Understanding How Users Prepare for and React to Smartphone Theft (Extended Version)

Divyanshu Bhardwaj[⋆†], Sumair Ijaz Hashmi[⋆†], Katharina Krombholz[⋆], Maximilian Golla[⋆]
⋆ *CISPA Helmholtz Center for Information Security,* † *Saarland University*

Abstract

Smartphone theft is common, yet little research explores how users prepare for or respond to such incidents. To address this gap in the literature, we conducted 20 semi-structured interviews with victims who had experienced smartphone theft in the past two years. These cases ranged from opportunistic thefts to armed robberies. Our findings show that users are often unprepared and rely on basic protection measures like screen locks. After theft, they attempt to track their phones, activate *Lost Mode* and frequently turn to family and friends for moral support. Many experience significant distress, particularly from privacy concerns, loss of photos, and disrupted access to essential services like online banking. Recovery is often complicated by challenges such as SMS-based two-factor authentication (2FA). Our study identifies opportunities for phone vendors and service providers to enhance security features and recovery tools that address both technical and social aspects of smartphone theft.

1 Introduction

Smartphones provide access to a wealth of sensitive information and services, including online banking, credit card details, digital keys, control over IoT devices, passwords and two-factor codes, health data, business and personal communication, private photos, and cloud storage access. Losing one can be more than a personal inconvenience; it often presents significant social and economic challenges, potentially leading to financial fraud [105] and identity theft [47].

Smartphone theft has become increasingly common, particularly in large metropolitan areas [77, 93, 106]. Although smartphone theft is a global issue, its prevalence and nature vary significantly across countries: In 2022, around 90,815 phones were stolen in London [69], averaging one theft every six minutes [30, 47]. By 2024, this number has risen to 116,676 [70], showing a worrying upward trend. Similarly, in Brazil, over 937,294 phones were reported stolen in 2023 [82], underscoring the severity of phone theft in this region. In Germany, the police recorded approximately 185,000 incidents of phone theft in 2022 [90], and a representative survey from 2023 revealed that 21% of Germans reported having had their phone stolen at least once in their lifetime [16]. According to the GSMA, participating network operators report device theft affecting about 1% of active subscribers annually [43].

To address this, responsible entities have begun to shift their dependence on technology to locate and better protect stolen phones. For example, the government of Brazil launched a dedicated app to assist victims [44]. Phone vendors have recently introduced more advanced protection features, by expanding their threat model to also consider stolen PINs [7, 77], "offline" tracking [64], motion-based locking to fight phone snatching [35], and activation locks for phone parts [29].

Prior work has explored existing authentication methods on phones and their effectiveness in protecting user privacy [21, 58, 61], and reported the increasing reliance on technology for tracking stolen devices [44, 52, 99]. To the best of our knowledge, there is no empirical data on how people prepare for, experience, and mitigate the effects of phone theft.

To fill this gap, we investigate how individuals prepare for smartphone theft, their immediate concerns, reactions, and challenges following such incidents by interviewing 20 victims whose phones were stolen within the last two years. Our research is guided by the following research questions:

RQ1 *How do users prepare for smartphone theft? What risks do they associate with theft?*

RQ2 *What immediate concerns do users have upon losing access to their device? What is their first response, and where do they seek assistance?*

RQ3 *What harms and threats do users deal with after smartphone theft?*

Our findings indicate that people are ill-prepared, leading to panic and significant fear of potential consequences. To protect themselves, they rely on basic measures such as the screen lock. Their immediate concerns center around the loss of photos, which quickly evolves into a fear of unauthorized access, something many view as a violation of their privacy. People try to track their phones and enable *Lost Mode* to regain con-

trol and reduce potential privacy breaches. They often seek advice from family and friends during this stressful time. The experience of theft causes psychological harm and anxiety, largely due to losing access to essential services like online banking. Restoring data on a new phone can be challenging due to two-factor authentication (2FA), sometimes leading to the misconception that 2FA is more of a hindrance than a protective measure. Eventually, people begin to reconsider their approach and rely more on non-technical measures. Based on these findings, our paper makes the following contributions.

1. Empirically grounded insights into user behavior *during* and *after* smartphone theft informed by detailed interviews with individuals who have lived through theft incidents.
2. A thematic map capturing the temporal progression of users' perceptions and responses, intended to inform interventions that better support victims of smartphone theft.
3. Stakeholder-oriented recommendations based on users' lived experiences, aimed at informing the development of more robust security measures and support mechanisms.

We highlight opportunities for phone vendors to develop enhanced security features and recovery tools that address both technical and non-technical measures before, during, and after smartphone theft. Our findings emphasize the importance of preparedness and provide actionable guidance for all stakeholders involved to better protect users.

2 Related Work

We discuss previous research on device theft, authentication methods, and user awareness of unauthorized access risks. Appendix A offers current anti-theft methods and advice.

2.1 Theft of Personal Devices

The past decade has seen a notable rise in the number of personal digital devices, including mobile phones and personal computers, which led to an increase in theft incidents. Prior research [20,53,57,79] has focused on utilizing technology to locate stolen phones, primarily through the application of machine learning and automated methods that detect such theft by analyzing sensing data. Dimkov et al. [27] looked into the effectiveness of security measures against laptop theft in universities. Their research revealed that the success or failure of thefts was more closely linked to the security awareness of users than to the effectiveness of access control and CCTV protection mechanisms. In 2012, Tu et al. [97] surveyed how people cope with device loss and theft based on the protection motivation theory. They found that victims' responses to theft are influenced by threat appraisal and social influences. In a follow-up study from 2015 [96], they surveyed 339 people and combined protection motivation and social learning theories to show how information sources like experience and social measures influence people's threat appraisals and coping intentions to device theft.

2.2 The Role of Authentication

The role of authentication as the primary defense mechanism in safeguarding privacy on mobile devices has been extensively researched; In an evaluation on smartphone locking, Harbach et al. [46] found that PINs, pattern unlock, and slide-to-unlock allow users to balance security and convenience. Albayram et al. [3] concluded that users tend to choose less secure screen-locking methods, such as pattern unlocks and slide-to-unlock, more due to a lack of risk awareness than convenience. Cho et al. [22] discovered that users favored fingerprint scanners but believed that pattern-based screen locks were adequate for protecting their devices from unauthorized access. Markert et al. [61] have investigated the security of 4-digit and 6-digit PINs under blocklisting and rate-limiting constraints as implemented by modern smartphone operating systems. Bailey et al. [12] investigated the strategies and effectiveness of novice attackers attempting to guess unlock PINs. Their research revealed that these attacks can be surprisingly successful, with novice participants managing to guess the PINs of approximately 1 in 8 strangers.

2.3 Unauthorized Access

Gallardo et al. [36] examined four stalking scenarios through interviews, finding that most participants struggled to detect smartphone compromises due to a lack of technical expertise. They recommended that phone and app vendors improve interface usability and clarity for non-experts to detect device or account compromise. Marques et al. [62] collected narratives from 102 participants to explore how people perceive incidents of unauthorized access to their smartphones. They found unauthorized access predominantly involved text-based communications, such as text messages, instant messages, and emails. Muslukhov et al. [72] found that 12% of 746 surveyed participants reported experiencing unauthorized access to sensitive data, while 9% admitted to accessing another person's smartphone without permission. More closely related, Dixon et al. [28] explored users' perceptions of unauthorized smartphone access by presenting scenarios in which phones were lost. They found that users underestimated insider threats while overestimating external hacking capabilities.

In summary, prior research has explored the technological aspects of theft detection, the effectiveness and usability of mobile authentication, and the social and psychological dimensions of unauthorized access. Most existing work has examined individual aspects of phone theft in isolation and relied on hypothetical or survey-based methods, which fail to capture the complexities of real-world experiences. However, there remains a significant gap in our understanding of how people respond in practice to actual phone theft incidents, particularly in the moments immediately following the theft and in their journey to recover from it. Our study addresses this gap through in-depth interviews with people who have person-

ally experienced phone theft. This allows us to uncover rich, firsthand insights into the challenges they face, the protective actions they take, and the sources of support or advice they rely on. By grounding our findings in real-world experiences, our work contributes empirical depth to understanding user behavior and risk perception following phone theft.

3 Method

Our approach was exploratory, given the limited understanding of how people safeguard their privacy and react after their phones were gone. For this, we conducted semi-structured interviews with individuals who had experienced phone theft within the last two years. Our complete study setup is shown in Figure 1. We began by developing an interview guideline, which was subsequently refined through a pilot study involving three participants. Following this, we distributed a screening survey, which received 166 responses. Recruitment was conducted iteratively based on the screening responses. We excluded respondents identified as fake based on responses and those flagged by our survey software Qualtrics as duplicates or fraudulent. This process resulted in 22 interviews, of which two were excluded prior to analysis due to issues related to data quality and coherence. The final dataset comprised 20 interviews, which were analyzed using thematic analysis to identify and develop key themes.

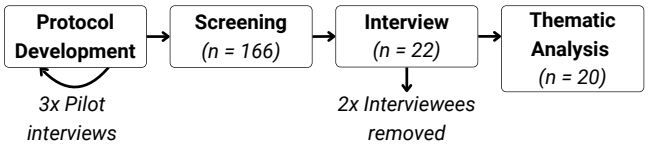


Figure 1: Overview of our recruitment and analysis approach.

3.1 Study Protocol and Design

We targeted recruiting people who had actually experienced phone theft, recognizing that such situations are inherently complex and demand quick decision-making under pressure, coupled with social stress and anxiety. In contrast, individuals who have not experienced phone theft must imagine themselves in such a hypothetical situation and predict how they would behave, leading to unrealistic responses and biases [17, 63, 86, 102].

In pilot tests, we found that participants who had firsthand experience with phone theft provided nuanced insights and could recall specific incidents, actions, and outcomes based on their experiences. These contextual details were essential for understanding the complete scope of individual reactions to phone theft. In turn, this helped ground our collected data in real-world experiences, thereby enhancing external validity.

We opted for semi-structured interviews, which allowed us to follow a guideline while also enabling follow-up questions on the topic. To facilitate this, we developed an interview protocol designed to delve into experiences. The interview guide (see Appendix B), was structured as follows:

1. *Informed Consent*: Every participant completed a consent form via a Qualtrics survey. The form explained that the interview would focus on phone theft and the events that occur when a phone is stolen. The consent outlined the study's objectives, the rights of the participants, data collection procedures, and requested their written consent.
2. *Introduction and Agenda*: We provided a brief overview of the interview and presented additional instructions. We emphasized that we were solely interested in their perspectives and reassured them that there were no right or wrong answers. At this point, we once more requested oral consent to record the interview.
3. *Warm-Up Phase*: To help ease participants into the discussion and build rapport, we began with some general questions about smartphone usage.
4. *Preparation*: We asked participants what they think happens when someone steals their phone, how they prepare for such a situation, and what steps they take to ensure that no one other than them can access their phone.
5. *Content Warning and Incident Description*: Participants were then asked to describe the incident that resulted in their phone being stolen. Before delving into this sensitive topic, we issued a warning, reminding participants that they could pause at any time and were not obligated to answer any questions they felt uncomfortable with.
6. *Theft Phase*: After participants shared their experiences with the incident, we inquired about their initial concerns and actions taken in the immediate aftermath to understand their advice-seeking behaviors, specifically who or where they turned for assistance.
7. *Post-Theft Phase*: We then asked about the outcome of the incident, whether they were able to get their phone back, and what their recovery journey looked like.
8. *Harms and Most Critical Applications*: Next, we explained the various dimensions of harm associated with phone theft and asked participants if they experienced any specific harm during the incident. We also requested that they share the five applications on their phones that they would not want anyone else to access.
9. *Cool Down Phase*: Finally, to help participants decompress after the interview, we discussed phone theft protection measures, such as stolen device protection [7].

In addition, we collected demographic information in line with best practices [85], including age, gender, IT background, and their current mobile screen locking mechanism. We also gathered data on app usage habits, how regularly they performed backups, and the types of applications they had on their phone for contextualization.

Pilot Testing. We conducted three pilot tests to validate our approach. Participants were recruited from among acquaintances of the researchers, including one individual who had experienced phone theft, another who had misplaced their phone, and a third whose phone had unexpectedly overheated and stopped working. While two pilot participants had not experienced phone theft, they lost access to their phones and did not know if and when they would get back their devices. Hence, our research team deemed them fit to act as pilot participants to help us test and refine our study. Of the three participants, two had backgrounds in security research, while one did not have a formal education in computer science. Informed consent was obtained from all participants. We reviewed the interview process with the pilot participants and solicited detailed feedback. In response to their input, we made minor adjustments to eliminate redundancies in the interview guideline. Each pilot test also allowed us to refine and adapt the flow of the interview and improve questions.

3.2 Recruitment and Demographics

To gain an accurate understanding of the experience of phone theft in the real world, we focused on individuals who have actually been victims of such incidents within the last two years. This timeframe was selected to ensure that the events remained vivid in the participants' minds, while also considering that the technical protection measures, such as tracking and Lost Mode, have remained consistent during this period.

We recruited participants between Sep. 2024 and Jan. 2025. Recruiting this specific population is a challenging task. During the initial ideation phase, we found several anecdotal examples on Reddit from phone theft victims seeking advice, which motivated us to understand their experience better. Hence, we turned to Reddit to access this diverse but hard-to-recruit population. To reach potential participants, we advertised our study on relevant forums that discuss phone theft, including *r/LostMyPhone* and *r/iphonehelp* among others. Our advertisement post outlined the participation requirements, specifically that individuals must have personally experienced phone theft, as well as details concerning monetary compensation, a link to the screening survey, and the primary author's contact information. Additionally, participants needed to be fluent in English, which was a prerequisite in the interview screening. Prior to posting our ad, we communicated with community moderators to explain our project, and they approved our post. Recognizing that many community members, similar to the typical Reddit user base, would participate remotely, we structured our study to be entirely online.

Participants were compensated with 50 Euros and provided with a phone theft emergency kit (see Appendix D) and a guide on how to prepare for and respond to theft. Recruitment continued until we observed a decline in new topics during analysis, indicating saturation. We had 166 respondents in our screening. We iteratively selected participants and did not contact those we identified as fake based on survey responses or flagged by our survey software Qualtrics as fraudulent. Our final dataset included 20 participants, 12 male and 8 female, from 9 countries. Most were aged 25–34, held a bachelor's degree, and about half had an IT background. There was an almost equal split between Android and iOS users. 17 participants had SIMs linked to their IDs. See Table 1 for the sociodemographics of our sample.

3.3 Data Collection

We conducted a total of 22 interviews. The duration of the interviews ranged from 29 minutes to 1 hour and 17 minutes, with an overall interview time amounting to 20 hours and 53 minutes, yielding an average interview duration of 59 minutes. All interviews were conducted via Zoom. However, we opted to exclude one interview from the dataset, as the participant had not experienced a theft but had misplaced their phone, which they subsequently recovered. Additionally, another interview was removed due to discrepancies that we identified. We noticed that the participant's story of their phone theft contradicted the details provided in our screening survey, and they struggled to answer basic questions regarding the stolen device and its location. These inconsistencies raised suspicions about the authenticity of the theft claim. After a review of the recording with the research team, we decided to exclude this participant from our study. Both of these participants were fully compensated. With these omissions, our final dataset comprised of 20 participants.

3.4 Data Analysis

We used thematic analysis to examine the data, as it is particularly effective for exploratory research aimed at understanding end-users, and has been widely used in similar exploratory studies [37, 50, 71, 74]. Our approach followed the six-step procedure outlined by Braun and Clarke [18]. The process began with transcribing the collected interview data orthographically by a GDPR-compliant third-party service, with interviewees providing consent for this process. Using an inductive, bottom-up approach aligned with open coding principles, the two primary researchers independently coded the same two interviews to generate initial codes. Subsequently, they met to compare findings, resolve discrepancies, and collaboratively develop an initial codebook. This codebook was used to independently code two additional interviews, with the researchers meeting weekly to discuss disagreements and refine the code definitions as needed, resulting in the final codebook (see Appendix C). The researchers then split the remaining interviews among themselves and used the final codebook to code them. As coding progressed, researchers wrote summaries and analytic memos to organize and track potential themes. Based on these, we conducted a thematic analysis [18, 101], grouping codes axially to examine their

relationships and develop overarching themes and subthemes. Throughout the thematic analysis, we consistently revisited the relevant transcript segments to ensure the analysis remained firmly grounded in the data. From this analysis, we developed a *thematic map* [18], which provides a visual representation of relationships between themes and sub-themes identified in the data (presented in Figure 2). We reached thematic saturation [48, 49] after 16 interviews in relation to participants' preparedness for and responses to phone theft. To confirm saturation and ensure that no new themes emerged, we conducted six additional interviews. Two of these were excluded due to concerns about their authenticity, resulting in a final sample of 20 interviews included in the analysis. Inter-rater reliability was not calculated, as the two primary researchers held weekly meetings to discuss the collected data, to resolve coding disagreements, and to update the codebook until consensus, following recommended qualitative research practices [13, 66, 80]. The entire team worked together to find the best method for reporting the results.

3.5 Limitations

Interview studies rely on self-reported data, which can lead to under- or over-reporting of experiences [75]. To address this, we developed a guide focused on specific experiences related to phone theft and included prompts to aid memory recall.

Studies can be biased due to participants trying to present themselves in a socially desirable way [33]. This is particularly true for studies that prioritize privacy. To minimize biases, we took steps to avoid influencing participants during recruitment and reassured them that our primary interest was understanding their experiences, emphasizing that we would not judge their actions or responses. This allowed participants to speak honestly about their experiences.

We acknowledge that our findings may be biased by the highly educated nature of our sample, which could be partly attributed to our use of Reddit as a recruitment platform. Reddit communities often attract younger, educated, and digitally literate users, and participants recruited through Reddit are likely to be more tech-savvy [89]. While qualitative studies like ours do not have strict requirements for representation, we made intentional efforts to recruit a diverse range of participants from around the world. We also acknowledge that the potential trauma associated with phone theft may result in some participants choosing not to engage with us, which could introduce survivorship bias. As a result, individuals who experienced more severe consequences of phone theft may have opted out of participating in our study.

Despite these limitations, our study provides valuable insight into how people experience and respond to phone theft and how existing protection features are understood and used in practice. These findings help identify where current assumptions about user behavior misalign in practice and can inform the design of more usable and effective solutions.

4 Results

We discuss the themes that emerged from our analysis. We use the following qualifiers to indicate the prevalence of themes: codes appearing in 0–20% of interviews are labeled as "a few," 21–40% as "some," 41–60% as "about half," 61–80% as "many" or "most," and 81–100% as "almost all" or "all."

Our analysis yielded three temporal phases of phone theft: *pre-theft*, *theft*, and *post-theft*. We begin by examining the *pre-theft* phase, which encompasses the period leading up to the theft. Next, we discuss the *theft* phase, detailing the moment the theft occurs and the subsequent immediate timeframe. Finally, we explore the *post-theft* phase, referring to the period after the theft, once the initial shock has subsided and individuals have moved past the immediate aftermath. Omissions and edits for brevity, readability, and context are denoted with square brackets. Figure 2 provides an overview.

The users, influenced by their habits and feeling unprepared for the possibility of theft, harbor concerns about smartphone theft. They rely on technical measures for protection in the event of theft, which shapes their behavior related to smartphone theft. During an actual theft, the user's behavior evolves as they react to initial concerns. The theft triggers an immediate response and initiates a cycle of seeking advice and support. These actions shape and reinforce their behavior for future contexts. In the post-theft phase, the user shifts towards recovery, managing resulting harms and addressing privacy threats, which prompts further behavioral adjustments. At this stage, they begin to adopt non-technical methods as their primary means of protection.

4.1 Pre-Theft Phase

We examine usage habits, unpreparedness for theft, and the measures users take, as shown in Figure 2.

4.1.1 Usage Habits

Phones have become ubiquitous, with most viewing their devices as integral extensions of themselves (n = 14; P1 - P4, P6, P9, P12 - P17, P19, P20). They described them as the primary means of interacting with the world. Participants noted that banking and payment have become so prevalent that they often overlook these features unless prompted. For instance, P6 remarked, '*I manage all personal matters, all my finances on my phone, since it's in front of me all the time. And I had a laptop and I sold it simply because I was using my phone for everything.*' P12 reinforced this ease of payments and explained to only carry a wallet for cards that are required for identification or getting access.

> "*Nowadays, you don't need your wallet unless you need your [...] ID to scan into a building or something.*"P12

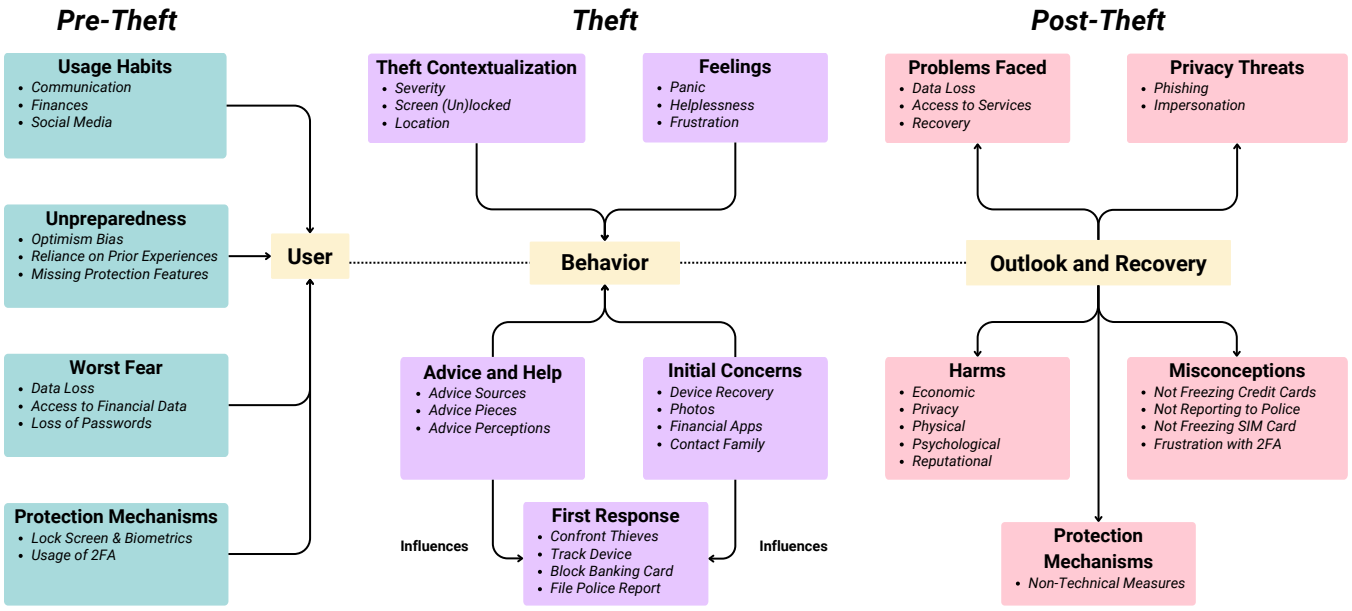


Figure 2: Thematic map of the phone theft journey. This figure captures user experiences, perceptions, and challenges across three uncovered stages of smartphone theft. (i) Pre-Theft: Highlights user habits and lack of preparation, (ii) Theft: Covers emotional responses, initial concerns, and first actions, and (iii) Post-Theft: Addresses recovery, harms, and risks.

We found that participants were so accustomed to the convenience of mobile payments that they often neglected to mention these until specifically asked. Beyond this, participants mainly used their phones for communication, social media, web browsing, navigation, and entertainment, including listening to music, streaming videos, or playing games. Some also utilized their phones for work emails and related tasks The complete list can be found in Appendix E.

4.1.2 Unpreparedness

A prevalent theme was the participants' lack of preparedness for the possibility of phone theft. Many underestimated the likelihood of it happening to them (n=12; P1 - P4, P6 - P9, P12, P13, P14, P16). This optimism bias [104], which is a cognitive tendency to underestimate personal risk, left them susceptible to theft. Once the theft occurred, some participants realized how ill-prepared they actually were and felt uncertain about what to do next (n=7; P1 - P4, P8, P12, P13). Participant P2 reflected on this, *'I was totally unprepared.'* P3 echoed this, expressing that no one prepares for this.

> *"[...] you just don't know what to do. You're confused. No one prepares for stuff like this, right?"*P3

However, a few participants demonstrated some preparedness, which they attributed to previous experiences with such incidents (n=3; P1, P5, P6). This familiarity allowed them to remain calmer and better equipped to handle the situation. P5 shared *'Since it was my second experience, it was easier because I understand that most of the stuff is in our heads.'*

The significance of experience was notably expressed by P13, for whom this was the first incident. They conveyed, *'I was pretty much in panic. I didn't know what to do, where to go, whom to ask. [...] That's the very first experience for me to get something stolen.'* Additionally, a few participants recognized that their phones lacked features that could have better prepared them for theft (n=2; P2, P14). In cheaper devices, device tracking, remote locking, and remote wiping are often unavailable [14] which further compromises preparedness.

> *"My current Android phone doesn't have that kind of feature, so remote logout or remote lock. I can only go to the police and file a case or inform the authorities."*P2

4.1.3 Worst Fear

We asked participants about their current fears of phone theft, unrelated to past incidents. They expressed that lack of preparedness contributed to significant fear regarding the consequences. This primarily stemmed from anxiety surrounding the potential loss of personal data, with photos being the most valued. Fear intensified depending on backup habits, with those who consistently backed up their data feeling less anxious than those who did not. Participants were also concerned about the security of their banking details and stored payment methods. P5 said: *'The worst thing is that the lads would get full access to my phone. So they would access personal data and, most importantly, banking.'* A few participants (n=2; P12, P14) emphasized their apprehension regarding the exposure of their home and device location, with P12 saying,

'They probably see the location of my other devices and know where I live because then they'd have access to the Find My and they'll see where my laptop is and where my air tags are.' One participant highlighted the fear of having a phone stolen in a crowded setting. They noted that in such environments, one cannot be sure whether their PIN was compromised, and if breached, it would create limitless opportunities to exploit.

> *"Because, in a concert, you don't know if someone is standing behind you. They saw your PIN [. . .]. They could, of course, [unlock] the phone and then use it. There's a lot on our phones. Actually, our whole history, present and past, is on our phones."*P13

4.1.4 Measures Against Theft

The first line of defense for most was the lock screen, with almost all opting for biometrics like fingerprint or face recognition, complemented by fallback methods such as 4- or 6-digit PINs (n=15; P1, P3, P5 - P14, P16, P17, P19, P20). P8 noted, *'I usually use face authentication, but if face authentication doesn't work, iPhone works like this, that it lets you give a PIN. So those are two layers of accessing the iPhone.'*

P18 stated they do not use a lock screen due to being a low-vision user; entering a pattern or PIN each time was challenging and too time-consuming. We found participants often set their PIN to something personal, making them less secure against insiders. A few chose pattern locks instead (n=2; P2, P4), believing they offer greater security, with P4 arguing *'I use a pattern lock, I make the lines invisible and I swipe very fast. As opposed to typing where anybody could actually follow, I think there is a better chance of them recognizing what it is.'* Only two participants reported using alphanumeric passwords. Additionally, a few participants indicated that they enabled 2FA (n=2; P1, P8).

> *"I ensure that I turn it on for every domain on every device, and it's linked to my iPhone. So I get a one-time password on my iPhone."*P8

Summary

In response to RQ1, participants reported being underprepared for theft. This lack of preparedness led to a significant fear about potential consequences. To protect themselves, they primarily relied on basic technical measures, such as their lock screen.

4.2 Theft Phase

The next section delves into the theft phase, as shown in Figure 2. We examine the feelings people experience when the theft happens, their mental models that shape their initial concerns, and their first responses. Additionally, we look into the help people receive and the problems they face due to not having access to their phones anymore.

Table 1: Participants Demographics (by Incident Severity)

PID	G	Age	Edu	IT	CC	Location	OS Vendor	Lock	S	T	R
Low Severity (e.g., Opportunistic Thefts with Phones Placed Out in the Open)											
P1	W	25-34	Bachelor	○	AT	Uber Car	Apple	6-digit	○	●	○
P5	M	35-44	Master	●	UK	Football F.	Google	4-digit	○	○	○
P7	W	25-34	Bachelor	○	US	P. Residence	Apple	4-digit	●	●	●
P11	W	25-34	Master	●	US	Gym	Apple	6-digit	●	●	○
P12	W	25-34	Ph.D.	●	US	Restaurant	Apple	4-digit	●	●	●
P15	M	45-54	Master	●	DE	P. Transport	Apple	Passw.	●	○	●
P20	M	35-44	Bachelor	○	PT	P. Transport	Samsung	8-digit	○	○	○
Medium Severity (e.g., Pickpocketing)											
P2	M	25-34	Master	●	BD	P. Transport	HTC	Pattern	●	○	○
P3	M	25-34	Master	●	ES	P. Transport	Huawei	6-digit	●	○	○
P4	M	25-34	Master	●	FR	City Center	Google	Pattern	●	○	○
P6	M	45-54	Bachelor	●	AR	Restaurant	Apple	Passw.	●	●	○
P9	W	25-34	Master	●	US	P. Transport	Apple	6-digit	●	○	○
P10	W	18-24	H. School	○	PK	P. Transport	Oppo	6-digit	●	○	○
P13	M	18-24	H. School	●	IN	Concert	Apple	6-digit	●	●	○
P16	W	25-34	Bachelor	○	PK	University	Google	4-digit	○	●	○
P17	M	25-34	Master	○	DE	Nightclub	Samsung	6-digit	●	●	○
P18	W	25-34	Bachelor	○	JM	P. Transport	Samsung	Swipe[1]	●	○	○
P19	M	25-34	Bachelor	●	IN	P. Transport	OnePlus	4-digit	●	●	○
High Severity (e.g., Armed Robberies and Phone Snatching)											
P8	M	25-34	Bachelor	○	PK	City Center	Apple	6-digit	●	○	○
P14	M	18-24	Bachelor	●	PK	Highway	Samsung	8-digit	●	○	○

G: Gender (Woman, Man); **IT**: IT background; **CC**: Country of theft; **S**: SIM card bound to victim's ID; **T**: Tracking used to recover phone; **R**: Recovered phone.
[1] Low-vision user.

4.2.1 Contextualizing Phone Theft

For context, we asked participants to share where, when, and how their phones were stolen. For the majority, the theft occurred through pickpocketing (stealing directly from a victim's clothing, bag, or pocket without their notice) (see Table 1). These incidents usually took place in crowded places, e.g., city centers, universities, nightclubs, and while using public transportation. A few participants reported that their phones were stolen while being in plain view, such as when placed on a restaurant table or seat on a train.

Of the high-severity cases, one participant had their phone snatched from them in broad daylight in the city center. As they exited a building while using their phone to call an acquaintance, a bike with a pillion passenger approached, and the pillion forcibly grabbed the phone out of the victim's hand. Another participant was traveling on a highway on the outskirts of a city when armed robbers approached them and pointed a gun, demanding to hand over their phone.

Only three participants were able to recover their phones. All the stolen phones were modern smartphones, not feature phones, and they operated on either iOS or Android. Table 1 presents the details of the phone theft incidents.

4.2.2 Feelings

Participants shared their immediate feelings upon realizing that their phone had been stolen. They described an overwhelming sense of helplessness, often followed by panic. Many expressed frustration and anger, blaming themselves for the theft (n=14; P1 - P8, P10 - P12, P15 - P17). For instance, participant P15 conveyed, *'At first, I was really stressed and nervous and angry with myself because I didn't*

take care of it.' Overall, navigating the situation proved to be extremely challenging and agonizing for the participants.

> "*I have everything on my phone, my banking, my credit card, my social media, everything, even personal documents. So when I lost it, it seemed like a nightmare.*"[P2]

The feeling of being completely blank stemmed from inadequate preparation. Panic engulfed participants, leaving them uncertain about their next steps. It took time and conversation with others to regain composure, which ultimately enabled them to think more clearly and determine a way forward.

4.2.3 Mental Models

Participants perceived stolen phones as inaccessible to attackers, with P1 noting, '*[...] It's pretty useless without me. Because they [attackers] can't access it.*' They believed that biometrics (i.e., Face ID), provide a high level of security and regarded iPhones as more secure than Android devices [1].

> "*Android phones are kind of bypassable with their security, but iPhones, which is what I use, are not.*"[P6]

Even in cases where biometrics reverted to PINs, P3 felt that these PINs were unlikely to be guessed. Participants acknowledged the usefulness of tracking applications like 'Find My' although many admitted they did not fully understand how these work. '*I knew it was an option in the Find My app. But I guess I don't exactly know what it does. I know [...] it can display a message [...], but I'm not sure if it does anything to improve the security that no one can access.*'

About half of the participants believed phones are typically stolen for resale, either as complete devices or for parts (n=10; P1, P4, P6, P8, P10 - P13, P16, P17). P4 said, '*I either assume the phone would be dismantled for the worth of its components or it would have to be shipped outside the country to be used.*' Participants also felt thieves were uninterested in their personal data, leading to a lack of concern about privacy.

> "*Do they even need the data, since they turn it off first thing after they steal it?*"[P10]

4.2.4 Initial Concerns

The pre-existing perceptions influenced initial reactions following the theft. After recovering from the initial shock, some participants quickly focused on recovering their devices (n=6; P4, P5, P6, P8, P12, P13). For instance, P4 and P6 took it upon themselves to pursue the thieves. Participants were also concerned about losing personal photos that had not been backed up. This concern quickly evolved into a privacy issue, with P10 expressing, '*In terms of the information that I was the most concerned about, it was [...] definitely my gallery, because you know, it had my face and everything else.*' Conversely, P12 was more apprehensive about the possibility of the attackers accessing sensitive information on their phone.

> "*I did not want those people to know where I live, my bank account, my address and all of that.*"[P12]

For participants such as P7, the foremost concern was related to financial applications. They remarked, '*My first concern was my banking [. . .] I really did not want anyone to be able to get access to my bank accounts.*'

4.2.5 First Response

Participants' initial reactions to the theft were primarily influenced by their immediate concerns. Some attempted to confront the attacker (n=5; P3, P4, P6, P8, P13). P8 recounted, '*Two guys came on a bike and the one who was sitting at the back, he snatched it from my ear [...] I didn't know what happened. And then I ran behind them.*'

About half of the participants expressed a strong desire to track their device, provided it had such functionality (n=9; P1, P6, P7, P11 - P13, P16, P17, P19). If they succeeded in locating it, they would activate Lost Mode, allowing them to remotely lock it and display a message indicating that the device was lost, along with their contact information. They believed that taking this action restored some control over their device and prevented a potential privacy breach. P5 reflected on this, stating, '*When I came home, there was an option to track it. If you cannot find it, you can mark it as stolen, and then it locks all that stuff. So, I chose this option.*'

P2 and P10 prioritized contacting their banks to block their cards, aiming to prevent the thief from any financial gain. However, this was more challenging for those who were traveling and away from their bank's country. Additionally, participants also sought to block their SIM cards.

Reporting to the police was another common course of action, with eleven participants filing a police report, although they had low expectations regarding the outcome. Participants noted that they filed a police report primarily as a precaution.

> "*The only reason I made an FIR was that if the phone is somehow used for [malicious] activities, I can legally say that, hey, my phone was lost. I made a complaint. Don't hold me accountable if anything happens.*"[P4]

4.2.6 Advice and Help

Participants sought assistance from various sources. We broadly categorized the assistance into three types: the sources of advice, the specific help provided, and participants' perceptions of the assistance.

Advice Sources

Most participants turned to family and friends as their primary sources of advice (n=13; P2, P3, P5 - P7, P9 - P14, P16, P17). Notably, participants recalled that their partner often served as a reliable support. Friends also acted as advice sources, especially if they were present during the theft. A

few people who offered advice had personally experienced similar situations (n=2; P7, P13).

> “*My fiance was there, and was a help to me. I also had a friend I was texting and getting some advice. I think they also had their phone stolen at some point.*”P7

Additionally, participants sought advice from the police when filing a report about their stolen phone. Others tried to reach out to device manufacturers and network service providers. Consulting with banks was also mentioned, as participants looked for advice on managing financial applications and bank cards that were linked to their phones. Lastly, more tech-savvy participants highlighted that online communities like *Reddit* provided anonymous advice associated with phone theft, which they could draw upon.

Advice and Help Pieces

Participants were advised by their families to avoid confronting attackers alone, as this could be dangerous. They warned participants to be wary of phishing scams, which could lead to attackers getting into their accounts. Additionally, they were cautioned by both their families and the police that stolen phones are often disassembled and sold for parts, making recovery challenging. In contrast, friends offered more practical technical advice. They recommended tracking the device and remotely locking it when possible. If devices were capable, they also suggested activating Lost Mode, which would display a message on the device indicating that it is lost and providing contact information for the owner. In terms of tangible assistance, family and friends offered support by helping to file a police report, ensuring that the authorities received all the necessary details. P16 said that, in more conservative cultures that they are part of, women are unable to file police reports by themselves and rely on family members for assistance. Finally, the police assisted P12 after they had managed to track their phone by ensuring safety when it came time to confront the thief, ultimately helping them recover their stolen phone from the attackers.

Advice Perception

The support participants received from their family was largely emotional rather than technical, which helped them cope with frustration and helplessness. Participants valued this moral support, as it provided relief during a difficult time. However, the advice was often perceived as unhelpful, being either too generic or already known.

Tech-savvy individuals sought information online. Participants also reached out to the police, but typically found these interactions not helpful. They felt that police responses were inadequate, with the authorities clarifying that they could not assist in tracking down their device. As such, most regarded filing police reports as a mere formality.

4.2.7 Problems Faced

Participants experienced a loss of access to essential services that impact daily life, such as banking, social media, and transportation. P1 noted this saying, ‘*I couldn’t access my online banking, because I have to log in with my phone [...] and I also had my ticket for public transport on my phone, so when I went home, I was without a ticket.*’ Furthermore, participants noted the loss of important documents, alongside difficulties logging out of their accounts.

Participants mentioned utilizing 2FA on accounts they deemed important. However, for some, this 2FA was linked to the stolen phone number, complicating matters further and, in some instances, completely logged them out of their accounts (n=8; P1 - P3, P5, P10, P11, P13, P15). This situation created numerous issues when trying to log in and out of accounts, prompting the need to change passwords for critical accounts, such as their Apple account.

> “*I thought logging in to the Apple ID from another phone would help with Find My and tell my phone’s location [...], but the OTP was sent to the stolen phone.*”P13

To address this issue, participants often required a replacement SIM card. This proved challenging for some, as they were not in their home country, and their SIMs were tied to their national identity.

Summary

In response to RQ2, participants expressed concern primarily over the loss of photos and the possibility of unauthorized access to these images, which they viewed as a violation of privacy. In terms of immediate actions, participants attempted to track their phones and activated the Lost Mode. They felt that these steps helped them regain control over their device and mitigated the risk of a privacy breach. When confronted with theft, most participants turned to family and friends for advice.

4.3 Post-Theft Phase

Next, we explore the post-theft phase as illustrated in Figure 2. We discuss the privacy threats and harms that participants endured, and their journey to recovery.

4.3.1 Privacy Threats

Participants talked about the different privacy risks they encountered. Phishing links were highlighted as one of the most pressing concerns. Some participants reported receiving a phishing link a few days after the theft (n=6; P6 - P8, P11 - P13). This link was either sent via SMS to their new SIM card or to the number they provided in the Lost Mode details. The message appeared to come from someone impersonating Apple Customer Service, claiming the need to ‘confirm their identity’ by asking them to sign into their Apple account.

The link redirected them to a fraudulent website designed to steal their credentials. Once the attackers obtained the credentials, they logged into the victims' accounts and removed the device, allowing them to reactivate and resell the iPhone.

> "*I received a message on my phone on my number which I ported, that your phone has been located. Kindly log in to the iCloud account. When I opened that link, it was literally the same as the iCloud sign-in page.*"P13

While some participants, such as P7, fell victim to this scheme and had their lost phones removed from their Apple accounts, others managed to avoid this situation thanks to prior knowledge of similar phishing attempts or warnings from acquaintances. For instance, one participant shared that their brother, who previously experienced the theft of his iPhone, was instrumental in helping them recognize the scam.

> "*I had my brother with me, and previously his phone was also stolen. He said, No, it's fake! He had logged in to that website when his phone was stolen, and his phone was removed from Find My immediately.*"P13

Additionally, a few participants reported incidents of impersonation, where attackers scammed their family members and relatives (n=2; P2, P3). P2 shared their experience with this type of social engineering attack, receiving calls and messages requesting money under false pretenses saying '*We received lots of calls. They were asking for money.*'

4.3.2 Harms

The theft of a mobile phone can result in various forms of harm to individuals. Drawing inspiration from the work of Agrafiotis et al. [2], we categorized these harms into five dimensions relevant to our context.

- *Economic Harm*: Refers to any financial losses as a result of phones being stolen.
- *Psychological Harm*: Includes the mental health implications, the effects of a digital detox, and coping mechanisms following the theft.
- *Reputational Harm*: Involves the loss of reputation in the eyes of family, friends, and employers.
- *Privacy Harm*: Encompasses identity theft, unauthorized access to accounts, and leakage of sensitive information.
- *Physical Harm*: Refers to any physical harm that arises due to the theft of the phone.

After discussing these harms, we asked participants to share their experiences. Most participants emphasized the economic impact, citing the costs of buying a new phone (n=13; P1 - P7, P10, P11, P13, P14, P16, P17). Additionally, many recounted the psychological harm, expressing ongoing anxiety about whether their phone would be recovered and if attackers could access their personal information, thereby compromising their privacy (n=13; P1 - P7, P9, P10, P12 - P14, P17).

> "*I was freaking out the entire time and trying to see where these thieves are because I think it's just different knowing that your phone is in a friend's hand versus someone you don't know.*"P12

We enquired participants about the effect of digital detox due to phone theft. Contrary to voluntary digital detox, phone theft forces an abrupt and anxious disconnection [51]. Because people are so accustomed to having their phones constantly with them, the sudden absence can intensify feelings of anxiety, loss, and disorientation. Participants generally agreed that this forced period of digital detox had a negative effect on them rather than a positive one.

About half of our participants endured reputational harm, facing blame and being labeled as careless (n=12; P1 - P7, P12 - P14, P16, P17). P12 shared, '*My mom was criticizing me, saying, why do you leave your things everywhere? I think it might become a trust issue for her.*'

More importantly, participants from more conservative backgrounds expressed concerns about the reputational risks associated with potential leaks of their photos to family and acquaintances. They feared consequences if their community became aware of their personal lives.

> "*I was also worried because in my gallery I have some photos [...]. My home country is conservative, and romantic relationships are not widely accepted.*"P2

While participants were uncertain about whether they had experienced any privacy harm, they expressed concerns about potential risks and hoped that their protective measures could prevent attackers from accessing their stolen phones. Only one participant reported experiencing physical harm; P8 sustained a small cut on their ear when attackers snatched the phone from their grasp, leaving a minor scar.

4.3.3 Recovery

For about half of our participants, the journey to recovery began with the purchase of a new device (n=12; P1 - P6, P9, P11, P13, P14, P16, P17). They subsequently set about reinstalling apps and regaining access to important services. This process proved challenging for some, as they faced hurdles in authenticating. Risk-based authentication (RBA) triggered by their new device often made it more difficult. Banking and payment apps were particularly cumbersome to restore, as they required extensive checks.

Foreigners faced extra challenges as many of their accounts and services were tied to national identity. They also struggled to contact family and friends, fearing their loved ones might panic if they could not reach them. Moreover, social structures of the host country added another layer of complexity.

> "*My parents will be trying to reach me. And if they're not able to contact me, they might think of the worst.*"P9

Among all participants, only three managed to retrieve their phones, made possible by immediate access to a device al-

ready logged into their personal account. P7 had a phone, P12 a laptop, and P15 an iPad with them at the time of the theft, all logged into their accounts. As soon as they realized their phone was stolen, they activated Lost Mode using these secondary devices, leaving a message saying the phone had been stolen. P12 recounted how the police assisted in recovering the phone after it was marked as lost, while P15 noted their phone was placed in a "Lost and Found" at a train station.

4.3.4 Misconceptions

Based on the mental model participants held during the theft phase (see Section 4.2.3), we now address some misconceptions that emerged afterward in the post-theft phase. While mental models reflect participants' broader beliefs about phone theft, misconceptions involve specific interpretations contributing to increased vulnerability. P13 mentioned that they chose not to freeze their bank account, awaiting a sign from the thief that the phone was active and in use. Similarly, P12 indicated that they refrained from freezing their cards for fear of losing access to their funds. Additionally, P6 opted not to freeze their cards, deeming it too inconvenient.

P12 held the misconception that their SIM card was necessary for the phone tracking application, which deterred them from freezing their SIM. They also expressed indifference towards potential misuse of their number, citing an unlimited contract with their wireless carrier. Modern phones can be tracked offline [64] without a SIM card using Wi-Fi and Bluetooth networks. They can communicate with nearby devices to send the location of the missing device to the Find My network. Both P5 and P12 chose not to erase the data, hoping to recover their devices. They expressed that doing so would contradict their temperament, as deleting all the data would signify acceptance of their phone's permanent loss.

> "*I haven't erased my device. Based on my temperament, I wouldn't erase that device. Because if I did, then it would really 100% be a lost cause and I would never get it back. But I feel like if I kept my account, there might be an off chance that I could track it back.*"P12

Alarmingly, participants expressed frustration and annoyance with two-factor authentication, as it was sending one-time passwords to their stolen phones. They argued that while 2FA is designed to enhance security, it can ultimately work against users in this case. P13 even went on to say that turning on 2FA for their Apple account was a mistake.

> "*I think 2FA is supposed to protect me, but it doesn't help me and ends up making me feel vulnerable.*"P2

4.3.5 Protection Measures

In the aftermath of the theft, we observed a noticeable shift in the protective strategies employed by participants compared to pre-theft, as in Section 4.1.4 (Measures Against Theft). Prior to the incident, most participants relied on basic technical measures, such as their screen lock. However, in the post-theft phase, interviewees increasingly turned to non-technical measures. Participants acknowledged that while their phone usage habits largely remained unchanged, they began to avoid situations that previously made them vulnerable.

For instance, P13 noted that they refrain from using their phone in public or crowded settings, like concerts. P6 and P11 mentioned that they consistently keep their phones with them instead of placing them down in locations such as restaurant tables. P17 expressed heightened awareness of individuals who come too close and make physical contact. P19 mentioned that they now keep a cheap *burner phone* with limited capabilities when visiting crowded areas. Lastly, P9 stated that they no longer keep their phone in their back pocket and now use covers to obscure the brand of the phone, remarking, '*I use a cover which doesn't show that it's an iPhone.*'

Based on our interviews, we theorize that the experience of losing a phone is full of challenges, compounded by the fact that a phone serves as an extension of one's digital identity. Consequently, participants prefer to address the threat of theft through non-technical measures, which ideally prevents it from happening in the first place. As a result, participants invest significantly more effort into non-technical strategies rather than focusing on more advanced technical protection.

Summary

In response to RQ3, many participants described experiencing psychological harm as a result of the anxiety linked to the theft. Several iPhone users reported threats targeting Activation Lock, by means of phishing links and scam calls that they received pretending to be from Apple Inc. Recovery on a new device proved challenging due to the obstacles presented by 2FA and RBA. Consequently, some participants developed the misconception that 2FA was not serving as a protection, but rather working against their interests.

4.4 Process Flow Analysis

To look for behavioral cues in how people react and what actions they take, we visualize all steps in Figure 3. Participants adopted a combination of technical and non-technical actions.

Regarding technical measures, most participants attempted to track their phones or activate Lost Mode. A smaller number opted to change their passwords following the theft. Only 4 out of 20 participants executed a remote wipe or logged the phone out of their accounts. Upon further inquiry, the others expressed a reluctance to lose the data stored on their phones. Likewise, most participants showed unwillingness to change their passwords, demonstrating a tendency to stick with their current ones. On the other hand, regarding non-technical measures, nearly all participants contacted their carrier to freeze the stolen SIM card and acquire a new one. This step was considered crucial for recovering the second authentication factor

Figure 3: An overview of the actions taken by our participants in response to smartphone theft.

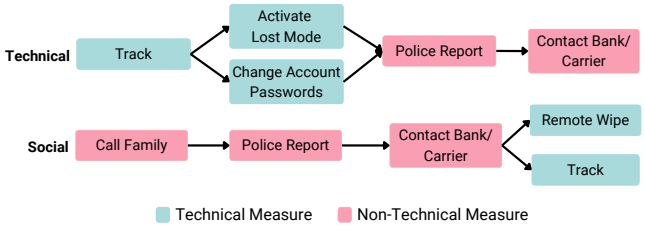


Figure 4: Aggregated process models illustrating the behaviors participants adopted. The figure visualizes major behavioral patterns that emerged from participants' actions: One primarily focused on technical actions such as tracking and activating lost mode, and another driven by social or institutional responses like contacting family and filing a police report. While the individual sequences of actions varied (see Appendix F), these two overarching patterns reflect distinct behaviors in which participants reacted to phone theft.

linked to their accounts. Many participants filed a police report, although this was primarily a precautionary measure in case their phone would ever be used for malicious activities.

To better understand the process flow, we reintroduced the actions into the temporal context and traced the chain of actions performed rather than treating them as isolated events. The most frequently occurring initial technical actions included tracking phones and activating Lost Mode, while the predominant non-technical initial steps involved filing a police report and contacting wireless carriers. We examined the sequence of events for each of these actions to identify the most common steps, as outlined in Appendix F.

By aggregating the sequence of actions participants took, we developed high-level behavioral patterns based on their technical knowledge and preparedness. We identified two distinct patterns, as shown in Figure 4. These patterns represent different approaches, highlighting two tendencies: (i) individuals who initiate action independently through technical means as opposed to (ii) those who begin through social means. Our analysis revealed that the exact order of events is not critical. For instance, whether or not they filed a police report first did not significantly impact outcomes. Thus, the temporal aspect is not overly important as long as some actions have been taken. Instead, the key distinction lies in whether the actions are driven by technical means or by social dynamics.

4.5 Perceived Risks to Applications

Towards the end, we introduced the participants to a *hypothetical scenario* in which they were asked to imagine their current phone had been stolen. In this hypothetical scenario, they should imagine that the thief also had access to the phone's PIN, granting full access to their device. Participants were encouraged to immerse themselves in this scenario, reflect on potential harms (see Section 4.3.2), and review their currently installed applications to evaluate the specific risks associated with each app. It became apparent that participants often forgot about the various applications on their phones, requiring them to frequently check their devices to remember the different ways attackers could inflict harm. Participants overlooked the email access, failing to consider the risks associated with attackers misusing it to reset passwords.

We also inquired participants about the most critical applications they would not want attackers to access to perceive which applications they deemed the most important. The results of this experiment are shown in Figure 5. While we report numbers in the figure, our qualitative data is not suitable for drawing direct numerical comparisons, considering the confounding demographic of participants. Instead, our data identifies broader overarching patterns and trends. Financial applications topped the list for most, as participants expressed concerns that attackers could exploit them for unauthorized transactions. This perspective corroborates the worst fears pre-theft as reported in Section 4.1.3. Many participants also viewed messaging and photo-sharing applications as crucial, arguing that both contain private content they would prefer attackers not to access or, worse, release online. Concerns were also raised about social media, particularly the potential scenario in which attackers could post content that harms

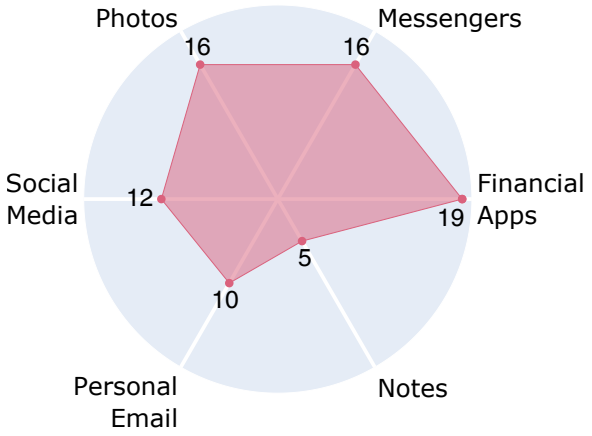


Figure 5: Participants' most critical phone apps to protect from unauthorized access (based on a hypothetical scenario).

their reputation. About half of the participants identified personal email as critical. Beyond the usual privacy concerns about email breaches, they noted that most online services are linked to email addresses, implying that access to their email account could facilitate password resets for those services. Finally, some participants highlighted the importance of their notes app, as they used it to record important work-related information and even store passwords [81].

5 Discussion

Our findings revealed that while numerous protective and recovery measures are in place for smartphone theft, they tend to be overly complicated due to the involvement of different stakeholders like phone vendors, app developers, wireless carriers, financial institutions, and law enforcement.

The actions that need to be taken are not clearly defined and despite their existence, people still experience panic and helplessness, which indicates a deeper issue. This issue is further illustrated by the majority of our participants, whose phones were permanently lost and never retrieved. It reflects a broader failure of existing systems in supporting users under stress, especially when actions are distributed across platforms and services. Our work highlights how this problem stems from a combination of technological and social factors. Next, we discuss our findings, give recommendations, and outline future work.

5.1 Gaps in Readiness

People were unprepared for the theft of their device, not due to a lack of concern, but because theft felt unlikely in everyday use. They exhibited an inherent optimism bias [104], believing that they are unlikely to experience theft and tended to downplay the risk. This optimism is not limited to mobile phones but reflects a broader trend in other domains, such as privacy behaviors [23] and bicycle theft [25, 88], where even effective deterrents are ignored due to underestimated risk. Psychological analyses [32, 54] show that being unprepared due to underestimating risks is common. This is particularly true for phone theft, as the lack of strong cues or requirements from vendors to encourage preventive measures worsens unpreparedness. To combat this behavior, prior work has explored the role of loss aversion [91], showing that users are more likely to take protective actions when the potential consequences of inaction are clearly articulated [98, 107]. However, existing phone theft protection measures are not framed or presented this way. This disconnect between available protections and everyday user behavior highlights the need for more proactive, context-aware interventions. Next, we present actionable recommendations for stakeholders across the mobile ecosystem to better support users in the event of phone theft.

5.2 Better Assisting End-Users

Our study demonstrates how support for users can be improved before, during, and after theft incidents. While motivated to protect themselves, our participants encountered barriers in using the existing measures. Below, we outline recommendations rooted in our data, grouped by key stakeholders and their ability to address the problems surfaced.

Phone Vendors. Uncertainty about data backups made participants reluctant to perform remote wipes. To address this, devices should display backup metadata during actions like remote wipe (e.g., "Last backup: 2 days ago. Your photos and apps are safe. You can use it to set up a new device."). This contextual reassurance could help reduce panic and encourage a timely response. Our participants also described situations where they would have benefited from stricter security in crowded spaces (e.g., concerts or public transport) where the threat of shoulder surfing is elevated. Vendors could introduce a high-risk mode that temporarily enforces biometric authentication for sensitive actions. In contrast to iOS's Stolen Device Protection [7] or Android's Identity Check [45], it should extend to assets our participants cared about, such as photos and third-party apps handling sensitive or financial data. It could be triggered by contextual cues such as location, time of day, scheduled events, or inferred from wallet items such as tickets. Our participants reported reaching out to family and friends in the aftermath of phone theft. Recovery infrastructure should acknowledge that people often rely on their societal network immediately after theft. Vendors could support this by allowing trusted contacts to trigger emergency actions such as locking the phone remotely or verifying identity, offering a fallback when users lack quick access to a second device. Our participants were unsure regarding the purpose and functioning of protection features such as Find My, highlighting the need for more explicit onboarding. Rather than relying on user initiative, vendors could explain features like offline tracking during the initial device setup with a short

real-world scenario explaining how it supports them in case of theft. Finally, thieves attempted to gain access to accounts of stolen phones by sending phishing messages or socially engineered SMS to victims. These messages often urged recipients to remove the phone from their account, thereby unlocking functionality and increasing the resale value. To mitigate this, vendors could enforce stricter controls on device de-registration, such as requiring a phishing resistant factor or only allowing such actions from previously used devices and trusted locations [35].

App Developers. Apps on stolen phones often remain logged in, which can put users' accounts at risk. Participants in our study struggled to identify which of their accounts might be vulnerable. To better support account remediation [76], apps and connected services should list active sessions and offer an emergency option to revoke access. A few of our participants were unsure whether only their phone had been stolen or if the lockscreen PIN had also been compromised. This uncertainty increases anxiety, as people often reuse the same PIN across multiple high and low-valued accounts [55], raising the potential consequences of phone theft. As such, developers should warn about reusing the lockscreen PIN during app and account setup. Participants also struggled with out-of-band authentication mechanisms, especially when traveling. Securing accounts was often hindered as the stolen phone still had access to factors like email, SMS, or push notifications [4]. To mitigate this, apps should offer alternative recovery options [56].

Wireless Carriers and Banks. Participants contacted their banks and carriers immediately following theft but faced friction in verification. While users depend on their phones to access essential services like banking and communication, services often lack robust fallback identity verification. Providers need to reduce reliance on using phone numbers as identifiers [65] and proactively test their verification options with a phone theft scenario. Additionally, banks should reassure people that freezing an account does not result in loss of funds, but instead helps prevent unauthorized access to their finances.

Law Enforcement and Policymakers. National-level tools such as Brazil's Celular Seguro app [44], India's CEIR portal [52], and the U.S. IMEI checker [99] offer models for centralized reporting and blocklisting. Especially, Brazil's app demonstrates the value of collaborative actions, where law enforcement, wireless carriers, and financial institutions work together to combat phone theft. Encouraging such collaboration between stakeholders is essential to streamline theft responses and minimize harm. At the same time, policymakers must address how stolen phones are monetized by disassembling and shipping them abroad quickly [34]. Recent measures, such as Apple's enforcement of Activation Lock on individual components [29], represent a meaningful shift toward limiting the profitability of stolen parts. Still, widespread adoption will require time and raise concerns around repairability and sustainability [103]. Additionally, participants perceived the received advice as too generic. This points to a need for a service that can provide more tailored guidance to people dealing with phone theft. Agencies such as consumer protection groups [24] could develop a platform to support victims of smartphone theft. This service could offer step-by-step procedural guidance tailored to the user's specific situation, along with emotional support to help them navigate this challenging experience.

5.3 Exploring Evolving Threat Models

Our findings point to several important avenues for future research in exploring evolving threat models. We anticipate two distinct types of threat models when it comes to smartphone theft: (i) hardware-related risks, such as the resale of the phone or its parts, and (ii) more sophisticated forms of misuse that exploit access to phone contents requiring knowledge of screen-locking secrets and leading to more severe consequences including financial loss, leakage of sensitive information, or even identity theft. While our study primarily focused on the first threat model, recent reports have highlighted the second as an emerging concern [77, 93, 94]. Recognizing this risk, future quantitative studies should explore the frequency and broader implications of these more sophisticated threat models along with the effectiveness and real-world usage of protection mechanisms. Additionally, many theft protection features are less accessible or entirely unavailable on budget phones. We open this up for future work to consider how protective technologies can be made more inclusive across devices. Finally, theft scenarios involving phones shared among family members or used for business need to be studied, as they comprise different social norms and threat models.

6 Conclusion

Despite having technological measures to protect information, our research indicates that victims still feel helpless due to their unpreparedness, the significant task overhead, and having to reach out to multiple stakeholders separately when dealing with smartphone theft. We must ensure that people feel supported and that their cognitive load is minimized in such challenging situations. Achieving this goal requires not only design changes but also a societal shift to reassure people that it is not embarrassing to have their phones stolen, thereby reducing the potential for harm. By providing a clear set of actionable steps along with psychological support, we can help users navigate this challenging ordeal more effectively.

7 Ethics Considerations

Our university's ethical review board (ERB) granted approval for our study design, the survey material, and our interview guideline. Throughout the research, we took steps to minimize the collection of personally identifiable information (PII) and restricted access to non-anonymized data to a limited number of individuals. We ensured that all data storage and processing complied with GDPR requirements. We recognized that discussing the phone theft incident might be challenging for participants and could evoke unpleasant memories. Therefore, at this stage of the interview, we provided a content warning and reiterated that participants had the option to pause the interview or skip questions at any time without explanation. We also encouraged participants to inform us if they felt uncomfortable sharing any details. None of our participants stopped the interview and were open to sharing their experiences. At the conclusion of the interview, we shared security and privacy advice with our participants on how to protect themselves in the event their smartphone is stolen. This guidance was presented through a website that detailed essential steps for safeguarding their phone, including measures to take before it is lost and important actions to follow after a loss. Additionally, we provided participants with an emergency kit that they could fill in, print, and store in a secure location. The emergency kit contained crucial information, such as the IMEI number, that individuals would need should their phone go missing. Beyond meeting the approval of our institution, we worked to uphold the ethical principles outlined in the Menlo Report [100].

8 Open Science

In alignment with the principles of open science, we will provide research artifacts to facilitate the reproduction and validation of our results. To support transparency and reproducibility, we share the following artifacts, available at: https://doi.org/10.5281/zenodo.15576154

- *Consent Form*: The consent form used to obtain informed consent.
- *Interview Guide*: The complete semi-structured interview protocol used to conduct interviews.
- *Codebook*: The full codebook used for analyzing the interview transcripts.
- *Recruitment Materials*: The original website and flyer utilized for participant recruitment.
- *Phone Theft Emergency Kit*: A practical resource designed to assist individuals in preparing and responding to phone theft incidents.
- *Help Website*: A dedicated website offering additional information and guidance on preventing and mitigating phone theft.
- *Smartphone Usage Habits*: A complete list of all apps and features participants reported using or having installed on their devices.
- *Process Flow*: A diagram visualizing the sequence of actions participants took in response to phone theft, highlighting the most common combination of technical and social steps.

We do not share interview transcripts because of the sensitive nature of the experiences shared by our participants. Completely anonymizing these transcripts would significantly lower the meaning and value of the data. Additionally, our institutional ERB requires strict confidentiality for all data provided by participants. During the consent process, participants were assured that their raw interview data would be kept confidential. Maintaining this confidentiality encouraged honest and open responses about this distressing experience.

Acknowledgments

We thank Helene Nuettgens for her time and support in developing the Help Website and other materials used in this study. We also thank the reviewers for their valuable and constructive feedback, which helped us improve the paper. Finally, we thank the participants for sharing their experience.

References

[1] Desiree Abrokwa, Shruti Das, Omer Akgul, and Michelle L. Mazurek. Comparing Security and Privacy Attitudes Among U.S. Users of Different Smartphone and Smart-Speaker Platforms. In *Symposium on Usable Privacy and Security*, SOUPS '21, pages 139–158, Virtual Conference, August 2021. USENIX.

[2] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate. *Journal of Cybersecurity*, 4(1):1–15, October 2018.

[3] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "...better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In *Symposium on Usable Privacy and Security*, SOUPS '17, pages 49–63, Santa Clara, California, USA, July 2017. USENIX.

[4] Sabrina Amft, Sandra Höltervennhoff, Nicolas Huaman, Alexander Krause, Lucy Simko, Yasemin Acar, and Sascha Fahl. "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. In *ACM Conference on Computer and Communications Security*, CCS '23, pages 3138–3152, Copenhagen, Denmark, November 2023. ACM.

[5] Android Open Source Project. Android 15 – "Vanilla Ice Cream": GateKeeper – ComputeRetryTimeout Function, February 2023. https://android.googlesource.com/platform/system/gatekeeper/+/refs/heads/android15-release/gatekeeper.cpp#295, as of June 12, 2025.

[6] Apple Inc. Find Your Lost iPhone or iPad, September 2024. https://support.apple.com/101593, as of June 12, 2025.

[7] Apple, Inc. iOS: About Stolen Device Protection for iPhone, December 2024. https://support.apple.com/120340, as of June 12, 2025.

[8] Apple, Inc. iOS: Activation Lock for iPhone and iPad, February 2024. https://support.apple.com/108794, as of June 12, 2025.

[9] Apple, Inc. iOS: Apple Platform Security Guide, December 2024. https://support.apple.com/guide/security/, as of June 12, 2025.

[10] Apple, Inc. iOS: Restore Your iPhone, iPad, or iPod Touch from a Backup, September 2024. https://support.apple.com/118105, as of June 12, 2025.

[11] Apple, Inc. iOS: Locate a Device in Find My on iPhone, January 2025. https://support.apple.com/guide/iphone/locate-a-device-iph09b087eda/, as of June 12, 2025.

[12] Bailey, Daniel V. and Munyendo, Collins W. and Dyer, Hunter A. and Grant, Miles and Markert, Philipp and Aviv, Adam J. "Someone Definitely Used 0000": Strategies, Performance, and User Perception of Novice Smartphone-Unlock PIN-Guessers. In *European Symposium on Usable Security*, EuroUSEC '23, pages 158–174, Copenhagen, Denmark, October 2023. ACM.

[13] Rosaline S. Barbour. Checklists for Improving Rigour in Qualitative Research: A Case of the Tail Wagging the Dog? *The BMJ*, 322(7294):1115–1117, May 2001.

[14] Dario Bertini. Fairphone Lack of Support for Quick Remote Lock (Part of the New Theft Protection Features), November 2024. https://forum.fairphone.com/t/fairphone-lack-of-support-for-quick-remote-lock-part-of-the-new-theft-protection-features, as of June 12, 2025.

[15] J. D. Biersdorfer. How to Prepare for a Lost, Stolen or Broken Smartphone, February 2023. https://www.nytimes.com/2023/02/08/technology/personaltech/what-to-do-lost-stolen-smartphone.html, as of June 12, 2025.

[16] Bitkom e. V. The End of Smartphones: Stolen, Lost, Broken, February 2023. https://www.bitkom.org/Presse/Presseinformation/Smartphone-Gestohlen-verloren-kaputt, as of June 12, 2025.

[17] Ron Bitton, Kobi Boymgold, Rami Puzis, and Asaf Shabtai. Evaluating the Information Security Awareness of Smartphone Users. In *ACM Conference on Human Factors in Computing Systems*, CHI '20, pages 1–13, Honolulu, Hawaii, USA, April 2020. ACM.

[18] Virginia Braun and Victoria Clarke. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2):77–101, July 2006.

[19] British Broadcasting Corporation (BBC), UK. What to Do If Your Phone Is Stolen, November 2024. https://www.bbc.co.uk/programmes/articles/4SRrKX6GQdcqsGGNz4tvmqk/what-to-do-if-your-phone-is-stolen, as of June 12, 2025.

[20] Jiayi Chen, Urs Hengartner, Hassan Khan, and Mohammad Mannan. Chaperone: Real-time Locking and Loss Prevention for Smartphones. In *USENIX Security Symposium*, SSYM '20, pages 325–342, Virtual Conference, August 2020. USENIX.

[21] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. On the Impact of Touch ID on iPhone Passcodes. In *Symposium on Usable Privacy and Security*, SOUPS '15, pages 257–276, Ottawa, Canada, July 2015. USENIX.

[22] Geumhwan Cho, Jun Ho Huh, Soolin Kim, Junsung Cho, Heesung Park, Yenah Lee, Konstantin Beznosov, and Hyoungshick Kim. On the Security and Usability Implications of Providing Multiple Authentication Choices on Smartphones: The More, the Better? *ACM Transactions on Privacy and Security*, 23(4):22:1–22:32, November 2020.

[23] Hichang Cho, Jae-Shin Lee, and Siyoung Chung. Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience. *Computers in Human Behavior*, 26(5):987–995, September 2010.

[24] Citizens Advice, UK. What to Do If Your Mobile Phone Is Lost or Stolen, August 2024. https://www.citizensadvice.org.uk/consumer/phone-internet-downloads-or-tv/what-to-do-if-your-mobile-phone-is-lost-or-stolen/, as of June 12, 2025.

[25] Achituv Cohen, Trisalyn Nelson, Moreno Zanotto, Dillon T. Fitch-Polse, Lizzy Schattle, Seth Herr, and Meghan Winters. The Impact of Bicycle Theft on Ridership Behavior. *Journal of Sustainable Transportation*, 18(5):453–463, May 2024.

[26] CTIA, Wireless Association, USA. Protecting Your Data, April 2024. https://www.ctia.org/consumer-resources/protecting-your-data, as of June 12, 2025.

[27] Trajce Dimkov, Wolter Pieters, and Pieter Hartel. Laptop Theft: A Case Study on the Effectiveness of Security Mechanisms in Open Organizations. In *ACM Conference on Computer and Communications Security*, CCS '10, pages 666–668, Chicago, Illinois, USA, October 2010. ACM.

[28] Dixon, Matt and Sillence, Elizabeth and Nicholson, James and Coventry, Lynne. Better the Devil You Know: Using Lost-Smartphone Scenarios to Explore user Perceptions of Unauthorised Access. In *European Symposium on Usable Security*, EuroUSEC '23, pages 86–96, Copenhagen, Denmark, October 2023. ACM.

[29] Filipe Espósito. Apple Brings Activation Lock to iPhone Parts, September 2024. https://9to5mac.com/2024/09/12/apple-activation-lock-iphone-parts/, as of June 12, 2025.

[30] Jacob Evans. Phone Reported Stolen in London Every Six Minutes, April 2023. https://www.bbc.com/news/uk-england-london-65105199, as of June 12, 2025.

[31] Federal Communications Commission (FCC), USA. Protect Your Smart Device, December 2019. https://www.fcc.gov/consumers/guides/protect-your-mobile-device, as of June 12, 2025.

[32] Baruch Fischhoff. *Risk Perception and Communication*, chapter 1, pages 1–30. Taylor & Francis, London, United Kingdom, 1 edition, 2011.

[33] Robert J. Fisher. Social Desirability Bias and the Validity of Indirect Questioning. *Journal of Consumer Research*, 20(2):303–315, September 1993.

[34] Graham Fraser and Tom Gerken. Thieves Snatched His Phone in London: It Was in China a Month Later, September 2024. https://www.bbc.com/news/articles/c3rdy132q3lo, as of June 12, 2025.

[35] Suzanne Frey. Android's Theft Protection Features Keep Your Device and Data Safe, May 2024. https://blog.google/products/android/android-theft-protection/, as of June 12, 2025.

[36] Andrea Gallardo, Hanseul Kim, Tianying Li, Lujo Bauer, and Lorrie Cranor. Detecting iPhone Security Compromise in Simulated Stalking Scenarios: Strategies and Obstacles. In *Symposium on Usable Privacy and Security*, SOUPS '22, pages 291–312, Boston, Massachusetts, USA, August 2022. USENIX.

[37] Christine Geeng, Mike Harris, Elissa M. Redmiles, and Franziska Roesner. "Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *USENIX Security Symposium*, SSYM '22, pages 305–322, Boston, Massachusetts, USA, August 2022. USENIX.

[38] Google Inc. Protect Your Personal Data Against Theft, September 2024. https://support.google.com/android/answer/15146908, as of June 12, 2025.

[39] Google, Inc. Android: Back Up or Restore Data on Your Android Device, January 2025. https://support.google.com/android/answer/2819582, as of June 12, 2025.

[40] Google, Inc. Android: Find, Secure, or Erase a Lost Android Device, January 2025. https://support.google.com/android/answer/6160491, as of June 12, 2025.

[41] Google, Inc. Android: How Find My Device Protects Your Data, January 2025. https://support.google.com/android/answer/14796936, as of June 12, 2025.

[42] Leonid Grustniy. What to Do If Your Phone Gets Stolen, June 2021. https://www.kaspersky.com/blog/what-to-do-if-your-smartphone-is-stolen/40148/, as of June 12, 2025.

[43] GSMA Device Security Group. Mobile Device Theft: State of Affairs Report, February 2025. https://www.gsma.com/solutions-and-impact/industry-services/device-services/mobile-device-theft-state-of-affairs-report, as of June 12, 2025.

[44] Joan Royo Gual. Brazil Creates an App to Block Stolen Cell Phones: 'They Will Be a Useless Piece of Metal', December 2023. https://english.elpais.com/international/2023-12-20/brazil-creates-an-app-to-block-stolen-cell-phones-they-will-be-a-useless-piece-of-metal.html, as of June 12, 2025.

[45] Jianing Sandra Guo and Nataliya Stanetsky. Android Enhances Theft Protection with Identity Check and Expanded Features, January 2025. https://security.googleblog.com/2025/01/android-theft-protection-identity-check-expanded-features.html, as of June 12, 2025.

[46] Marian Harbach, Alexander De Luca, and Serge Egelman. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *ACM Conference on Human Factors in Computing Systems*, CHI '16, pages 4806–4817, San Jose, California, USA, May 2016. ACM.

[47] Simon Heath. iPhone Theft and Resulting Loss of Money, Identities and Personal Data, May 2023. https://www.thefinalstep.co.uk/bytesizebulletins/iphone-theft-losing-money-apple-id, as of June 12, 2025.

[48] Monique M. Hennink and Bonnie N. Kaiser. Sample Sizes for Saturation in Qualitative Research: A Systematic Review of Empirical Tests. *Social Science & Medicine*, 292:114523:1–114523:10, January 2022.

[49] Monique M. Hennink, Bonnie N. Kaiser, and Vincent C. Marconi. Code Saturation Versus Meaning Saturation: How Many Interviews Are Enough? *Qualitative Health Research*, 27(4):591–608, September 2016.

[50] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *USENIX Security Symposium*, SSYM '23, pages 2311–2328, Anaheim, California, USA, August 2023. USENIX.

[51] Cynthia A. Hoffner, Sangmi Lee, and Se Jung Park. "I Miss My Mobile Phone!": Self-Expansion via Mobile Phone and Responses to Phone Loss. *New Media & Society*, 18(11):2452–2468, December 2016.

[52] Indian Ministry of Communications. Central Equipment Identity Register, September 2019. https://www.ceir.gov.in, as of June 12, 2025.

[53] Meng Jin, Yuan He, Dingyi Fang, Xiaojiang Chen, Xin Meng, and Tianzhang Xing. iGuard: A Real-Time Anti-theft System for Smartphones. In *IEEE Conference on Computer Communications*, INFOCOM '17, pages 1–9, Atlanta, Georgia, USA, May 2017. IEEE.

[54] Daniel Kahneman and Amos Tversky. Prospect Theory: An Analysis of Decision Under Risk. In Leonard C. MacLean and William T. Ziemba, editors, *Handbook of the Fundamentals of Financial Decision Making*, pages 99–127. World Scientific Publishing, Singapore, July 2013.

[55] Hassan Khan, Jason Ceci, Jonah Stegman, Adam J. Aviv, Rozita Dara, and Ravi Kuber. Widely Reused and Shared, Infrequently Updated, and Sometimes Inherited: A Holistic View of PIN Authentication in Digital Lives and Beyond. In *Annual Conference on Computer Security Applications*, ACSAC '20, pages 249–262, Austin, Texas, USA, December 2020. ACM.

[56] Leona Lassak, Philipp Markert, Maximilian Golla, Elizabeth Stobert, and Markus Dürmuth. A Comparative Long-Term Study of Fallback Authentication Schemes. In *ACM Conference on Human Factors in Computing Systems*, CHI '24, pages 970:1–970:19, Maui, Hawaii, USA, May 2024. ACM.

[57] Xinyu Liu, David Wagner, and Serge Egelman. Detecting Phone Theft Using Machine Learning. In *ACM International Conference on Information Science and Systems*, ICISS '18, pages 30–36, Jeju, Republic of Korea, April 2018. ACM.

[58] Marte Løge, Markus Dürmuth, and Lillian Røstad. On User Choice for Android Unlock Patterns. In *European Workshop on Usable Security*, EuroUSEC '16, Darmstadt, Germany, July 2016. ISOC.

[59] London Metropolitan Police Service (Met Police), UK. Mobile Phone Advice, August 2023. https://www.met.police.uk/cp/crime-prevention/personal-safety-how-to-stay-safe/mobile-phone-advice/, as of June 12, 2025.

[60] Macquarie Group Limited, Australia. What to Do If Your Phone Is Lost, Stolen, or Compromised, October 2024. https://www.macquarie.com.au/help/personal/fraud-disputes-and-security/protecting-your-information/what-to-do-if-your-phone-is-lost-stolen-or-compromised.html, as of June 12, 2025.

[61] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. On the Security of Smartphone Unlock PINs. *ACM Transactions on Privacy and Security*, 24(4):30:1–30:36, September 2021.

[62] Diogo Marques, Tiago Guerreiro, Luis Carriço, Ivan Beschastnikh, and Konstantin Beznosov. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In *ACM Conference on Human Factors in Computing Systems*, CHI '19, pages 589:1–589:13, Glasgow, Scotland, United Kingdom, May 2019. ACM.

[63] Peter Mayer, Yixin Zou, Byron M. Lowens, Hunter A. Dyer, Khue Le, Florian Schaub, and Adam J. Aviv. Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches. *ACM Transactions on Computer-Human Interaction*, 30(5):77:1–77:53, September 2023.

[64] Benjamin Mayo. iOS 15: Find My Network Can Still Find Your iPhone When It Is Powered Off, or Factory Reset, June 2021. https://9to5mac.com/2021/06/07/ios-15-find-my-network-can-find-your-iphone-when-it-is-powered-off/, as of June 12, 2025.

[65] Allison McDonald, Carlo Sugatan, Tamy Guberek, and Florian Schaub. The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling. In *ACM Conference on Human Factors in Computing Systems*, CHI '21, pages 559:1–559:14, Yokohama, Japan, May 2021. ACM.

[66] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. In *ACM Conference on Computer-Supported Cooperative Work and Social Computing*, CSCW '19, pages 72:1–72:23, Austin, Texas, USA, November 2019. ACM.

[67] Melanie Pinola, Consumer Reports, USA. 5 Steps to Protect Your Smartphone From Theft or Loss, October 2022. https://www.consumerreports.org/electronics-computers/cell-phones/steps-to-protect-your-smartphone-from-theft-or-loss-a1204843165/, as of June 12, 2025.

[68] Metropolitan Police Department of the District of Columbia (MPD), USA. Tips for Preventing Theft of Laptops and Personal Electronics, June 2024. https://mpdc.dc.gov/page/tips-preventing-theft-laptops-and-personal-electronics, as of June 12, 2025.

[69] Metropolitan Police Service (Met Police), UK. Mobile Phone Thefts in London in 2022, June 2024. https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2024/june-2024/thefts-mobile-phones-january2017-february2024/, as of June 12, 2025.

[70] Metropolitan Police Service (Met Police), UK. Mobile Phone Thefts in London in 2024, March 2025. https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2025/may-2025/mobile-phones-reported-stolen-january2022-february2025/, as of June 12, 2025.

[71] Jaron Mink, Harjot Kaur, Juliane Schmüser, Sascha Fahl, and Yasemin Acar. "Security is not my field, I'm a stats guy": A Qualitative Root Cause Analysis of Barriers to Adversarial Machine Learning Defenses in Industry. In *USENIX Security Symposium*, SSYM '23, pages 3763–3780, Anaheim, California, USA, August 2023. USENIX.

[72] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders. In *Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '13, pages 271–280, Munich, Germany, August 2013. ACM.

[73] N26, Germany. How to Protect Yourself When Your Phone Is Lost or Stolen, January 2022. https://n26.com/en-de/blog/stolen-phone, as of June 12, 2025.

[74] Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, Gabriel Kaptchuk, and Elissa M. Redmiles. What Are the Chances? Explaining the Epsilon Parameter in Differential Privacy. In *USENIX Security Symposium*, SSYM '23, pages 1613–1630, Anaheim, California, USA, August 2023. USENIX.

[75] Christie Napa Scollon, Chu-Kim Prieto, and Ed Diener. Experience Sampling: Promises and Pitfalls, Strength and Weaknesses. In Ed Diener, editor, *Assessing Well-Being: The Collected Works of Ed Diener*, pages 157–180. Springer, Dordrecht, Netherlands, June 2009.

[76] Lorenzo Neil, Elijah Bouma-Sims, Evan Lafontaine, Yasemin Acar, and Bradley Reaves. Investigating Web Service Account Remediation Advice. In *Symposium on Usable Privacy and Security*, SOUPS '21, pages 359–376, Virtual Conference, August 2021. USENIX.

[77] Nicole Nguyen and Joanna Stern. The iPhone Setting Thieves Use to Lock You Out of Your Apple Account, April 2023. https://www.wsj.com/articles/the-iphone-setting-thieves-use-to-lock-you-out-of-your-apple-account-716d350d, as of June 12, 2025.

[78] NJ TRANSIT Police Department, USA. Smart Phone Theft Prevention, July 2024. https://police.njtransit.com/theft, as of June 12, 2025.

[79] Donny Jacob Ohana, Liza Phillips, and Lei Chen. Preventing Cell Phone Intrusion and Theft Using Biometrics. In *IEEE Symposium on Security and Privacy Workshops*, SPW '13, pages 173–180, San Francisco, California, USA, May 2013. IEEE.

[80] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. Different Researchers, Different Results? Analyzing the Influence of Researcher Experience and Data Type During Qualitative Analysis of an Interview and Survey Study on Security Advice. In *ACM Conference on Human Factors in Computing Systems*, CHI '23, pages 864:1–864:21, Hamburg, Germany, April 2023. ACM.

[81] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why People (Don't) Use Password Managers Effectively. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 319–338, Santa Clara, California, USA, August 2019. USENIX.

[82] Gustavo Petró. Cell Phone Thefts Fall 10% in Brazil, Says Public Security Yearbook, July 2024. https://g1.globo.com/politica/noticia/2024/07/18/roubos-de-celulares-caem-10percent-no-brasil-aponta-anuario-de-seguranca-publica.ghtml, as of June 12, 2025.

[83] Police Service of Northern Ireland (PSNI), UK. Protect Your Mobile Phone and Tablet, September 2022. https://www.psni.police.uk/safety-and-support/keeping-safe/protecting-yourself/out-and-about/protect-your-mobile-phone-and, as of June 12, 2025.

[84] Hari Ravichandran. Stolen Phone? Don't Panic! Follow These 11 Steps Now, January 2023. https://www.aura.com/learn/what-to-do-if-your-phone-is-stolen, as of June 12, 2025.

[85] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. A Summary of Survey Methodology Best Practices for Security and Privacy Researchers. Technical Report CS-TR-5055, University of Maryland, May 2017.

[86] Elissa M. Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L. Mazurek. Asking for a Friend: Evaluating Response Biases in Security User Studies. In *ACM Conference on Computer and Communications Security*, CCS '18, pages 1238–1255, Toronto, Ontario, Canada, October 2018. ACM.

[87] San Francisco Municipal Transportation Agency, USA. Smartphone Safety, September 2024. https://www.sfmta.com/getting-around/safety/safety-education-campaigns/smartphone-safety, as of June 12, 2025.

[88] Marlies Sas, Koen Ponnet, Genserik Reniers, and Wim Hardyns. Nudging as a Crime Prevention Strategy: The Use of Nudges to Improve Cyclists' Locking Behavior and Reduce the Opportunities for Bicycle Theft. *Security Journal*, 35(2):463–485, February 2021.

[89] William Sattelberg. The Demographics of Reddit: Who Uses the Site?, April 2021. https://www.alphr.com/demographics-reddit/, as of June 12, 2025.

[90] Jörg Schieb. Cell Phone Stolen or Lost? What You Can Do Before and After, August 2023. https://www1.wdr.de/nachrichten/handy-geklaut-verloren-was-tun-100.html, as of June 12, 2025.

[91] Ulrich Schmidt and Horst Zank. What is Loss Aversion? *Journal of Risk and Uncertainty*, 30(2):157–167, March 2005.

[92] South Australia Police (SAPOL), Australia. Preventing Crime: Mobile Phone Theft, March 2024. https://www.police.sa.gov.au/__data/assets/pdf_file/0003/1287246/Mobile-Phone-Theft-2023.pdf, as of June 12, 2025.

[93] Joanna Stern and Nicole Nguyen. A Basic iPhone Feature Helps Criminals Steal Your Entire Digital Life, February 2023. https://www.wsj.com/tech/personal-tech/apple-iphone-security-theft-passcode-data-privacya-basic-iphone-feature-helps-criminals-steal-your-digital-life-cbf14b1a, as of June 12, 2025.

[94] Joanna Stern and Nicole Nguyen. Apple Makes Security Changes to Protect Users From iPhone Thefts, December 2023. https://www.wsj.com/tech/personal-tech/apple-iphone-ios-update-stolen-device-protection-698d760e, as of June 12, 2025.

[95] T-Mobile, USA. Lost or Stolen Device Help, September 2024. https://www.t-mobile.com/support/account/lost-or-stolen-device-help, as of June 12, 2025.

[96] Zhiling Tu, Ofir Turel, Yufei Yuan, and Norm Archer. Learning to Cope with Information Security Risks Regarding Mobile Device Loss or Theft: An Empirical Examination. *Information & Management*, 52(4):506–517, June 2015.

[97] Zhiling Tu and Yufei Yuan. Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft. In *IEEE Hawaii International Conference on System Sciences*, HICSS '12, pages 1393–1402, Maui, Hawaii, USA, January 2012. IEEE.

[98] Amos Tversky and Daniel Kahneman. The Framing of Decisions and the Psychology of Choice. *Science*, 211(4481):453–458, January 1981.

[99] U.S. Cellular Telecommunications and Internet Association. Stolen Phone Checker, May 2023. https://stolenphonechecker.org, as of June 12, 2025.

[100] U.S. Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, August 2012. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of June 12, 2025.

[101] Mojtaba Vaismoradi and Sherrill Snelgrove. Theme in Qualitative Content Analysis and Thematic Analysis. *Forum Qualitative Social Research*, 20(3):1–14, September 2019.

[102] Rick Wash, Emilee Rader, and Chris Fennell. Can People Self-Report Security Accurately?: Agreement Between Self-Report and Behavioral Measures. In *ACM Conference on Human Factors in Computing Systems*, CHI '17, pages 2228–2232, Denver, Colorado, USA, May 2017. ACM.

[103] Jess Weatherbed. Oregon's Governor Signs Right-to-Repair Law That Bans 'Parts Pairing', March 2024. https://www.theverge.com/2024/3/27/24097042/, as of June 12, 2025.

[104] Neil D. Weinstein. Unrealistic Optimism About Future Life Events. *Journal of Personality and Social Psychology*, 39(5):806–820, November 1980.

[105] Dan Whitworth. Mobile Fraud: Thieves 'Shoulder Surfing' Victims to Steal Phones, May 2023. https://www.bbc.com/news/business-65456325, as of June 12, 2025.

[106] Zoe Williams. 'They Rob You Visibly, with No Repercussions' – The Unstoppable Rise of Phone Theft, October 2024. https://www.theguardian.com/uk-news/2024/oct/09/they-rob-you-visibly-with-no-repercussions-the-unstoppable-rise-of-phone-theft, as of June 12, 2025.

[107] Kim Witte. Putting the Fear Back Into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, 59(4):329–349, December 1992.

[108] Maximilian Zinkus, Tushar M. Jois, and Matthew Green. Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions. *CoRR*, abs/2105.12613:1–118, May 2021.

A Background: Phone Theft Protection

In this section, we provide an overview of the various theft protection features and advice given to smartphone users. Interested readers can refer to a comprehensive technical description on the security of mobile devices [108].

Traditional Mobile Device Protection

Smartphones have traditionally protected user data in the event of theft through cloud backups, screen locking mechanisms, and device tracking. These features provide a basic level of defense against unauthorized access and misuse.

Screen Locking. To prevent unauthorized access, smartphones implement screen locks such as PINs, passwords, or patterns. Biometric authentication, including fingerprint and face recognition, are widely used to improve unlocking speed and convenience, while also resisting shoulder surfing attacks. However, upon boot, smartphones remain in an encrypted state and cannot be decrypted using biometrics alone. Instead, the PIN is required to derive the cryptographic keys needed to unlock the device, after which biometric authentication becomes available [21]. Therefore, even though users primarily interact with biometric unlocking, the underlying security of the device ultimately depends on the strength of the fallback mechanism. As a result, the guessability of the PIN directly influences the overall security of the phone [61].

Rate Limiting and Blocklisting. Both Apple's iOS and Google's Android operating systems incorporate rate-limiting mechanisms to restrict the number of consecutive incorrect PIN entries. In the case of Android, users are allowed up to five attempts, after which the system imposes a waiting period of 30 seconds before further input is permitted [5]. Once the number of failed attempts exceeds ten, the waiting period increases exponentially [5]. Similarly, iOS employs a rate-limiting mechanism but goes further by completely disabling PIN entry and requiring a device reset after ten consecutive incorrect guesses and by warning the user about "easily guessed" PINs via a blocklist [9]. Prior studies have investigated the security implications of 4-digit and 6-digit PINs under these rate-limiting and blocklisting constraints [61].

Device Tracking. Both Apple and Google have integrated device tracking systems to help users locate and recover lost or stolen devices. These systems enable users to view their device's location on a map [8, 11, 40]. Access to this functionality is available through other devices or the respective Find My websites, provided users are logged into their accounts. Additionally, Find My allows users to mark devices as lost and remotely wipe the phone. Recently, both platforms have extended the functionality to track devices that are offline (i. e., with the SIM card removed or in Airplane mode). Offline tracking uses a crowd-sourced network of nearby devices and Bluetooth signals to collect and relay the location of the device securely via the Find My network [41, 64].

Data Backup. To complement security and recovery mechanisms, many smartphone vendors integrate a backup service. These services enable users to safeguard their data, such as photos, contacts, and documents, by backing them up to cloud storage [10, 39]. Typically, users need to enable cloud backup functionality manually through their device settings. Users can then recover their information by signing into their accounts and activating the recovery feature on their new device.

Advanced Protection Mechanisms

In response to increasingly sophisticated phone theft attacks, in which attackers observe the PIN before stealing the device, vendors have introduced new protection mechanisms that go beyond traditional threat models. For the interested reader, we recommend coverage by the Wall Street Journal, which documents real-world cases of such attacks [77, 93, 94].

Protection Against Compromised PINs. For the threat model in which the PIN is compromised, vendors introduced targeted defenses such as Apple's Stolen Device Protection (SDP) [7] and Google's Identity Check [45]. For critical actions, such as disabling tracking or changing the account password, these protections require biometric authentication and, if attempted from an unfamiliar location, introduce a one-hour delay before the changes take effect.

Hardware Verification and Reset Protection. To deter resale of stolen devices and parts, Apple expanded Activation Lock, enforced after a reset, to cover individual hardware components [29]. This requires the original owner's credentials to verify replacements, preventing unverified parts from working in another device and lowering black market value. Its effect on repairability and the environment is still under evaluation [103]. Similarly, Google introduced Factory Reset Protection, which blocks unauthorized resets by limiting functionality until the original owner confirms their identity. To counter physical access attacks, both Apple and Google implemented automatic reboots after 72 hours of inactivity.

Phone Snatching Detection. To counter phone snatching, Google introduced Theft Detection Lock and Offline Device Lock. These use on-device machine learning to detect theft. The screen locks automatically if sudden movement suggests the phone was grabbed, or if it goes offline, such as through Airplane mode or SIM removal. Google's Remote Lock also lets users lock a device using only their phone number and secret answer to a security question, without needing account access.

App Locking and Private Space. To protect sensitive apps and data, Apple and Google added a second authentication layer, such as App Locking on iOS and Private Space on Android. As of June 2025, only Android lets users set a new (and hopefully different) PIN. iOS uses the device's unlock PIN, making the protection ineffective if that PIN is already known to an attacker.

Phone Theft Advice

To learn more about how one can protect against phone theft, we analyzed help pages and guidelines from

- banks [60, 73],
- consumer protection [24, 31, 67],
- news papers [15, 19],
- phone vendors [6, 38],
- police [59, 68, 83, 92],
- public transportation [78, 87],
- security product vendors [42, 84], and
- wireless carriers [26, 95].

We found advice that started by recommending end-users **not to panic** and double checking that the device is really gone. In contrast to other sources, advice given by the police focused on **being more attentive and aware of the surroundings** when using a phone and to never leave the phone unattended in public spaces. While the advice differed in quality and depth, the majority focused on the following actions and precautions:

- Writing down device identifiers like the **IMEI**, serial number, phone number, and phone vendor/wireless carrier credentials and customer support numbers.
- Setting up a **backup** of photos and important data.
- Configuring a secure **screen lock** (a secure PIN or alphanumeric password), enrolling **biometrics** to securely unlock the phone in public spaces, and enabling **advanced theft protection features**.
- Enabling the phone's **tracking features**, which often include an option to mark a phone as lost to remotely lock the device, leave a message, hide notifications, unlink credit cards, play a loud sound, and **remotely erase the phone**.
- Notifying the **wireless carrier** to freeze the SIM card, suspend services, and block the device and calling the **bank** to freeze or unlink credit cards and monitor the account for suspicious transactions.
- Warning close contacts including **family**, friends, or the employer as a precaution to identity theft and social engineering attacks.
- **Changing passwords** and monitoring accounts for suspicious activity or unauthorized orders.
- Filing a **police** report and informing the **insurance** about the device theft.

We summarized this advice in a form intended to be useful beyond this study, resulting in two research artifacts: Our Phone Theft Emergency Kit, which helps individuals prepare for and respond to phone theft, and our Help Website, which offers additional information on prevention and recovery. We shared both artifacts with our study participants. A download link can be found in Open Science 8.

B Interview Guide

Table 2: Interview guideline for the semi-structured interview (Part 1).

Part	Section	Questions and Explanation
1	**Informed Consent**	*Written and orally.*
2	**Introduction and Agenda**	Thank you for your participation in our interview study about what happens when someone steals your phone. We will start with some general questions regarding stolen smartphones and privacy. Then, we will ask you to describe the incident that led to your phone being stolen. Towards the end of the interview, we will ask you some questions based on some commonly used apps on phones. Before we proceed, please remember that there are no right or wrong answers and we ask you to say anything that comes to your mind. You also don't have to answer any questions that you don't want to. Are you OK to continue? Do you consent to recording this interview?
3	**Warm-Up Phase**	1. How long have you been using a smartphone? 2. What do you generally use your smartphone for? 3. Have you ever lost a smartphone? Follow-up: Was it stolen, or did you simply misplace it? *Make the participants feel comfortable with the interview and try to slowly bring in the main topic.*
4	**Preparation**	1. What do you think happens when somebody steals your phone? 2. What is the worst thing that you can think of if your smartphone is stolen? Follow-up: Why did you come up with these things? Follow-up #2: What about your privacy? *Follow-up #2 only used, if participants did not bring up privacy in the first question.* 3. What steps do you take such that no one can access your smartphone? Follow-up: In case your smartphone gets stolen, how do you make sure that no one other than you can access it? 4. Can you think of ways (e.g., settings on your phone) which make it difficult for people other than you to gain access to your smartphone?
5	**Content Warning and Incident Description**	**CONTENT WARNING: Next I would like to ask you to describe the incident that led to you having your device stolen.** I understand that this may be hard for you and bring back unpleasant memories. At this point, I would like to reiterate that you can pause this interview or skip questions at any time without reason. You can also tell us if you are uncomfortable sharing any details. Are you OK to continue?

Table 3: Interview guideline for the semi-structured interview (Part 2).

Part	Section	Questions and Explanation
6	**Theft Phase**	1. Can you describe the incident which led to you losing your smartphone? Follow-up: How did you feel when that happened? 2. What was your first concern after losing your smartphone? 3. Can you remember if your smartphone was locked or unlocked? 4. Who do you think could have access to your data? *Ask about 2FA, freezing bank cards and SIM card, Apple/Google Pay, backup behavior, Apple/Google account passwords, and password managers.* 5. At the time, were you aware of any settings on your phone that made it difficult for people other than you to gain access to your smartphone? Follow-up: Can you remember if any of these settings were enabled on your smartphone? 6. Can you walk us through the first things you did upon losing your smartphone? 7. How and why did you decide what to do these things first? 8. Did you seek any advice or help? Why/why not? Follow-up: Who or where did you seek advice from? 9. How helpful was the advice you received?
7	**Post-Theft Phase**	1. What actually happened after the incident? (Financial loss, data loss, identity theft?) 2. Did you regain access to your smartphone? 3. Have you changed the way you use your smartphone after this incident? 4. What additional precautions do you take to avoid such an incident? 5. Can you describe your experience trying to recover all the apps you had on your previous device? *Only ask, if participants said that they were not able to recover their device and bought a new one.* Follow-up: Did you face any difficulties? 6. Were you able to re-login to your old apps easily? Follow-up: Did you remember your passwords to re-login to the apps?
8	**Harms and Most Critical Apps**	Having your phone stolen can cause different kind of harms. We have categorized them into 5 dimensions. I will now show them to you by sharing my screen. 1. If you think about your incident, what kind of economic harm did you have to go through? *Now, let's consider the hypothetical situation that the attacker has your PIN.* 2. Can you point to specific applications on your phone which in your opinion can cause these harms? Follow-up: Repeat for each harm.
9	**Cooldown Phase**	Have you heard about what phone companies are doing to protect people in case they lose their phone? *Talk about Stolen Device Protection on iOS and Private Space on Android.*

C Codebook

Table 4: Codes resulting from qualitative data analysis along with their descriptions.

Theme	Sub-Theme	Description
Advice & Help	*Perception*	How the advice and help are perceived by the users.
	Pieces	Different pieces of advice and help available after the theft.
	Sources	Various sources from which advice and help can be sought following the theft.
Theft	*First Response*	The immediate steps or actions the users take after the theft.
	Feelings	Emotional reactions of the users, such as panic or helplessness.
	Context	Location, severity, and other contextual details.
	Initial Concerns	The immediate concerns the users face.
	Mental Model	User's understanding of the factors concerning theft.
Pre-Theft	*Experience*	User's previous experiences with theft or loss.
	Preparedness	Degree to which the user was prepared for theft.
	Usage Habits	User's daily interactions with their phone.
	Worst Fear	User's greatest fear related to losing their phone.
Post-Theft	*Anti-Patterns*	Ineffective actions taken after the theft.
	Problems	Challenges the user faces in the aftermath of the theft.
	Protection Mechanisms	Measures taken post-theft to protect the user from future incidents.
	Recovery	User's journey to recovery, including issues faced.
	Harms	Economic, psychological, reputational, privacy, or physical harm resulting from the theft.
Stakeholders	*Bank*	Bank's role in assisting users with financial losses or securing accounts.
	Carrier	Wireless carriers' involvement in suspending services or providing support.
	Police	Police's role in offering assistance.
	Vendor	Phone vendors' role in recovery or replacement.

D Research Artifact: Phone Theft Emergency Kit

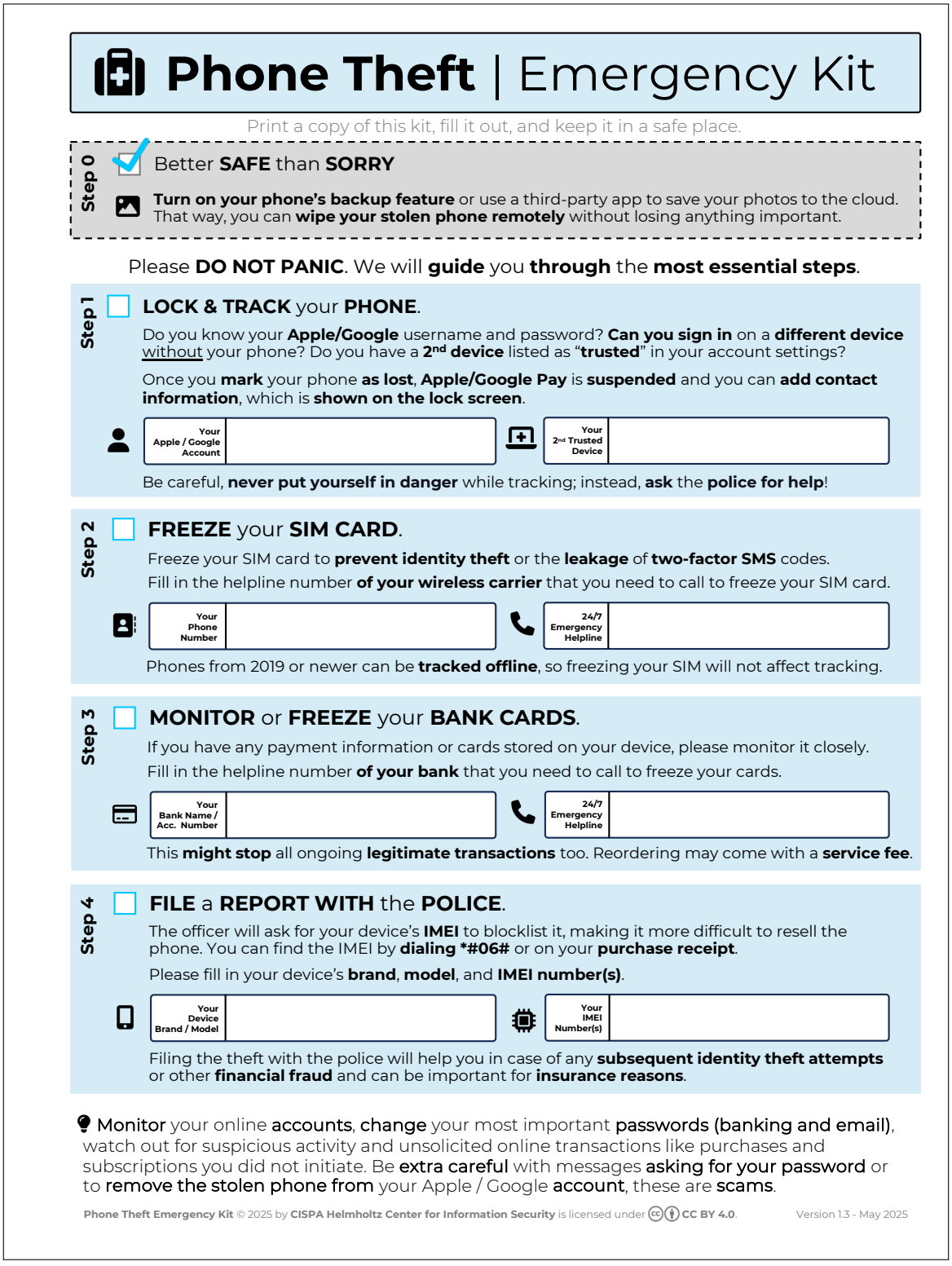
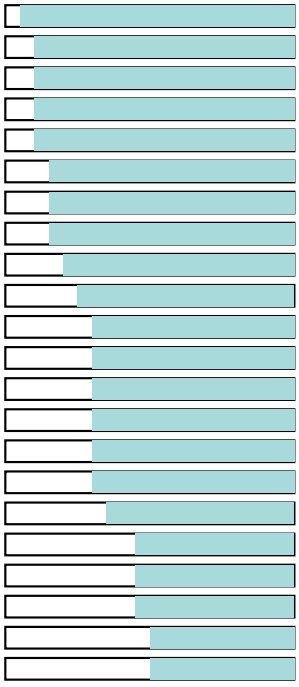
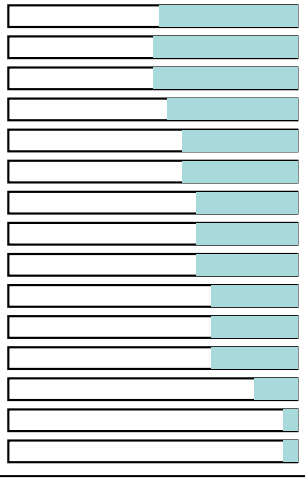


Figure 6: Emergency kit distributed to participants after interviews.

E Interviewees' Smartphone Usage

Table 5: To better understand our interviewees' smartphone usage, we describe the apps and features they reported having installed or using on their smartphone.

	Popularity Among Interviewees	Category	Examples
Installed/used on more than 50% of phones.		Browser	Chrome, Safari, Firefox
		Cloud Storage and Documents	Dropbox, Google Drive, OneDrive, NextCloud
		Messengers	WhatsApp, WeChat, Telegram, Facebook Messenger
		Music	Spotify, YouTube Music, Apple Music
		Social Media	Facebook, Instagram, Linkedin, X, Threads, TikTok, SnapChat
		Personal Productivity	Email, Calendar, Contacts, Documents
		Entertainment	Netflix, Amazon Prime, Disney+, YouTube
		Photos and Videos	Photos stored on your phone, iCloud Photos, Google Photos
		Wallet	Credit Cards, Membership Cards, Boardingpasses and Tickets
		Navigation	Google Maps, Waze Navigation
		Business Communication	Microsoft Teams, Slack, Zoom Workplace
		Finance	PayPal, Venmo, Online Banking, Trading
		Food and Drinks	McDonald's, Uber Eats, Delivery Hero
		Weather	AccuWeather, The Weather Channel
		Business Productivity	Email, Calendar, Contacts, Documents
		Shopping	Amazon, IKEA, Temu, Wallmart, Best Buy, Wish
		Health	Period tracker, Sleep tracker, Heart monitor, Doctolib
		Education	Duolingo, Babble, Google Classroom
		Ride Sharing	Uber, Lyft, Taxi
		Security Tools	Password Manager, 2FA codes, Vault Apps
		Personal Assistance	Alexa, Siri, Google Assistant, ChatGPT
		Location Sharing	Temporarily/permanently, Find My, Within Messengers
Installed/used on less than 50% of phones.		Travel	Booking.com, American Airlines, Airbnb, Amtrak
		Utilities	Shipment Tracking, Document Scanner, Calculator
		VPN	NordVPN, Proton VPN, CyberGhost, CISCO, Wireguard, IPSEC
		Games	Subway Surfers, Monopoly Go!, Candy Crush
		Fitness and Sport	Nike Training Club, Peloton, Strava, Garmin, Yoga
		News	CNN, The New York Times, FoxNews, ABC
		Lifestyle	Pinterest, Ticketmaster, Plant Parent, Lottery
		Reference	Google Translate, Dictionary, Wikipedia
		Smart Home	Google Smart Home, Amazon Alexa, Ring
		Books	eBooks, Stories, Magazines
		Dating	Tinder, Bumble, Match.com, Hinge
		Image Editing and Design	ProCamera, Prisma, Canva, Darkroom
		Digital Keys	Tesla, Volkswagen, Nuki Smart Lock, Nest Smart Lock
		Developer Tools	GitHub, Python Editor App
		Parenting	The Wonder Weeks, Luna Baby Monitor, Google Family, Parent Child Care App

F Process Flow Diagram

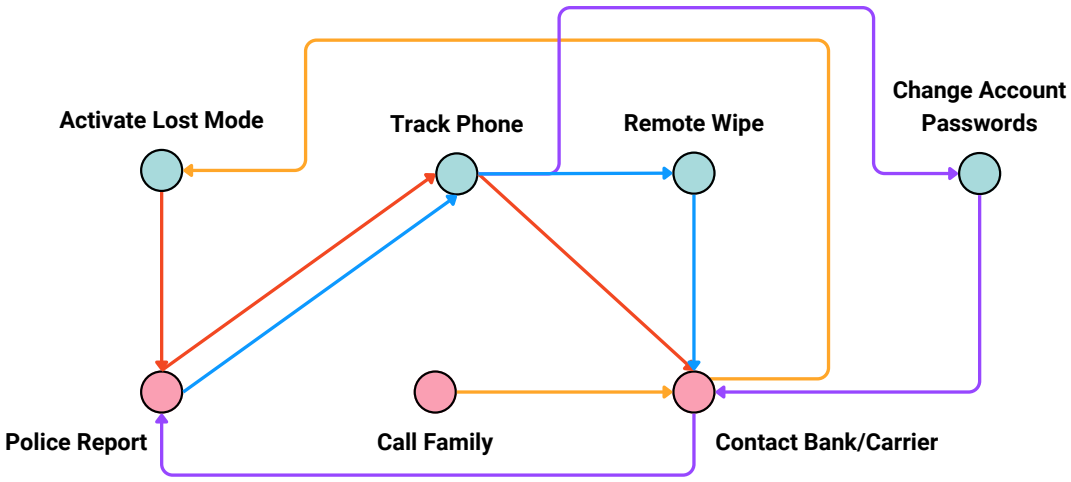


Figure 7: This figure outlines the sequence of actions in response to smartphone theft, highlighting the most common chain of technical and social actions performed. Every distinct line color represents a single chain of actions performed by participants. The *red* nodes represent non-technical actions while the *teal* nodes represent technical actions. For example, some participants start off by calling their family, then contacting their bank or wireless carrier and finally activating Lost Mode. These sequences highlight the diversity in how participants respond to theft. Some acted with technical interventions (e.g., location tracking, remote wipe), while others prioritized social steps (e.g., notifying family, filing a police report). The order and presence of actions vary depending on context, awareness, and available resources.