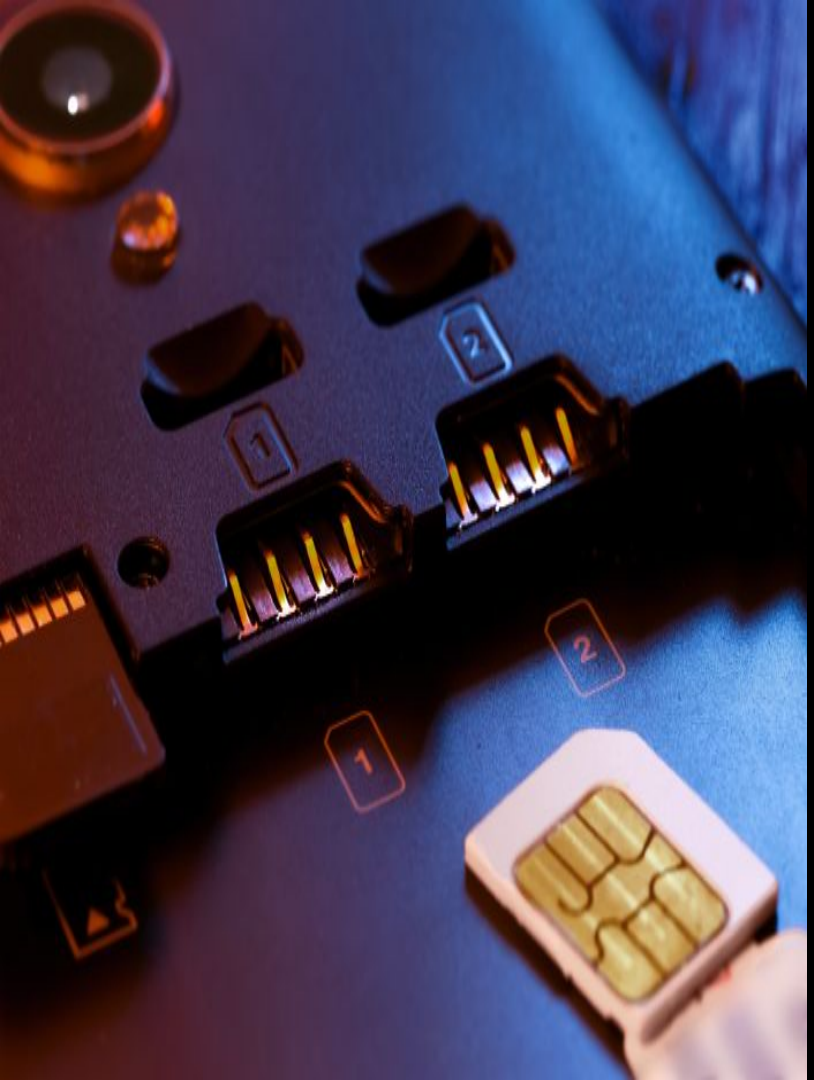


Mind the SIM: Awareness and Mental Models in a South Korean Case Study

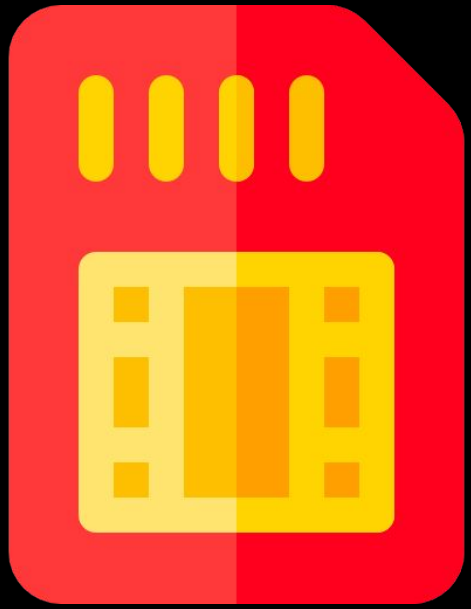
Hyunsoo Lee, Seyoung Jin
Hyoungshick Kim, Uichin Lee

Background: The SIM may be a tiny chip, but it is a critical security backbone

SIM (Subscriber Identity Module)

1. Identity
   - Identifies you on the network
   - Links phone number to device
2. Authentication
   - Stores secure credentials
   - Enables OTP verification
3. Connectivity
   - Connects to mobile network
   - Enables communication

SIM CARD CONNECTS:



IDENTITY

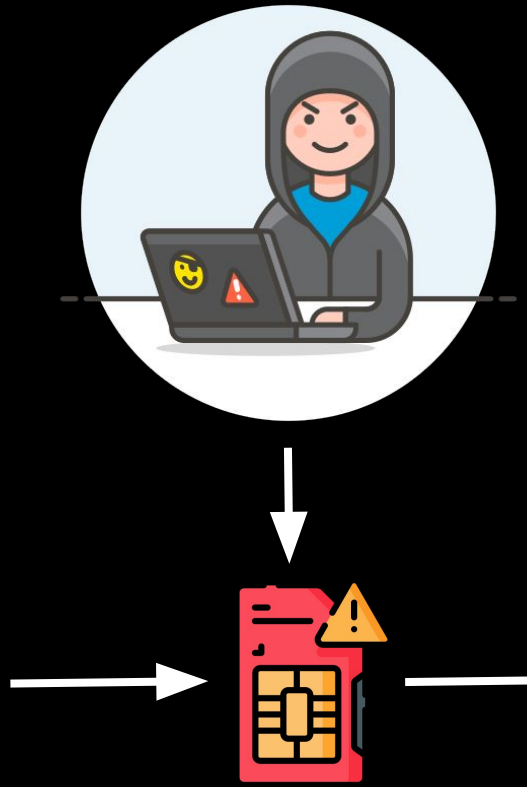
DEVICE

SERVICES (Bank, Apps)

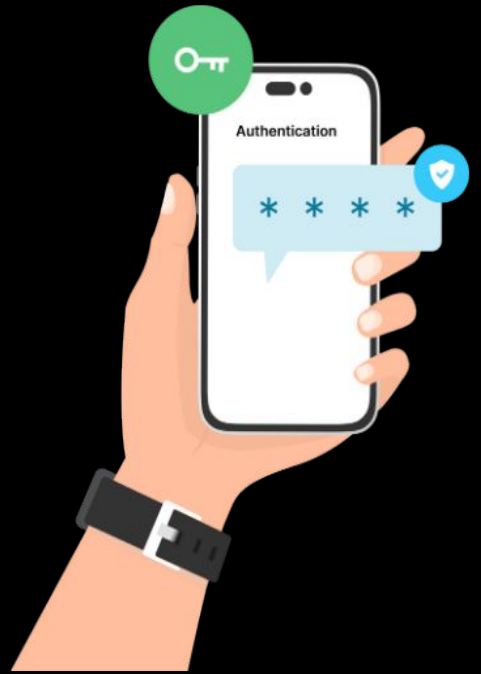
Background: What happens when the SIM is compromised?

SIM Swapping

NO SERVICE



MOBILE CARRIER



Motivation: SKT SIM Data Breach (2025)

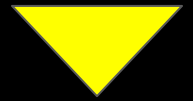
SK Telecom users' USIM data leaked in cyberattack

- South Korea’s largest telecom provider, SK Telecom (SKT), was breached
- Exposure of SIM authentication data affecting ~23 million users (~50% of the population)
- Leaked data included SIM identifiers (IMSI) and authentication keys (Ki)
- Carrier response: SIM replacement and additional security measures

BUT HOW DO USERS ACTUALLY MAKE SENSE OF THIS?

Large-scale breach

Critical security risk



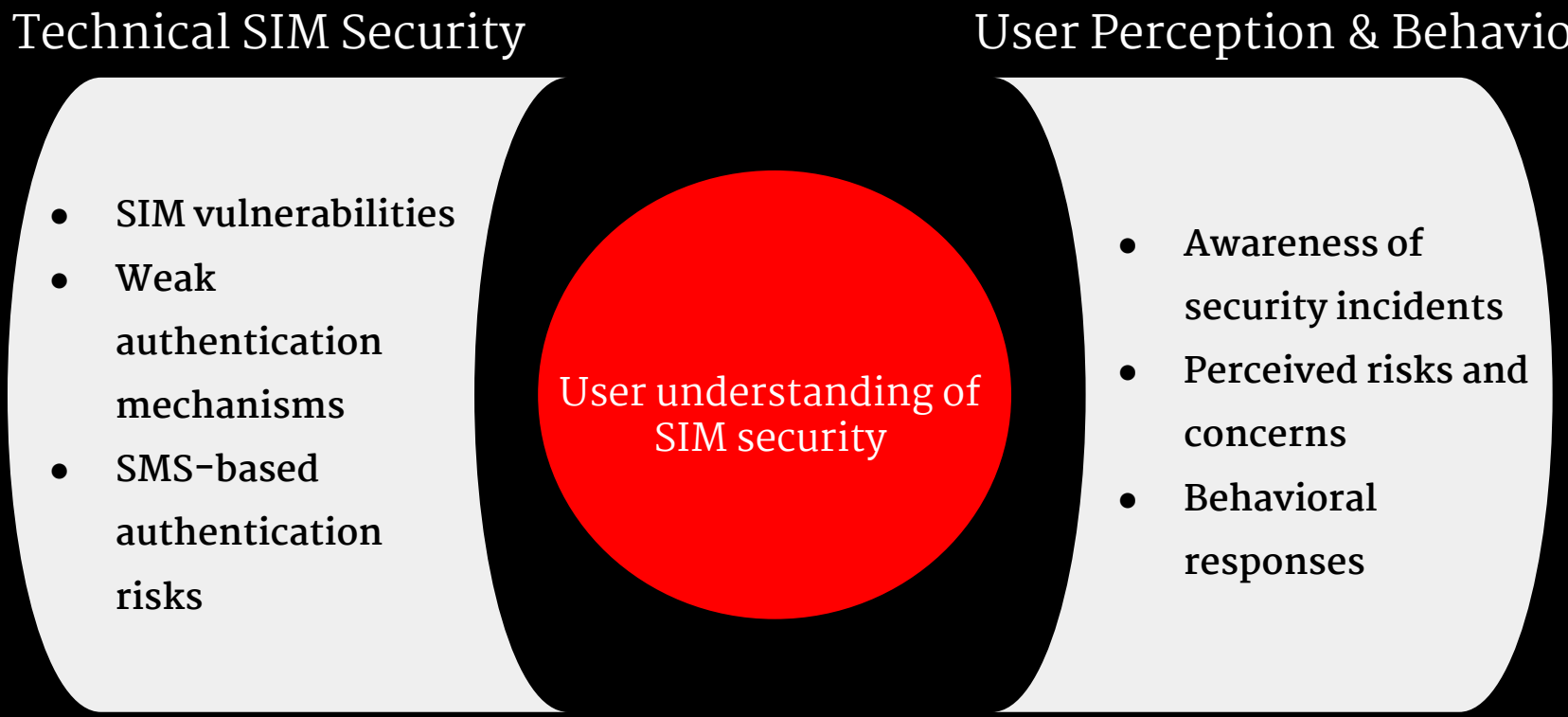
Do users understand what was exposed?

Do they realize the risks?

Do they take action?

A highly visible breach, rooted in an invisible infrastructure

Motivation: The missing piece – User Mental Model



SIM operates as a “black box” for users

Research Questions

Understand how users perceive, interpret, and respond to SIM security incidents

RQ1: **[Awareness]** How do users perceive the SKT SIM authentication key breach and understand the associated risks and impacts?

RQ2: **[Response]** How do users respond emotionally and behaviorally to the SIM security incident, and how do these responses differ between directly affected and unaffected individuals?

RQ3: **[Mental Model]** How do users conceptualize the operation of SIM cards and SIM-based authentication in everyday smartphone use?

Research Overview

Participants

- N = 33
- SKT / non-SKT
- Age: 20s–60s

Method

- Semi-structured interviews
- Drawing task
- Post-session reflection

Analysis

- Thematic analysis
- Mental models: Low / Mid / High

Participant Details

- **N = 33 participants**
- **Carriers**: SKT (17), non-SKT (16)
- **Age**: 20s–60+
- **SIM replacement (SKT users)**: 9 / 17

Demographics

- Gender-balanced
- Diverse education levels

Technology background

- Mostly non-CS
- Few with IT/security experience

Devices & SIM

- Android & iOS mix
- Physical SIM + eSIM

Research Questions

Understand how users perceive, interpret, and respond to SIM security incidents

RQ1: **[Awareness]** How do users perceive the SKT SIM authentication key breach and understand the associated risks and impacts?

RQ2: **[Response]** How do users respond emotionally and behaviorally to the SIM security incident, and how do these responses differ between directly affected and unaffected individuals?

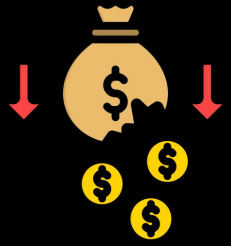
RQ3: **[Mental Model]** How do users conceptualize the operation of SIM cards and SIM-based authentication in everyday smartphone use?

Results (RQ1-1): Users lack understanding, but perceive risks

Understanding	Risk Perception
• “SIM ”= just a hack • Unaware of SIM functions • Could not explain what was exposed	• Financial loss • Identity theft • Personal / work / family risks

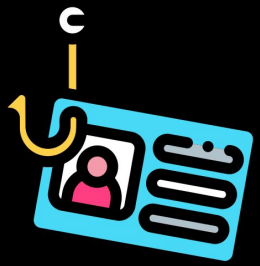
Risks are interpreted through familiar frames, not SIM understanding

Results (RQ1-1): Users lack understanding, but perceive risks



"*If whatever the thing called SIM gets hacked, somebody's going to take my money away.*" - P9 (SKT)

"*Smartphones are basically your identity card across apps… If that gets stolen? I don't even want to think about it.*" - P13 (non-SKT)



"*What if my hacked phone reaches out to my kids?*" - P22 (non-SKT)

Results (RQ1-2): Perceived risk does not lead to high concerns

Helplessness

Low data value

Safety Insensitivity

Trust

Limited Understanding

Research Questions

Understand how users perceive, interpret, and respond to SIM security incidents

RQ1: **[Awareness]** How do users perceive the SKT SIM authentication key breach and understand the associated risks and impacts?

RQ2: **[Response]** How do users respond emotionally and behaviorally to the SIM security incident, and how do these responses differ between directly affected and unaffected individuals?

RQ3: **[Mental Model]** How do users conceptualize the operation of SIM cards and SIM-based authentication in everyday smartphone use?

Results (RQ2-1): Trust varies, but personal relevance remains low

Low Trust

"*I don't know if just changing the SIM is really a solution. This wasn't some outside attack. It was a backdoor inside the system.*" - P12 (SKT)

"*This didn't happen because something was wrong with my SIM. It happened because the company failed to manage SIMs properly.*" - P16 (non-SKT)

High Trust

"*I trust them a lot. They're a big company. They give more data and discounts because of the accident.*" - P21 (SKT)

"*I'd feel safer with the physical SIM replacement. At least I can see it being done.*" - P27 (non-SKT)

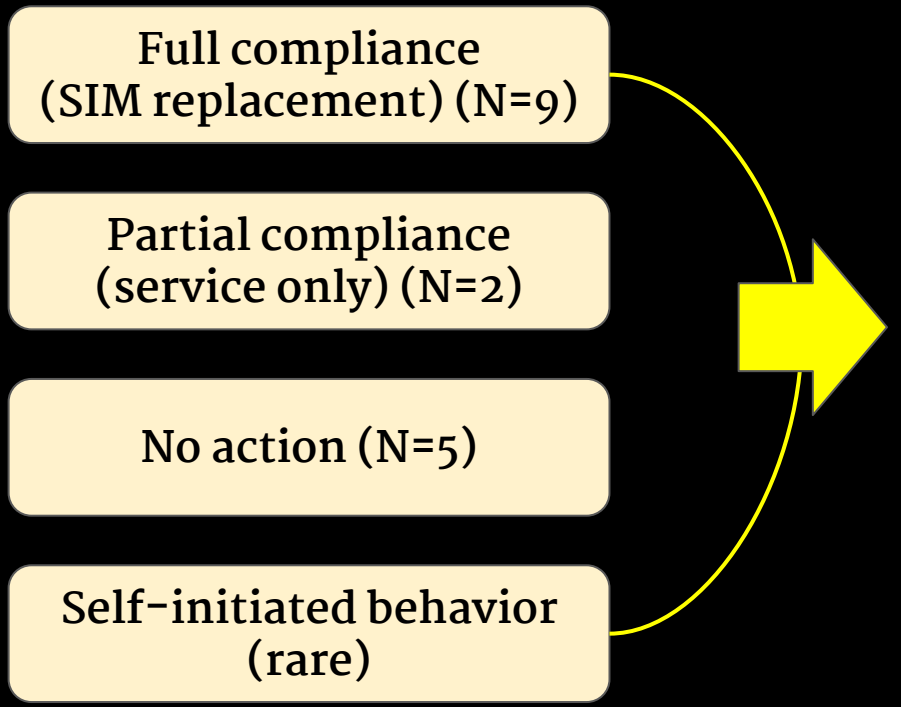
Results (RQ2-1): Trust varies, but personal relevance remains low

Affected users (SKT)	Non-affected users (non-SKT)
• Detached response • "Not me" perspective • Incident normalized	• Mixed attachment & detachment • Often redirected to others (e.g., family)

"*When I first received the message that my data was breached, I thought, 'Oh, okay.' It happens all the time to everyone, and I'm not the one hackers would target.*" - P2 (SKT)

"*I use LG U+, so at first I didn't pay much attention to the news. But my mom uses SKT, so I felt like I had to do something.*"
- P10 (non-SKT)

Results (RQ2-2): Users take action, but rarely take initiative



- Driven by cost, effort, convenience
- Fatigue / indifference
- Lack of visible threat
- Follow carrier guidance

Research Questions

Understand how users perceive, interpret, and respond to SIM security incidents

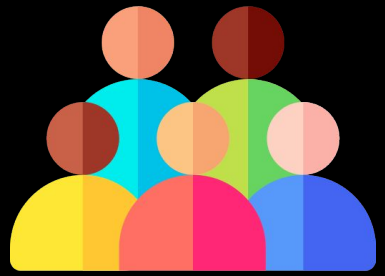
RQ1: **[Awareness]** How do users perceive the SKT SIM authentication key breach and understand the associated risks and impacts?

RQ2: **[Response]** How do users respond emotionally and behaviorally to the SIM security incident, and how do these responses differ between directly affected and unaffected individuals?

RQ3: **[Mental Model]** How do users conceptualize the operation of SIM cards and SIM-based authentication in everyday smartphone use?

Results (RQ3-1): People know SIM matters, but don't understand it

"It's necessary to activate a mobile phone. I don't really know what information it contains, but I assume it must include some personal information, since it's required for phone activation." – P19 (non-SKT)



Moderate understanding (N = 17) Low comprehension (N = 9) Accurate model (N = 7)

Results (RQ3-2): Diverse mental models of SIMs in practice

Call process

High-Level Understanding (N = 6)

"The signal is delivered to the telecom operator via SIM, then passed through the base station and finally to the recipient's phone." - P1 (SKT)

Mid-Level Understanding (N = 18)

"I don't think any other information is transmitted. Probably just the voice signal." - P10 (non-SKT)

Low-Level Understanding (N = 9)

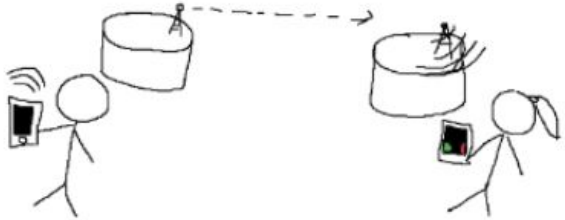
"The SIM in my ear absorbs the signals and delivers them to the brain. That way we communicate." - P21 (SKT)

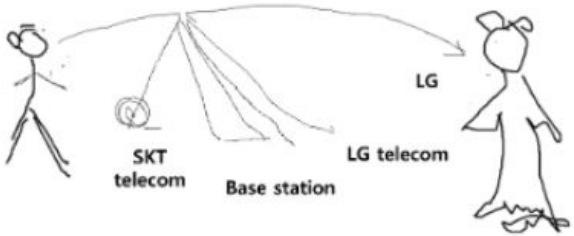
Results (RQ3-2): Diverse mental models of SIMs in practice

Call process

High-Level Understanding (N = 6)

"The signal is delivered to the telecom operator via SIM, then passed through the





(a) High level (P1) (b) Medium level (P10) (c) Low level (P21)

Low-Level Understanding (N = 9)

"The SIM in my ear absorbs the signals and delivers them to the brain. That way we communicate." - P21 (SKT)

Results (RQ3-2): Diverse mental models of SIMs in practice

🔐 Authentication

High-Level Understanding (N = 6)

"I submit my info to the bank, and then they rely on the mobile carrier to send me a one-time code through SMS. That code isn't generated by the bank itself but delivered via my SIM, so when I enter it back, the bank can verify both my identity and that I have access to my registered phone." - P29 (non-SKT)

Mid-Level Understanding (N = 16)

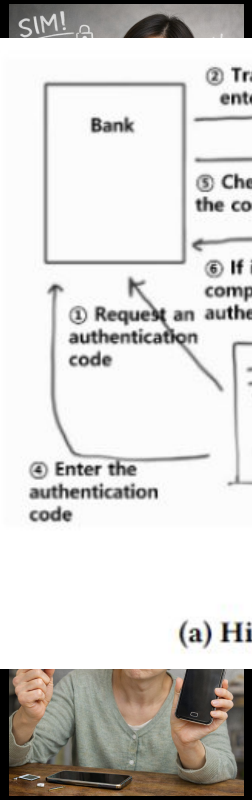
"I think there's a department at a bank fully dedicated to authentication. . . they issue and verify the code." - P2 (SKT)

Low-Level Understanding (N = 11)

"This is authentication done on the site, so it is possible without a SIM" - P26 (non-SKT)

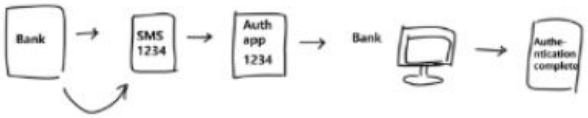
Results (RQ3-2): Diverse mental models of SIMs in practice

🔐 Authentication



High-Level Understanding (N = 6)

(a) High level (P29)



(b) Medium level (P2)

(c) Low level (P26)

"*This is authentication done on the site, so it is possible without a SIM*" - P26 (non-SKT)

Results (RQ3-3): Understanding SIM security without behavioral change

Upon seeing instruction video on SIM functionality…

Learning (Understanding)

What changed?

- 20 / 33 learned new information
- Misconceptions corrected
- Risk perceived as more serious

Action (Behavior)

What didn't change?

- 8 / 20 → no intention to act
- Limited behavior change overall
- Responsibility shifted to carriers

Learning ↑ ≠ Action ↑

Discussion: Phone Number as Digital Identity, but Limited Protection Awareness

Finding

- Phone number = **digital identity** (banking, authentication)
- Users aware of **financial / identity risks**

BUT

- “SIM = just hacked”
- **Shallow understanding**
- **Low personal action**

Low personal relevance, Reliance on carriers, Limited action

Discussion: Connect identity use to concrete security risks

Implication

#1. Focus on specific knowledge gaps and real-world relevance for education

#2. Use everyday scenarios (banking, messaging, OTP)

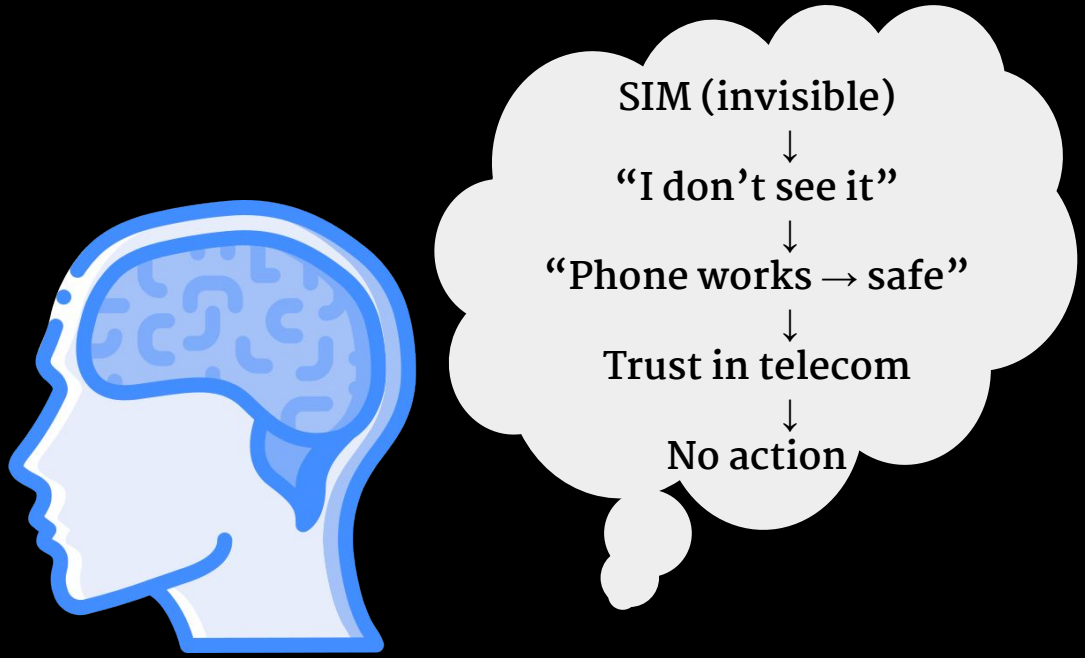
#3. Reflective framing + just-in-time nudges

#4. Cultural and social context adaptation

Explain SIM in ways that connect directly to everyday risks

Discussion: SIM as invisible infrastructure, default trust

Finding



Invisible systems lead to passive trust, not active protection

Discussion: Perceptible security touchpoints

Implication

#1. Make security perceptible at key interaction moments, not continuously

#2. Support functional understanding, not technical transparency

#3. Surface invisible authentication events to recalibrate user expectations

Make invisible authentication processes perceptible at the moment they happen

Mind the SIM: Key Takeaways

- **Awareness ≠ Action**

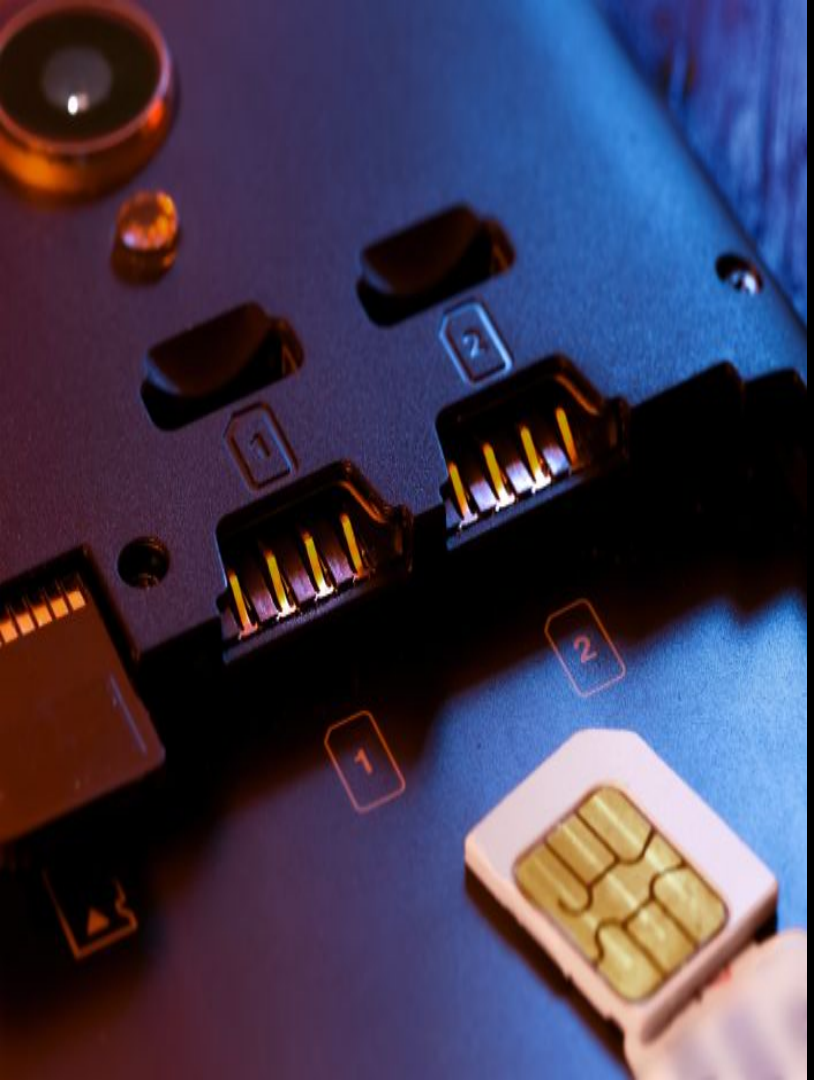
  → Users recognize risk, but rarely act
- **Shallow mental models**

  → SIM = “black box”, misunderstood or invisible
- **Perceived low personal relevance**

  → “Not me”, reliance on carriers
- **Invisible security → passive behavior**

  → “Phone works = safe” illusion

Make invisible security perceptible at the right moments



CHI'26

Mind the SIM: Awareness and Mental Models in a South Korean Case Study

Paper

Hyunsoo Lee

hslee90@kaist.ac.kr
hslee90@github.io

KAIST
SUNG KYUN KWAN UNIVERSITY