

# **Understanding How Users Prepare for and React to Smartphone Theft**

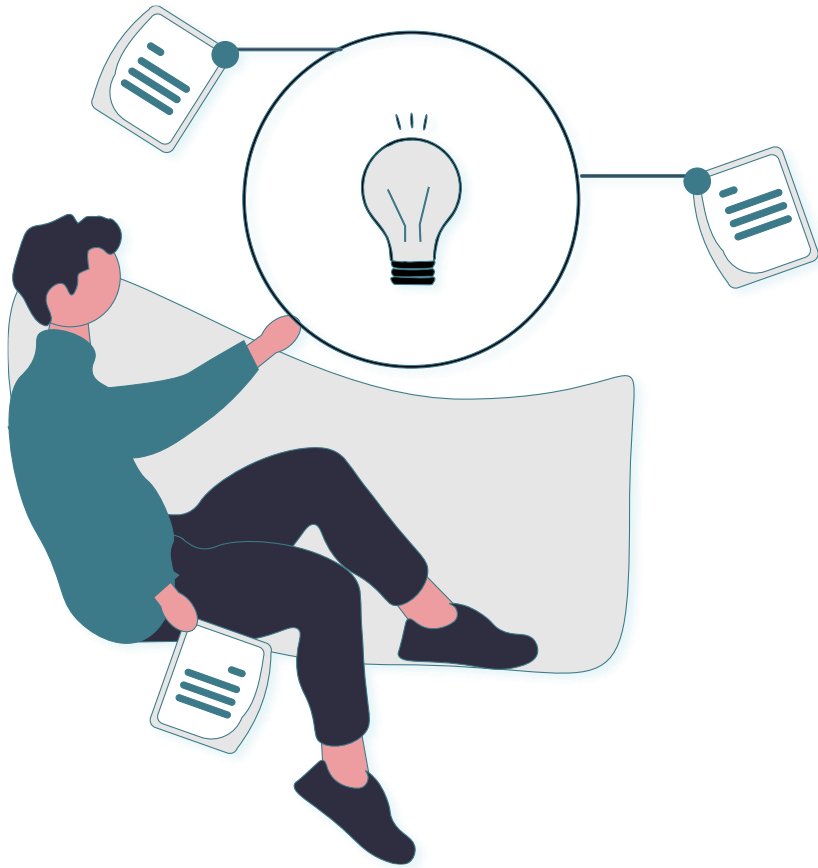
USENIX Security 2025 | Seattle, WA

Divyanshu Bhardwaj, Sumair Ijaz Hashmi, Katharina Krombholz, Maximilian Golla



# Smartphones: An Extension of Ourselves





# Motivation



**Imagine losing your  
phone in this  
situation!**

*What would you do?*



**“I had **everything** on my phone,  
my banking, my credit card, socials,  
even personal documents.**

**So when I lost it, it seemed like a  
**nightmare.”****



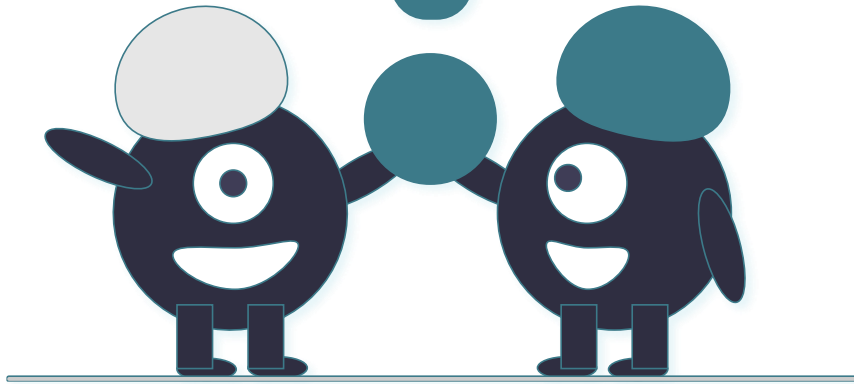
# Phone Theft Across Borders



• Common

• Traumatic

• Underexplored



# Research Questions



# Research Questions



## RQ1: Preparation

How do users **prepare** for smartphone theft?

What **risks** do they associate with theft?



## RQ2: Response

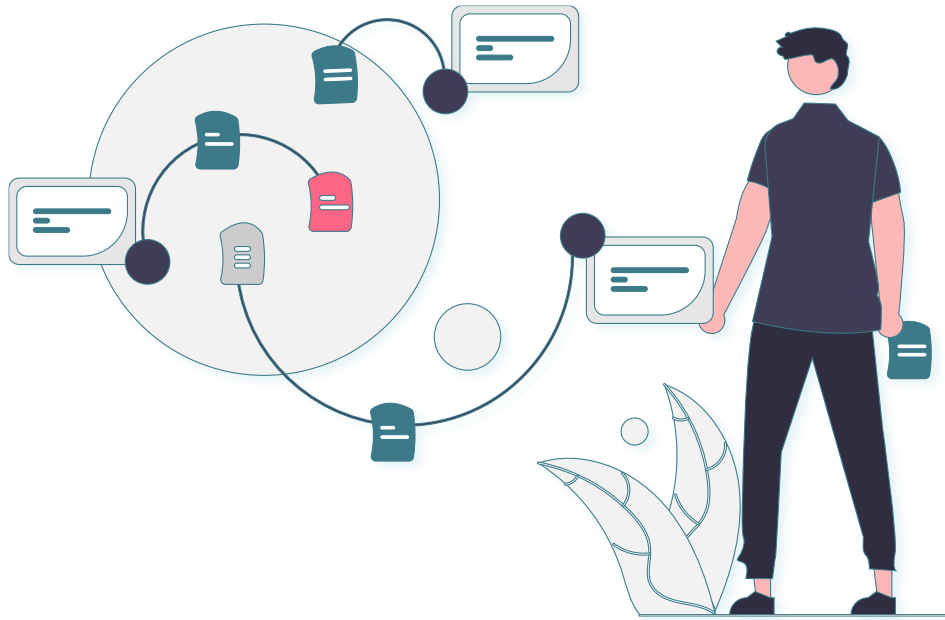
What **immediate concerns** do users have upon losing access to their device?

What is their **first response**, and where do they seek assistance?



## RQ3: Harms & Threats

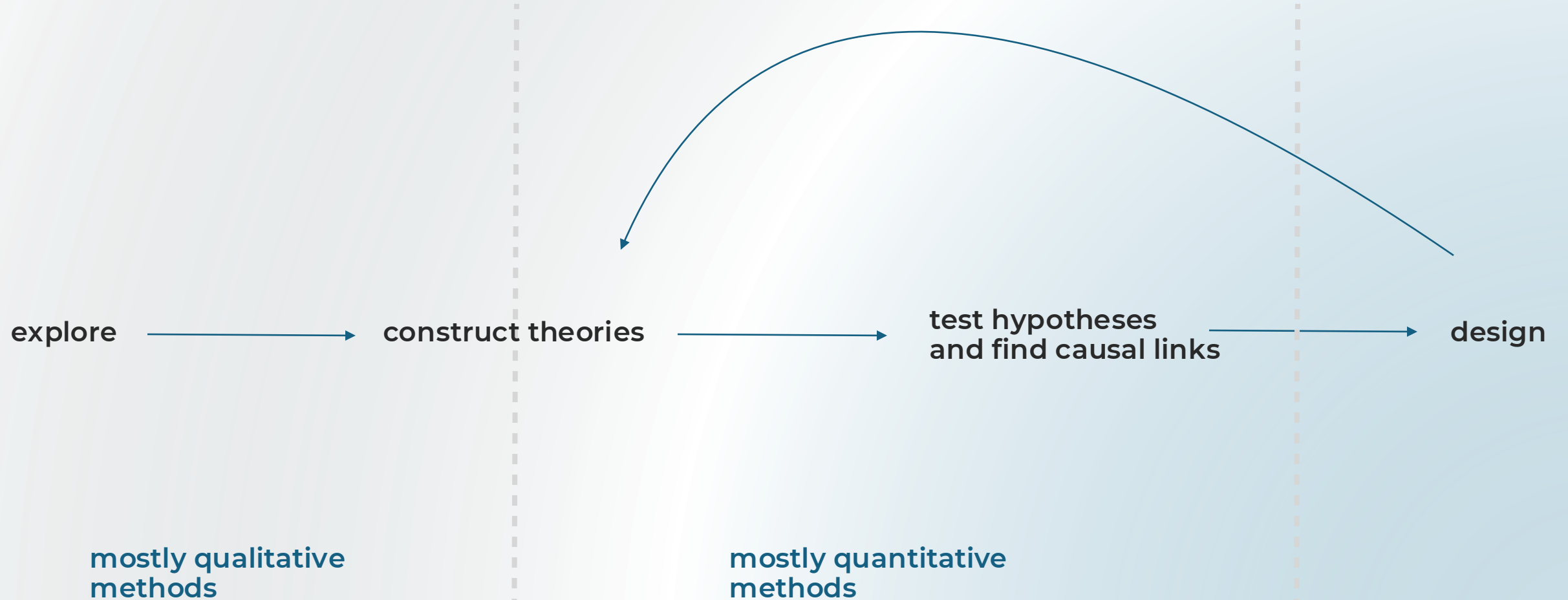
What **harms and threats** do users deal with after smartphone theft?



# Method

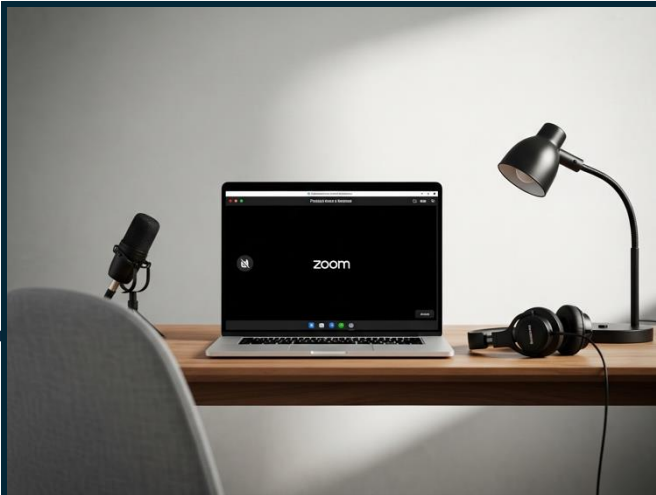


# Qualitative Approach



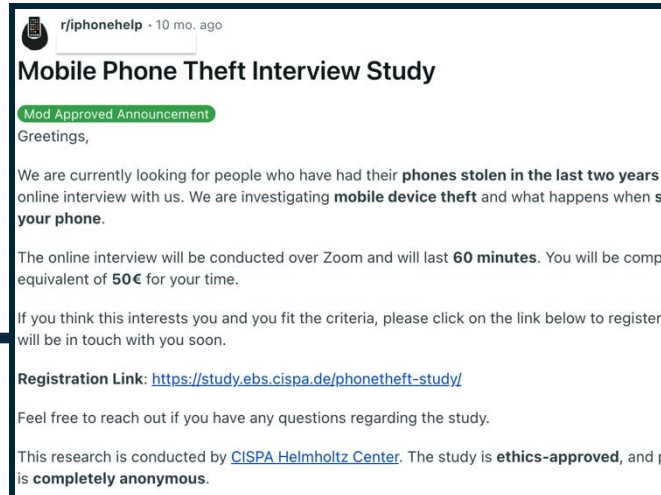


# Real Victims, Real Experiences



## Semi-Structured Interviews

- 20 Participants  
9 Countries



## Recruited over Reddit

- r/LostMyPhone,  
r/iPhoneHelp, ...



## Thematic Analysis

- Open Coding Principles



# Theft Severity

**7 participants**



**Low**

Opportunistic Thefts

**11 participants**



**Medium**

Pickpocketing

**2 participants**



**High**

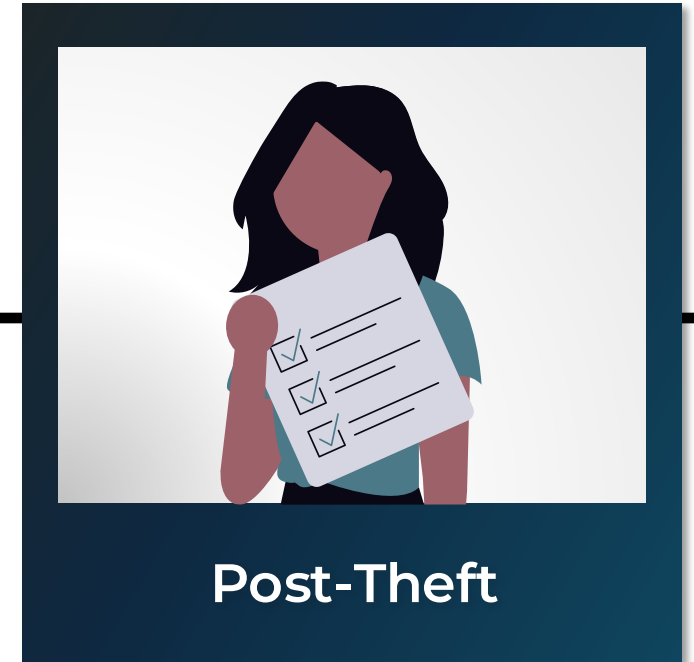
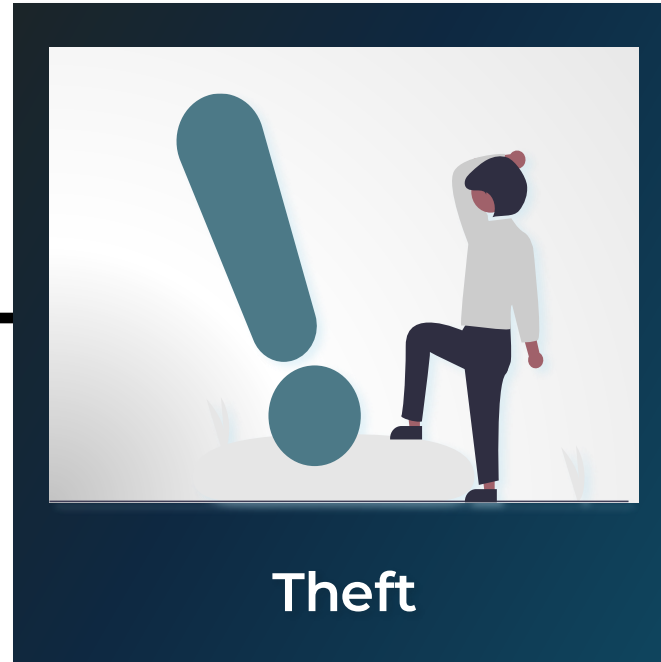
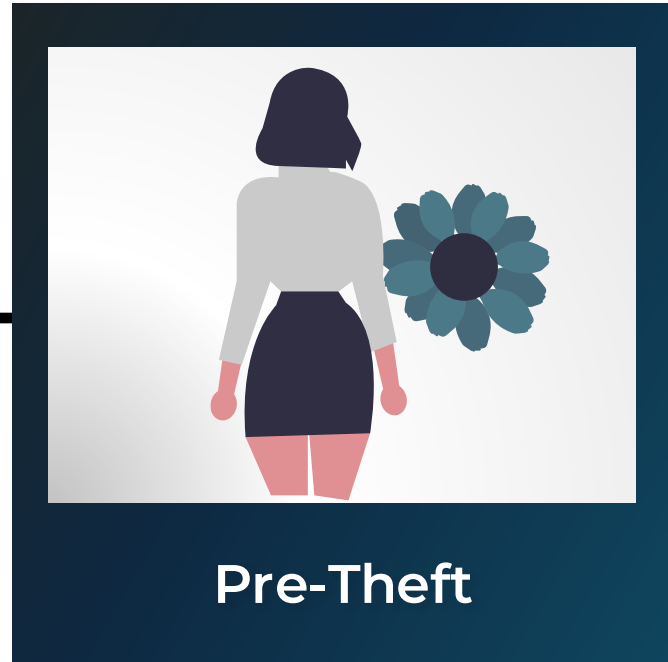
Armed Robberies



# Results



# Phone Theft Journey





# Pre-Theft Phase

## Optimism Bias

- **Low Preparedness:**  
Reliance on simple locks
- **Protection Methods:**  
Passcodes, biometrics,  
2FA for some services





# Theft Phase

1

## Emotional Chaos

Shock, Helplessness, Panic,  
Self-Blame

2

## Initial Actions

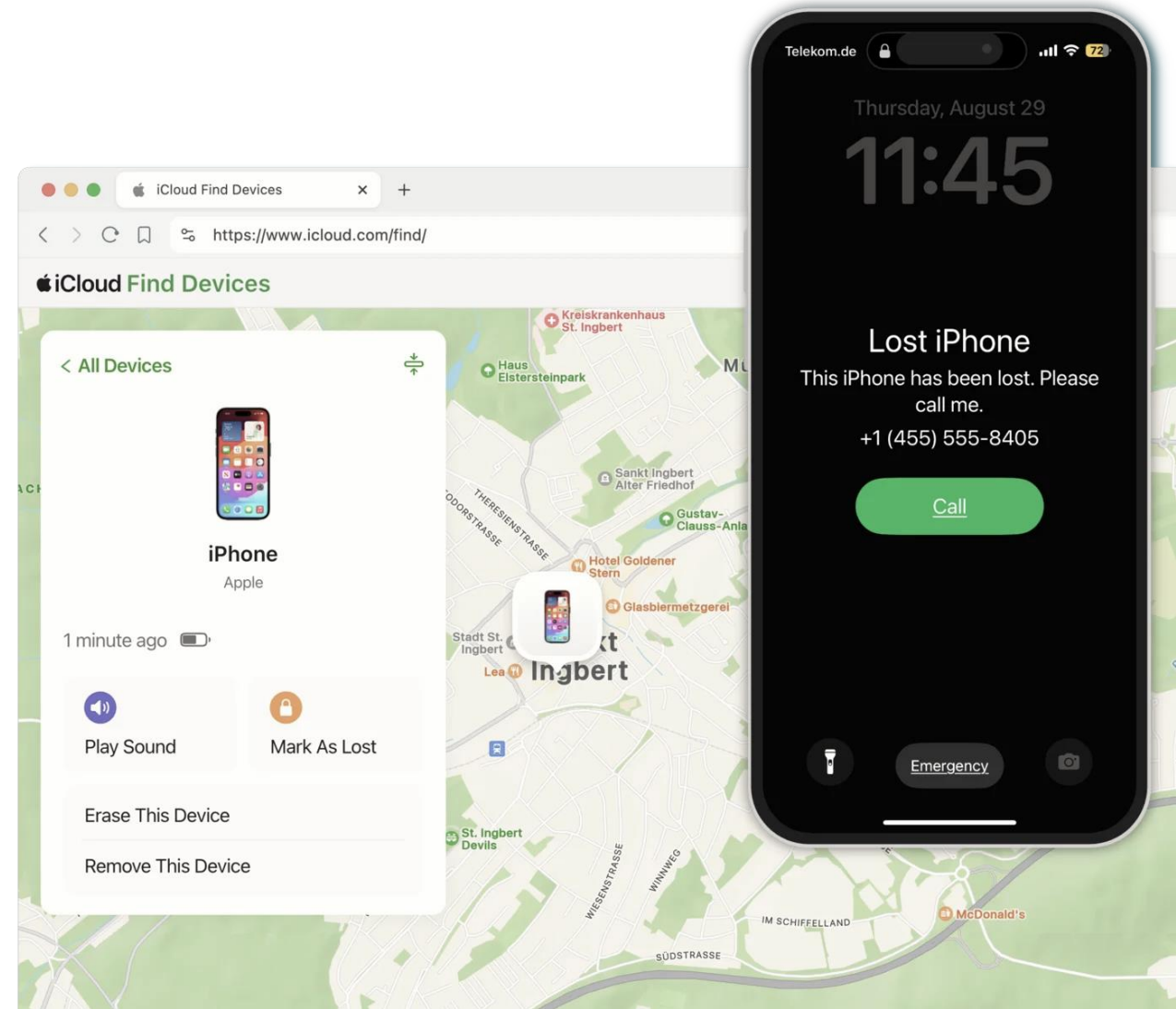
Tracking, Lost Mode,  
Blocking Cards

3

## Seeking Help

**Emotional:** Family/Friends

**Formal:** Police/Service Providers





# Post-Theft Phase

## Sophisticated Phishing



- Impersonating Apple support for credentials
- Attackers exploit distress

## Harms

- Economic, Psychological, Reputational Harms
- **Disrupted Access:** Banking, Transport, IoT, Health



# Phone Theft Journey

Pre-Theft	Theft	Post-Theft
<p><b>Unprepared:</b> People feel <i>safe</i>, <b>underestimate risk</b></p> <p><i>‘My phone will never get stolen’</i></p> <p><b>Protection:</b> Lock Screen &amp; Biometrics</p>	<p><b>Feelings:</b> Panic, Helplessness, Confusion</p> <p><b>Key concerns:</b> Photos, Financial Apps, Private Data</p> <p><b>First actions:</b> Track Phone, Lost Mode, Call Bank/Carrier</p>	<p><b>Problems:</b> 2FA, Access to Services</p> <p><b>Struggles:</b> Account Recovery, SIM Replacement</p> <p><b>Threats:</b> Phishing, Impersonation</p>



**3 out of 20** participants  
recovered their phone!





# Discussion



## The 2FA Paradox

“2FA is supposed to protect me, but it doesn’t help me and ends up making me feel vulnerable.”

## Behavioral Shifts

- Avoiding phone use in crowded spaces
- Carrying a burner phone

Technical

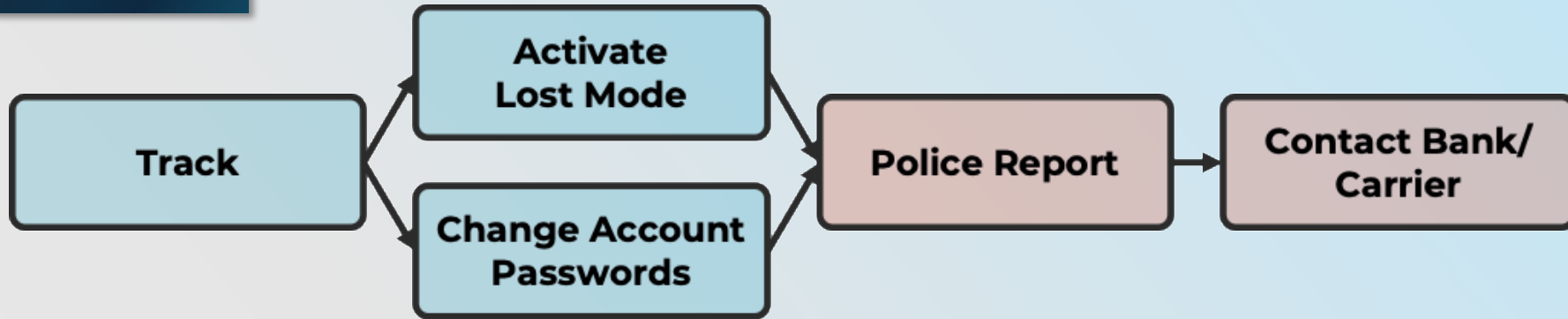


Non-Technical

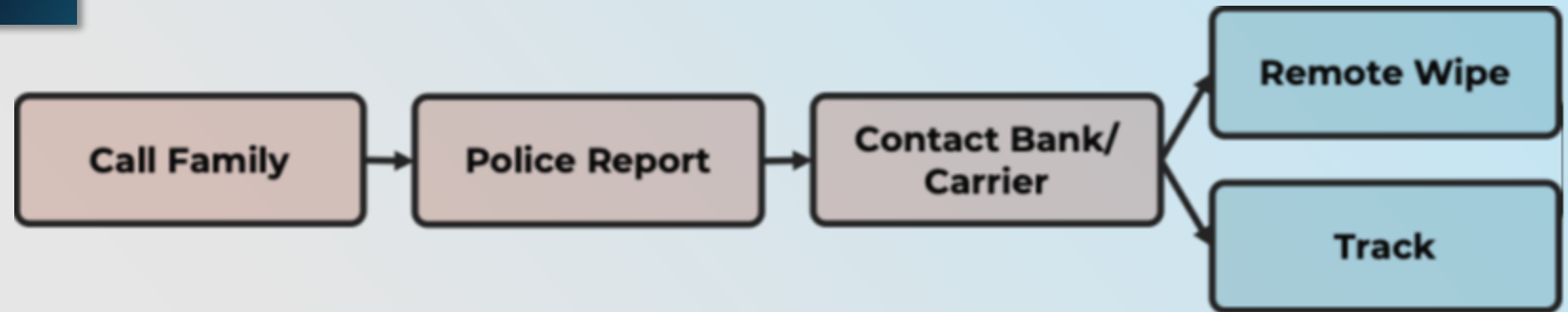


# Behavioral Patterns

## Technical

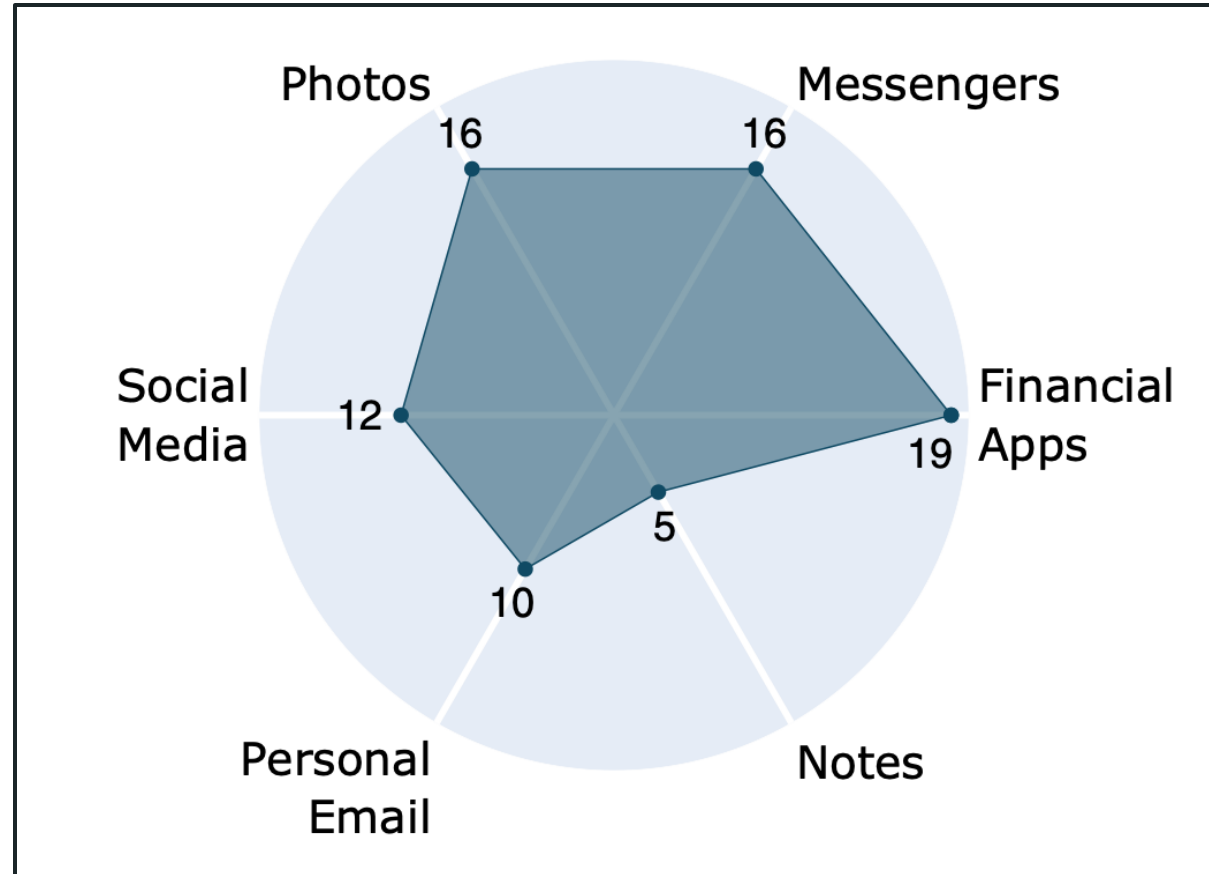


## Social





# What People Fear Most



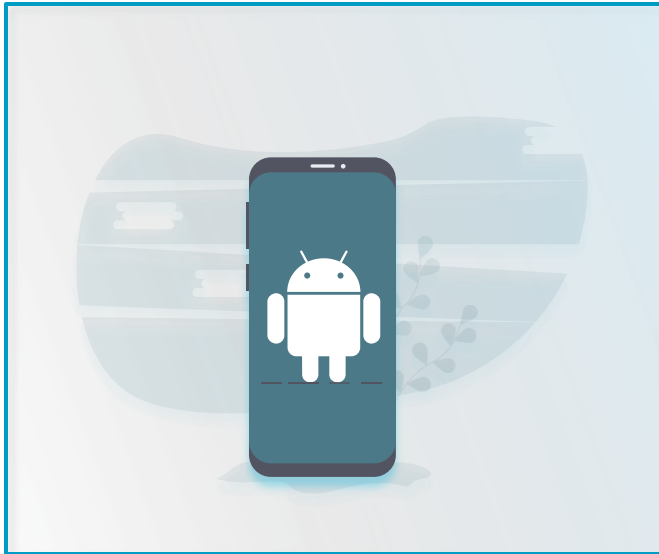
**Phone Apps to Protect from  
Unauthorized Access**



# Recommendations



# Key Stakeholders



**Phone Vendors**



**App Developers**



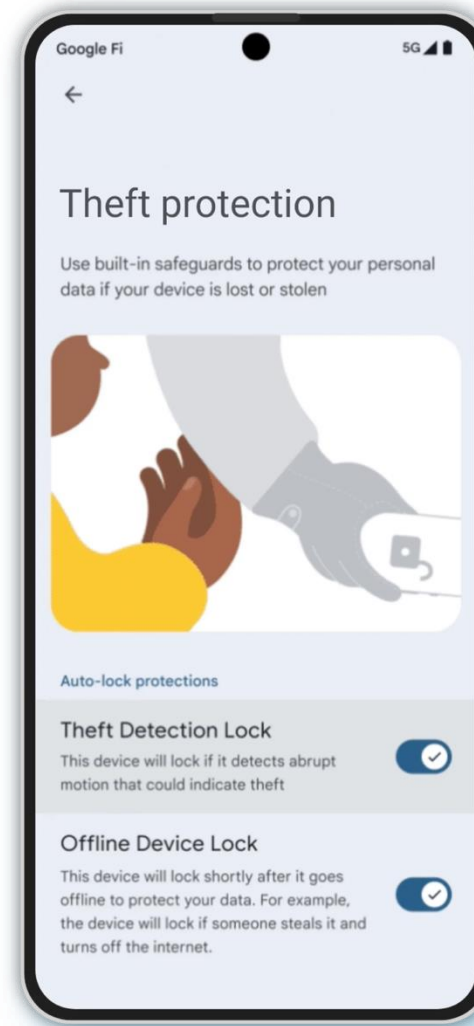
**Law Enforcement  
and Policymakers**



# What Are Vendors Doing



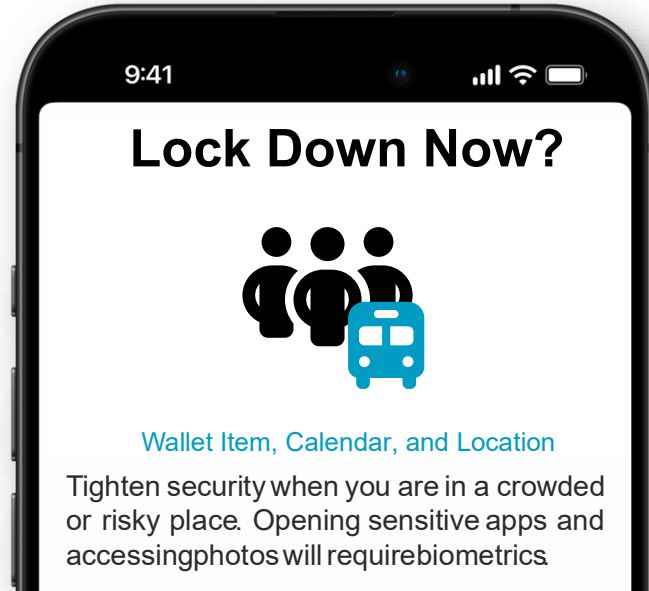
Apple



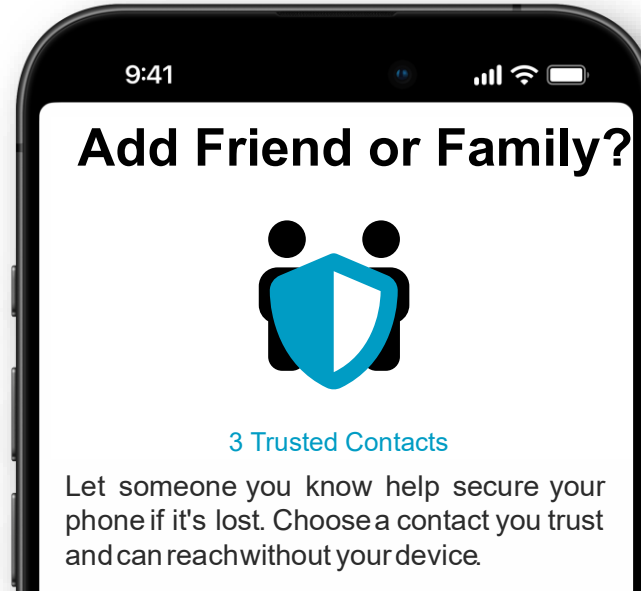
Android



# Phone Vendors



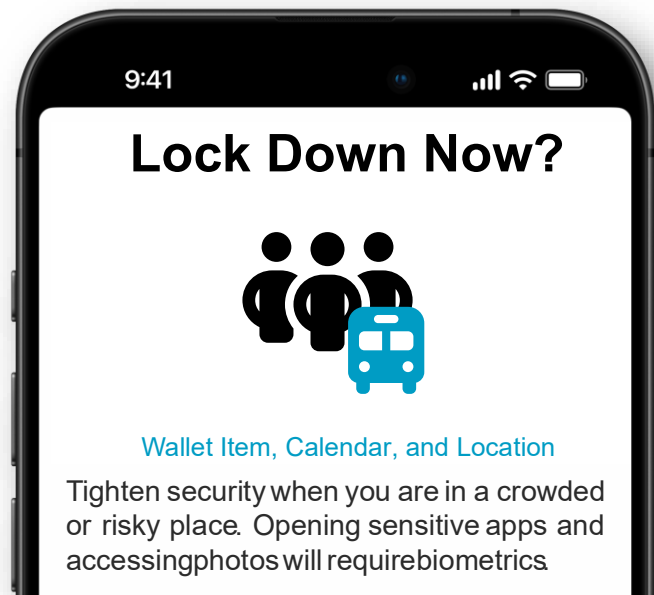
**Contextual  
Security**



**Social  
Recovery**



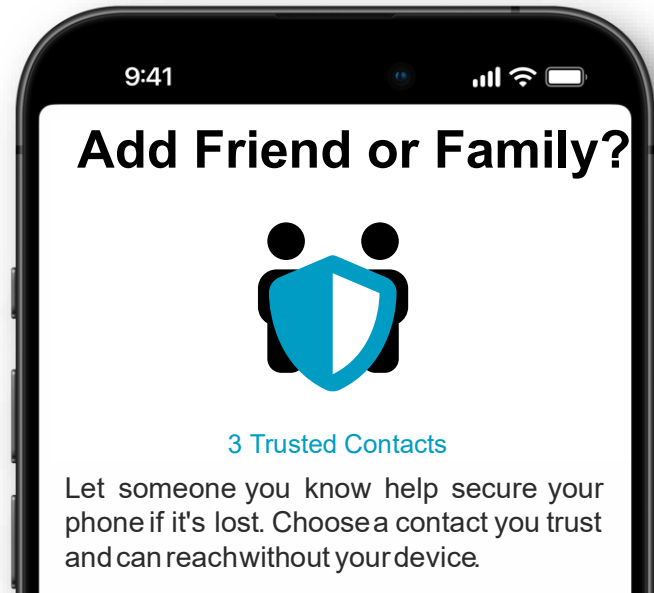
**Informed  
Reassurance**



## Contextual Security

### High Risk Mode

- Enforces biometrics for third-party apps, photos, and services
- Triggered by contextual cues such as wallet items, location, calendar



## Social Recovery

### Trusted Contacts

- Allows approved contacts to trigger Lost Mode
- Drives timely response, improves recovery odds



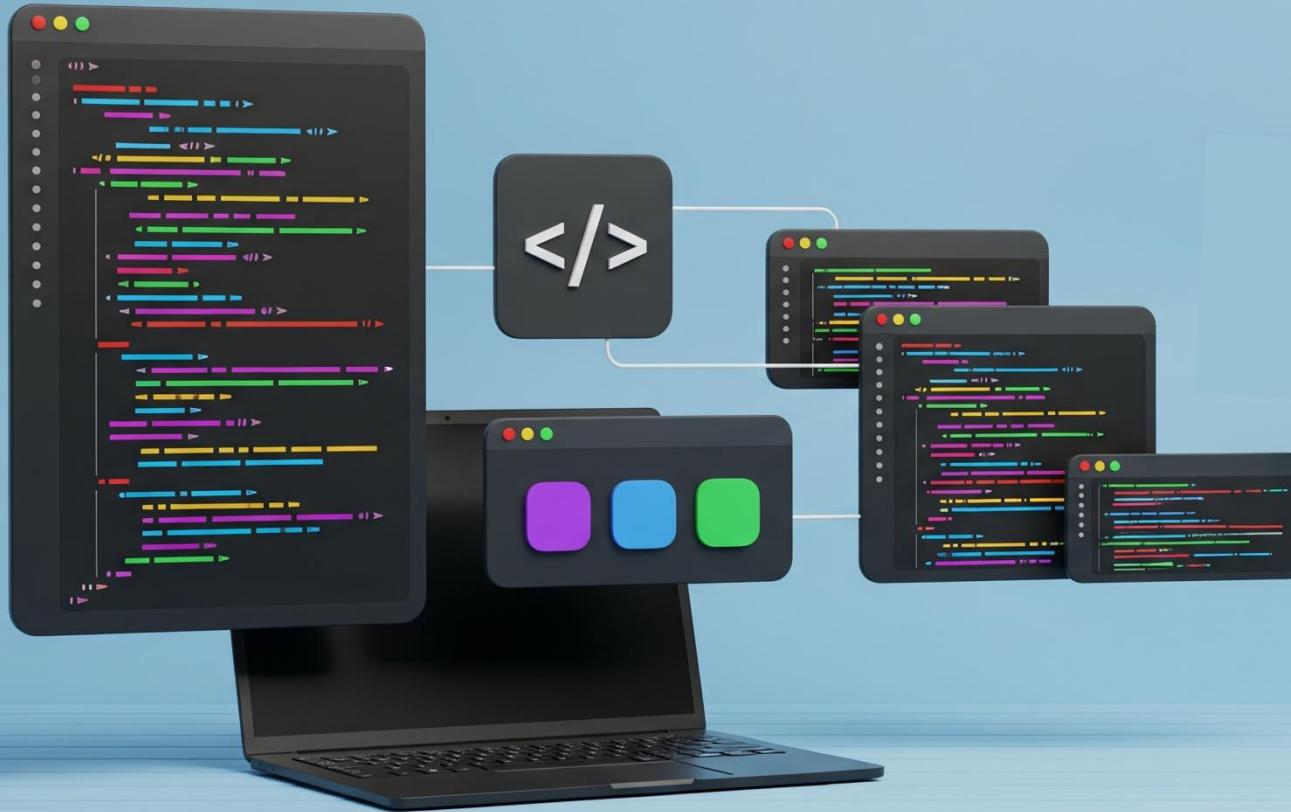
**Informed  
Reassurance**

## Backup Metadata

- Eases hesitation to trigger remote locking or remote wiping.
- Reduces panic, promotes secure behavior.



# App Developers



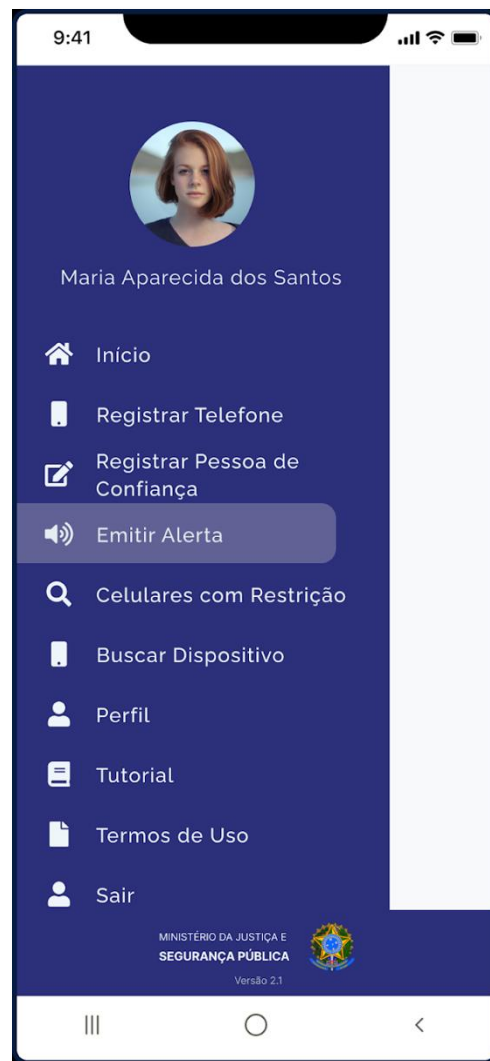
PIN Reuse  
Warnings

Emergency Account  
Remediations

Alternative Recovery  
Options



# Law Enforcement and Policymakers



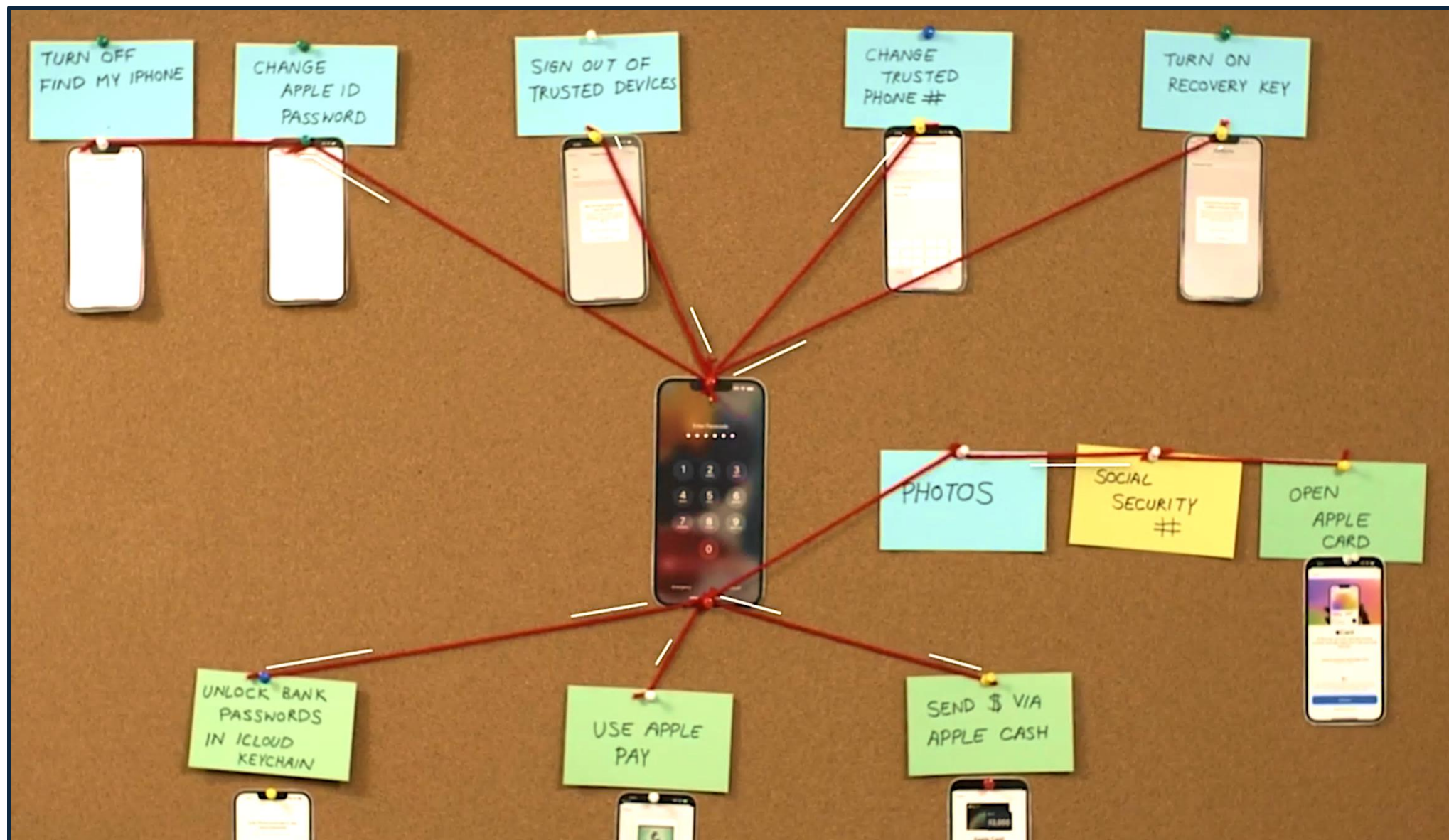
Centralized  
Reporting

Tailored  
Guidance

Stakeholder  
Collaboration



# An Evolving Threat Model





# Takeaway and Outlook

## Why Users Struggle

**Optimism Bias:**  
“It’ll never happen to me.”

**Existing Protections:**  
Scattered and complex

## Gaps in Support

**Recovery Path:**  
Unclear and unguided

**Obstacles:**  
2FA and receiving SMS

## Recommendation

**Key Stakeholders:**  
Phone vendors, service providers, app developers, policymakers



**Divyanshu Bhardwaj**



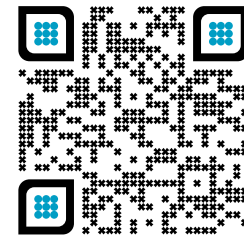
**Sumair Ijaz Hashmi**



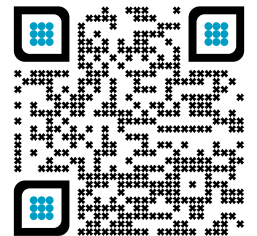
**Katharina Krombholz**



**Maximilian Golla**



**TL;DR Podcast**



**Emergency Kit**