give an example of someone who might be more vulnerable?
- Why do you think this person would be more vulnerable / what makes them vulnerable?
- Lastly, can you connect us with anyone else over here whom we could interview?

Notes for the interviewer: End the recording, thank them for their time and input, give them their compensation, reassure them of their anonymity and safety, good bye.

B CODEBOOK

See Tables 6 and 7.

C ADVICE PIECES FROM PARTICIPANTS

C.1 Cross-Check & Verify

- "So, unless you see something with your own eyes, you shouldn't believe in anything. Not until you talk to someone face-to-face. Like, you shouldn't believe in random things" *(F3_U)*.
- "We used to tell him [the cousin] the same thing that [he] was being foolish, he should have asked, should have called his cousins, told his mother and asked her if her sister was in such a condition and ask, they live nearby, not even far,

Top-level Category	Sub-Codes	Sub-sub-codes
Phone Usage and Onboarding	Device/Phone Ownership	• types of phones • owners of phones • owners of TVs and other devices
	Phone Sharing Practices	• sharers • reasons for sharing phones
	Phone Onboarding Behaviors	• helpers • phone buying - how did they buy the phone • apps and accounts onboarding • reasons for taking help
	Phone and Apps Usage	• phone used for work • used to make phone calls • used to watch videos • other apps and reasons
	Generic Phone/App Issues	• accidental misclicks • issues due to lack of tech savviness • issues due to their location (limited signals)
	Interaction with Device	• how do they interact with the device (text/voice) • which interaction type they prefer
	Passwords/PINs/Authentication	• has (no) password/PIN on phone • who setup this password
Threat Landscape	Threat Incidents (Online & Offline)	• extortion incidents • fraud: scam calls, fraud messages, offline frauds • phone sharing misuse • negative stories in installments and guarantees • Misc: phone thefts
	Victims	• who was the victim
	Defense Mechanisms	• technical behaviors (e.g., blocked the caller) • social behaviors (e.g., reached out for help)
	Consequences	• monetary losses • physical threats (e.g., house visits, harassment) • good endings (target did not fall victim)
	Reasons for compliance	• fell for greed • wanted to save personal reputation • no time/education/experience to validate • wanted to help others out
	Reasons for non-compliance	• took advice from helper • faced/heard about similar incident before
	Attackers and Victims' perceptions	• how attackers operate • who attackers are • who attackers target • which people are more vulnerable

Table 6: Codebook (Part 1)

just a difference of 1 or 2 stops, he could have gone there, then he wouldn't have been in such a situation" *(F1_U)*.
- "First, look and see if the caller is legit or not. If he's asking money from you, try to check what he is doing with that money" *(M1_U)*.
- "I didn't get scared when he tried to threaten me. Instead, I started asking him questions which he didn't have the answers to. So this is what I learned" *(M8_D)*.

C.2 Don't Share Personal Assets

- "I just tell them this: let's suppose you have a mobile account or any bank account. These banks have their official numbers from which they send messages, like don't share your password with anyone else etc etc. So, they will only call you from that number" *(M4_U)*.
- "Don't give your phone to anyone. Even if a friend says, 'Can you give me your phone for a bit? I need to make a call,' don't give it to him" *(M3_U)*.

Top-level Category	Sub-Codes	Sub-sub-codes
Advice Landscape	Advice Sources & Advisees	• advisees • advisors
	Advice Content	• threats – block and avoid – cross-check and verify narratives – don't share personal assets (phones, passwords) – online world is unsafe – contact the helper
	Methods of Advice Sharing	• medium – anecodotal stories ∗ anecdotes shared in-person ∗ anecdotes shared in videos – intermediation • advice used/shared as a defense mechanism • advice shared proactively to raise awareness
	Reasons for sharing/taking advice	• perceived competence/sense of goodwill – lack of others' education – lack of others' experience – poor financial situation of others – lack of support from friends, family • trust/mutual respect/friendship
	Reasons for not sharing/taking advice	• ridicule and victim blaming – others saying that the victim didn't act correctly • work induced challenges – sense of privacy when it comes to family matters – work is too demanding, prevents engaging socially – not allowed to use phones at work – new to the work place / city so no friends – does not want to make family worried
	Failed advice mechanisms	• hid on-going incident from helpers • did not adopt/implement advice given by helpers • helpers also fell for the scam narrative

Table 7: Codebook (Part 2)

C.3 Online World is Unsafe

- "I feel that this [access to the internet] is very dangerous because kids are not the right age for the things they can watch on mobiles. That's why I don't give my kids my mobile and have never gotten an [internet] package. Also, on social media, there is a lot of vulgar and fake content out there" *(F3_U)*.
- "If someone tries to take advantage of you, first of all, you should stay confident and know that you haven't done anything wrong. There is a lot of fake stuff out there. So don't focus on what the other person [on the call] is saying. You know how the saying goes: 'If someone runs away with your ear, you don't run after them; you first check your ear'" *(F3_U)*.

C.4 Contact the Helper

- "So, I told her, 'You should have asked us. We earn money with a lot of hard work, we can't just give it to anyone like that" *(F9_D)*.
- "I told my brothers that they should never talk to these scammers and immediately cut the call. And if they can't understand what's happening [if they cannot determine whether the call is legit or fake], then I've told them to call me immediately" *(M4_U)*.
- "I told my friend that she should ask me or reach out to someone else she trusts whenever she faces such calls" *(F9_D)*.

C.5 Avoid & Block

- "If you get a call from any other number that says, 'I am calling from the bank and this and that and please share your details because I don't know, your ATM card is blocked and to open that.' Then you should never talk to them, and cut the call immediately" *(M4_U)*.
- "It's better if you just avoid these people by blocking their number, or by just changing your own number instead of trying to get in touch with them because you never know what they are capable of doing. Because these people are different, the ones who do such things, they are different.

So it's better that, to avoid things from getting complicated, you simply block them or change your own number" *(F3_U)*.

- "And whenever she is outside she is unsafe. So just try to keep yourself safe from such things by just trying to avoid such people who are dangerous. And avoid them in a way that doesn't worsen things or complicate things further" *(F3_U)*.
- "Then there was my cousin, he told me that if it was a fraud, then you should delete it. So I deleted it" *(F6_F)*.
- "I told him that you don't follow along. That someone is trying to extort money from you" *(M2_U)*.
- "So I told him don't take it [the loan] from them [Barwakt app] they annoy you a lot. I made him delete this app from his phone" *(M4_U)*.
- "So once I had heard that someone got a phone call from a wrong number, I told them to block it. Because she didn't know the person on the call. And you shouldn't get frank with a stranger like this" *(F9_D)*.
- "When I heard this, I told her that, all of this that she did like telling her husband and then he got a lawyer and the police involved, like so much expense, she could have simply just blocked the number or just shut down her own number" *(F3_U)*.
- "If they [his wife and mother] get a call from an unknown number, I have forbidden them from picking it up" *(M7_F)*.