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

Hyunsoo Lee
School of Computing
KAIST
Daejeon, Republic of Korea
hslee90@kaist.ac.kr

Seyoung Jin
Department of Electrical and Computer Engineering
Sungkyunkwan University
Suwon, Republic of Korea
22sysy@g.skku.edu

Hyoungshick Kim
Department of Computer Science and Engineering
Sungkyunkwan University
Seoul, Republic of Korea
hyoung@skku.edu

Uichin Lee
School of Computing
KAIST
Daejeon, Republic of Korea
uclee@kaist.edu

Abstract

Mobile phone numbers function as single keys to banking, government, and commerce, making the Subscriber Identity Module (SIM) a critical element of security. In April 2025, South Korea's largest carrier experienced a SIM breach that compromised authentication keys and exposed nearly 27 million subscriber identifiers. We conducted semi-structured interviews with mental-model elicitation ($N = 33$) to examine user awareness, responses, and understanding of SIM-based authentication. Results reveal a pronounced awareness–action gap: participants recognized the breach yet held incomplete mental models, perceived little personal risk, and rarely acted protectively, even when affected. Learned helplessness, reliance on carriers, and the invisibility of SIM shaped these passive responses. Brief educational interventions improved conceptual understanding but seldom produced lasting behavioral change. Our findings demonstrate how technical opacity and psychological factors jointly inhibit protective action and offer design implications for usable security, emphasizing interventions that realign users' mental models with system risks to foster sustainable practices.

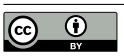
CCS Concepts

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

Keywords

SIM Security, Mobile Authentication, Usable Security

ACM Reference Format:
Hyunsoo Lee, Seyoung Jin, Hyoungshick Kim, and Uichin Lee. 2026. Mind the SIM: Awareness and Mental Models in a South Korean Case Study. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3772318.3791714



CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3791714

1 Introduction

The Subscriber Identity Module (SIM) card is a critical component of mobile communication and a key element of the security infrastructure that safeguards personal data. SIM attacks, such as SIM swapping, illustrate how weaknesses in mobile authentication can be exploited, leading to financial fraud or account takeovers [7, 33]. In April 2025, a major breach occurred in South Korea when malware compromised the Home Subscriber Server (HSS) of SK Telecom (SKT), the country's largest mobile carrier, which manages user identities and authentication. The Ministry of Science and ICT reported that the breach exposed SIM authentication keys (K_i) and about 27 million International Mobile Subscriber Identity (IMSI) records [46]. SKT responded with free SIM replacements and a SIM protection service, while the government imposed fines, issued administrative orders, and required a comprehensive security overhaul. Given the breach's scale and the carrier-wide response, all SKT subscribers were effectively part of the affected population.

This incident holds particular significance in South Korea, where phone-based authentication underpins access to essential digital services such as mobile banking, government services, e-commerce platforms, and simplified authentication systems, all of which verify users through their phone numbers [29]. The country also exhibits very high smartphone adoption, with over 97% penetration and around 73% of the population using mobile banking services [57]. The severity of the breach is further compounded by the nature of SIM cards, which store unique identifiers and authentication keys that enable network access and user verification [12].

Despite the widespread media coverage and public discourse surrounding the breach, research on how users understand and respond to SIM security incidents remains limited. While existing studies have focused on technical mechanisms or statistical analyses of breach likelihood [4, 6], how users conceptualize SIM-based authentication, perceive associated risks, and adapt their behaviors in response to such incidents remain unexplored. Understanding these perspectives is vital, as user knowledge gaps can amplify technical vulnerabilities and influence public trust in digital services [39].

This large-scale incident offers a timely opportunity to address these gaps. An incident of this magnitude provides a unique lens

through which to examine how users' perceptions, trust, and security behaviors are shaped in response to real-world threats. Specifically, this study investigates how users perceive and make sense of SIM-related security incidents, how they respond, and how their mental models of SIM cards and authentication relate to personal data protection. We also explore whether these perceptions, responses, and understandings differ between SKT subscribers directly affected by the breach and those who are not. Thus, we set the following research questions (RQs):

- 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?

To address these questions, we conducted an empirical study with 33 South Korean users (20s–60s), including both SKT subscribers and non-SKT users. SKT users were part of the carrier affected by the breach, which exposed authentication keys and IMSI records for all customers, meaning that the entire subscriber base was potentially impacted, even if we could not verify whether individual accounts were specifically compromised. We combined semi-structured interviews with a mental model drawing session to explore general mobile users' perceptions of SIM-related security risks, behavioral and emotional responses in the aftermath of the incident, and their mental models of SIM and the authentication process.

At the end of drawing session, participants watched a short YouTube video outlining how a SIM card works [1]. Then, participants answered a few brief reflection questions about whether the explanation differed from what they had previously assumed or whether it influenced how they might approach mobile use. These reflections offered additional context for interpreting their earlier comments.

Our results indicate that participants had only a general awareness of the SKT SIM authentication key breach, often describing it simply as "*being hacked*." Most were unsure what information had been exposed or how the incident had occurred. While they agreed the breach sounded serious, responses were largely passive, shaped by limited technical knowledge, trust in carriers, and a sense that individual actions would have little effect. Concerns focused mainly on financial fraud or account misuse, and behavioral responses ranged from replacing SIM cards to taking no action, with many simply following carrier guidance.

Participants' mental models of SIM functions were similarly limited and varied widely. Some described SIMs in abstract or metaphorical ways, while others recognized only the physical chip without understanding its role in authentication. Because SIM operations are largely invisible in everyday use, many underestimated potential risks and felt uncertain about their own exposure.

The key contributions of our study are as follows:

- We present a real-world breach-driven case study of a nationwide SIM authentication key breach involving SKT, South Korea's largest mobile carrier.
- We show a clear awareness–action gap, demonstrating that even users directly affected by the breach exhibited limited concern and rarely undertook protective measures.
- We provide actionable design insights for usable security, emphasizing the need for clearer risk communication and for interventions that align users' mental models.

2 Background and Related Work

2.1 SIM Operation and Threats

A SIM is a microprocessor chip in a mobile phone that enables user authentication on mobile networks. To use services provided by a mobile network operator, a user must maintain a valid subscription with that operator [41]. The SIM stores the information necessary for the device to connect to the cellular network, including the subscription profile required for carrier authentication. This profile includes essential identifiers such as the IMSI, K_i, and a phone number [12]. The IMSI is a permanent subscriber identifier that the carrier uses to uniquely identify the user, while the K_i is a secret authentication key shared only between the SIM and the carrier. Together, these elements enable the SIM to serve as a core component of mobile network authentication.

SIM plays a central role in both enabling communication and user authentication (see Figure 1). When a device connects to the network, the SIM authenticates the subscriber using its stored IMSI and K_i through a challenge-response protocol [16]. After authentication, encryption keys are generated to secure subsequent voice and data traffic. Beyond network access, SIM also anchors identity for services such as SMS-based two-factor authentication [47]. In this process, an authentication server generates a one-time password (OTP) and delivers it via the mobile carrier's infrastructure to the phone number uniquely bound to the SIM. The user then enters the OTP to complete the login or transaction, with the SIM ensuring the correct mapping between device, number, and subscriber, thereby linking authentication to the physical SIM card.

However, because the SIM is central to user authentication, it is also exposed to several security risks. While it does not store direct identifiers such as a national identification number, exposure of authentication data (e.g., IMSI, K_i) can still permit communication interception, account takeover, or location tracking. Major threat models include SIM swapping, SIM cloning, and Simjacker [49, 55, 56]. In a SIM swapping attack, for example, an attacker uses social engineering or leaked subscriber information to persuade the carrier to reassign a victim's phone number to another SIM, enabling interception of OTPs or account-recovery codes. In SIM cloning, attackers duplicate a subscriber's legitimate SIM to impersonate the victim on the network. Simjacker is a vulnerability in older SIM cards that allows attackers to send hidden messages containing SIM toolkit commands that remain invisible to the user, enabling them to determine the user's location or execute remote commands. Together, these threats show that the SIM is not a passive component but a critical part of the security infrastructure, underscoring the need for stronger protections to safeguard both privacy and communication integrity.

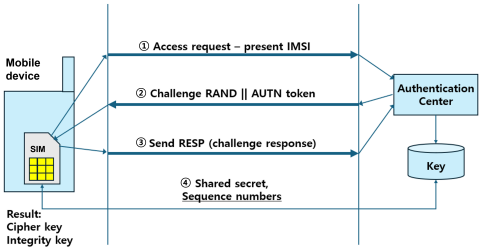


Figure 1: SIM authentication procedure. ① The mobile device sends its IMSI to the authentication center. ② The center replies with a challenge composed of a random number (RAND) and an authentication token (AUTN). ③ The device verifies the token and returns a response (RES). ④ Once verified, both sides derive cipher and integrity keys to secure subsequent communication.

2.2 SKT SIM Authentication Key Breach

In April 2025, SKT, a major South Korean mobile carrier, experienced a large-scale data breach when its HSS was compromised by malware [53]. According to a Korean government investigation [45], the leaked dataset included 25 types of SIM-related data, such as phone numbers, IMSI, and K_i, amounting to approximately 9.82 GB ($\approx$ 22.7 million records).

To mitigate risks, SKT introduced three security measures [42]. First, SIM replacement invalidated compromised identifiers such as IMSI and serial numbers, serving as the most fundamental countermeasure. Second, the SIM protection service blocked SIM usage on unregistered devices, preventing cloned SIM access but not addressing compromised keys or already registered devices. Third, the Fraud Detection System (FDS) detected and blocked abnormal authentication attempts from cloned SIMs, functioning only as a post-incident response. SIM replacement functioned as the primary solution, while the SIM protection service and FDS provided interim safeguards.

2.3 SIM Security: Technical Approaches and User Studies

Prior research on SIM cards has primarily focused on technical vulnerabilities and the identification of threats. Technical studies have analyzed weaknesses in authentication mechanisms and SMS security. For example, Anwar et al. [6] analyzed the authentication algorithms and demonstrated the feasibility of SIM cloning, while Ahmed [4] highlighted that remote provisioning in eSIM environments introduces new attack surfaces. Beyond technical feasibility, empirical work has shown how these vulnerabilities are shaped by both institutional practices and human factors. For example, Lee et al. [36] conducted an in-the-wild study of SIM swap procedures by creating prepaid accounts at five major U.S. carriers with simulated identities, revealing that customer service often relied on weak checks such as birth dates or security questions. They also analyzed 361 websites supporting SMS-based multi-factor authentication and found that in many cases SIM swap alone was enough to compromise accounts, highlighting the structural risks of SMS as an authentication channel. Blancaflor et al. [9] used penetration testing to study smishing attacks in the Philippines, showing that even with numbers registered under the SIM Registration Act, users remained vulnerable. Their work highlights how evolving social engineering techniques exploit human behaviors and knowledge gaps, emphasizing the need for education initiatives. Murugalakshmi et al. [40] provided an analysis of SIM swapping and cloning through case studies, highlighting these attacks as major threats to mobile security and proposing legal, organizational, and technical countermeasures.

2.4 Understanding Security Incidents Through User Mental Models and Behaviors

Existing research on security incidents encompasses both technical vulnerabilities and users' perceptions and responses. This body of user-centered work shows how gaps in knowledge and mental models can amplify technical vulnerabilities [39]. For example, Bhagavatula et al. [8] showed that most users ignored breach news unless incidents appeared personally relevant or severe, while a study [24] found through interviews and drawing tasks that although participants could visualize attack patterns like "backdoors" or "admin access," they lacked a systematic understanding of causes, responsibilities, and responses. Similarly, Mayer et al. [38]'s study reported that many real-world victims either failed to recognize their exposure or misattributed it to their own poor practices rather than organizational or attacker faults. In terms of trust and expectations, Hillmann et al. [26] and Fiesler et al. [18] showed that expectations toward breached organizations varied with incident severity and data sensitivity.

Despite such reported user concerns and awareness, many studies have demonstrated a persistent gap between perception and action. For example, Zou et al. [62] and Mayer et al. [37] both found that although users expressed concern after experiencing a security incident, but seldom engaged in tangible measures such as changing passwords. This gap between intention and action highlights a persistent challenge in everyday security practices.

While prior work has shed light on user-centered security, SIM-related incidents remain underexplored. Unlike typical data breaches, SIM compromises directly target the authentication layer, yet users often lack understanding of SIM operations and rarely recognize the SIM itself as a security vulnerability. Because SIM mechanisms largely function as a "black box" for end-users, this knowledge gap is even more pronounced, underscoring the need for further investigation.

Mental model provides a lens for analyzing how people interpret security and how these interpretations shape their behaviors [30]. Flawed mental models on password management, encryption, and smartphone security settings distort decision-making and constrain protective behaviors [14, 19, 30]. Recent work in smartphone security further demonstrated how both technical and social strategies shape users' intentions and practices [27]. Notably, drawing tasks have proven effective in externalizing users' mental models, revealing mismatches between technical mechanisms and user perceptions [14, 30].

3 Study Design

We conducted semi-structured interviews to investigate people's overall awareness, behavioral and emotional responses to the incident, as well as their mental models of SIM operations. Mental models are internal representations of real, hypothetical, or imagined situations that reflect how individuals think a system works and predict the outcomes of their actions [30]. This approach is particularly suitable for studies in usable security, where understanding users' mental representations of security-related systems helps explain their decisions and behaviors.

3.1 Participants

We recruited 33 participants through a local community platform, including both SKT (N= 17) and non-SKT users (N= 16) in their 20s through 60s. The incident occurred in April 2025, and recruitment took place from July onwards. Table 1 summarizes the demographic distribution by age, gender, carrier, SIM type, and device platform. The sample was balanced across most age groups, with diverse educational backgrounds and a mix of Android and iOS users. Among SKT users, 9 participants reported replacing their SIM cards after the incident. All participants provided informed consent and received approximately 30,000 KRW (about 20 USD) as compensation.

3.2 Procedure

Interviews were conducted online via Google Meet, with audio and screen-sharing permission, and lasted approximately 40 minutes. At the start of each session, participants were briefed on the study purpose and provided recorded verbal consent. Following the verbal consent, participants submitted a signed copy of the written consent form. A semi-structured interview guide, refined through pilot sessions, ensured consistency across sessions while allowing participants to elaborate in their own terms. The interview then proceeded through the following stages.

3.2.1 Awareness and Threat Perception. To establish participants' baseline understanding, each session began with a brief overview of the incident. Participants then described what they already knew, which threats felt most concerning, and their familiarity with SIM-related attacks such as SIM swapping or cloning.

3.2.2 Psychological and Behavioral Responses. Building on the initial awareness, participants discussed how they reacted to the incident. They reflected on their trust in SKT's security practices and any coping actions they had taken. SKT users were asked about SIM replacement decisions, while non-SKT users discussed whether the incident affected their general mobile usage. We did not measure trust or behavioral change; responses were collected through open-ended prompts only.

3.2.3 Mental Model Elicitation. To further examine how participants made sense of the incident, we asked them to complete a brief drawing task illustrating how they believed a SIM card works during phone communication and app authentication. Participants shared their screens and explained their sketches, allowing us to capture their reasoning and assumptions about SIM operations.

3.2.4 Post-Session Reflection. Because pilot interviews showed that many participants had limited baseline understanding of SIM functions, sessions concluded with a short explanatory video. This step was not intended as an educational intervention but simply provided an accurate technical context. After the video, participants were asked a small set of reflective questions. For example, whether any part of the explanation differed from what they had assumed earlier, or their willingness to change their mobile usage in a more protective manner. These questions were purely reflective; we did not evaluate learning, conduct pre-post comparisons, or assess changes in follow-up behaviors. Rather, reflections were treated as qualitative comments than indicators of improvement (see Appendix A for the complete interview questionnaire).

3.3 Data Analysis

All interview sessions were transcribed, with personal identifiers such as names or contact information removed. Demographic attributes relevant to the analysis (e.g., age group, carrier, OS, SIM type) were retained to allow comparisons across participant groups. Four researchers independently conducted initial open coding, then compared interpretations, resolved discrepancies, and iteratively refined a shared set of themes. Following a reflexive thematic analysis approach [10], we focused on how participants understood SIM functionality, interpreted the breach, and negotiated coping strategies within their everyday mobile practices.

In addition to thematic analysis, we examined participants' drawings to characterize their mental models of SIM operation. Prior work commonly distinguishes between functional and structural mental models [44, 48]. Functional models reflect a general sense of what a system does without detailed mechanism-level understanding, whereas structural models include more technically accurate representations of system components and their relationships [21]. Our low, mid, and high categories were inductively derived from the drawings based on their level of detail and reasoning style, but they partially align with this functional-structural distinction. Low-level drawings showed minimal or pre-functional reasoning and did not reach the level of a functional explanation. Mid-level drawings demonstrated primarily functional reasoning focused on process flow without technical structure. High-level drawings combined functional flow with partial structural elements such as network entities, authentication steps, or data transfer paths. We therefore interpret the three levels as points along a continuum from minimal to increasingly functional and partially structural mental models.

4 Results

4.1 Awareness: Perception of SIM Security Risks (RQ1)

Participants showed limited awareness of the incident, often describing it simply as a "SIM card hack" learned through brief news or acquaintances. Most could not explain which data had been exposed or how the breach occurred. In this study, we refer to affected users as those whose SIM belonged to the carrier targeted in the breach (SKT), acknowledging that while we cannot confirm whether their individual accounts were specifically compromised, the exposure of the carrier's authentication database meant that all subscribers were potentially impacted. Responses from affected and non-affected users were generally similar. Only a few participants had looked up SIM functions, and they were unaware of secondary

Table 1: Participant demographics and SKT SIM authentication key breach response attributes: carrier, SIM type, and SIM replacement status.

ID	Gender	Age	Education Level	CS Background/Experience	Mobile OS	Carrier	SIM Type	SIM Replacement
P1	Male	20s	Undergraduate (Enrolled)	No	Android	SKT	Physical SIM	No
P2	Female	20s	Undergraduate (Enrolled)	No	iOS	SKT	Not sure	No
P3	Male	20s	High School	No	Android	LG U+	eSIM	N/A
P4	Male	30s	Master's (Enrolled)	No	Android	SKT	Physical SIM	Yes
P5	Female	40s	Ph.D.	No	Android	SKT	Physical SIM	Yes
P6	Male	40s	Bachelor's	No	Android	SKT	Physical SIM	Yes
P7	Male	20s	Master's (Enrolled)	No	iOS	SKT	Physical SIM	Yes
P8	Male	30s	Bachelor's	3+ years in IT company (development lead)	Android	KT	Physical SIM	N/A
P9	Female	50s	Bachelor's	No	iOS	SKT	Physical SIM	Yes
P10	Female	50s	Bachelor's	No	Android	LG U+	Not sure	N/A
P11	Male	30s	Bachelor's	Military service in IT/InfoSec, certification	Android	LG U+	Physical SIM	N/A
P12	Male	30s	Bachelor's	No	Android	SKT	Physical SIM	No
P13	Male	50s	Bachelor's	No	Android	LG U+	Physical SIM	N/A
P14	Male	20s	Undergraduate (Enrolled)	No	iOS	KT	Physical SIM	N/A
P15	Female	20s	Master's (Enrolled)	No	Android	SKT	eSIM	Yes
P16	Female	60+	High School	No	iOS	KT	Physical SIM	N/A
P17	Male	40s	Master's	No	Android	KT	Physical SIM	N/A
P18	Female	30s	Bachelor's	Undergraduate C language coursework	iOS	SKT	Physical SIM	Yes
P19	Male	50s	Bachelor's	No	Android	KT	Physical SIM	N/A
P20	Female	20s	Undergraduate (Enrolled)	No	iOS	KT	eSIM	N/A
P21	Male	60+	Bachelor's	No	Android	SKT	Physical SIM	No
P22	Female	40s	Bachelor's	No	Android	LG U+	Not sure	N/A
P23	Female	30s	Bachelor's	No	Android	SKT	Physical SIM	Yes
P24	Female	20s	Undergraduate (Enrolled)	No	iOS	LG U+	Physical SIM	N/A
P25	Female	40s	Master's	No	Android	SKT	Physical SIM	No
P26	Female	40s	Bachelor's	No	iOS	LG U+	Physical SIM	N/A
P27	Male	40s	Bachelor's	No	iOS	LG U+	Physical SIM	N/A
P28	Female	50s	Bachelor's	No	Android	LG U+	Physical SIM	N/A
P29	Female	30s	Master's	No	Android	LG U+	Physical SIM	N/A
P30	Male	60+	Bachelor's	No	Android	LG U+	Physical SIM	N/A
P31	Female	60+	Bachelor's	No	Android	SKT	Physical SIM	No
P32	Female	50s	High School	No	Android	SKT	Physical SIM	No
P33	Male	50s	High School	No	Android	SKT	Physical SIM	Yes

threats like SIM swapping or cloning. Participants' overall awareness of the incident and their corresponding response patterns are summarized in Table 2.

The dominant concerns raised by participants were **financial loss** and **identity theft**, reflecting how mobile services are tied to banking and identification in Korea. P9 (SKT) said, "*If whatever the thing called SIM gets hacked, somebody's going to take my money away.*" P13 (non-SKT) noted, "*Smartphones are basically your identity card across apps... If that gets stolen? I don't even want to think about it.*" Some mentioned risks to children or work data; P22 (non-SKT) asked, "*What if my hacked phone reaches out to my kids?*" and P5 (SKT) said, "*I work at a biopharmaceutical company and I exchange lots of emails and messages regarding drug development. I'm more worried about such data leakage than the money loss.*" While participants occasionally mentioned other risks (e.g., reputational or social consequences), these were sparse and typically framed as extensions of financial loss or identity theft rather than distinct concern categories.

Despite acknowledging the severity of the incident, many felt low personal concern. Repeated exposure to security problems created a **sense of helplessness**, as P25 (SKT) remarked, "*We can't avoid being the target and there's nothing we can do about it.*" **Reliance on large companies** was common, summarized by comments like "*It's a big company, so they will take care of it.*" Participants generally viewed SIM-related security as a structural issue that companies should manage rather than an individual responsibility.

Limited understanding of the SIM's role was a frequently cited factor contributing to such reactions. P20 (non-SKT) said, "*The news says it's serious, but what exactly should I be worried about?*" and P2 (SKT) added, "*I don't even know what a SIM card actually is or what those 21 data types mean...*" Some recognized the severity only after simple external explanations, as P28 (non-SKT) described, "*I wasn't worried when I first heard the news. It was only after I came across a YouTube video explaining the incident and then I realized how serious this case is.*"

Some participants also believed their data had little value. **Perceived low data value** was reflected in comments such as P7 (SKT), "*If I rated my personal data, I'd say 150 won (approximately 0.11 USD).*" The **low visibility of harm** also made the threat seem distant and unlikely. Participants perceived the potential consequences of SIM card hacking as abstract and unlikely, partly because they had never encountered anyone who suffered serious problems directly due to SIM issues.

4.2 Response: Psychological and Behavioral Reactions (RQ2)

We further examined participants' psychological and behavioral responses to the incident. Differences between those directly affected (SKT) and non-affected (non-SKT) were minimal, suggesting that direct exposure did not strongly influence perceived vulnerability or coping actions.

Table 2: User awareness, psychological and behavioral response to the SKT SIM authentication key breach. (The counts reported in Awareness category indicate the number of participants who mentioned each theme at least once, rather than mutually exclusive categories. Counts in the Response category are mutually exclusive. Self-initiated coping includes participants from both SKT and non-SKT carriers.)

Category	Theme	Sub-Theme	Description	N
Awareness	Concern type	Financial loss	Risk of unauthorized financial charges or monetary harm.	25
		Identity theft	Risk of impersonation or misuse of personal identity data.	20
	Factors of low concern	Learned helplessness	Users normalized frequent security incidents (phishing, ransomware) as inevitable.	31
		Reliance on big-tech companies	Users assumed large companies (telecoms, tech giants) would handle security.	18
		Lack of knowledge	Limited understanding of SIM functionality and data breaches; information felt unclear or overwhelming.	22
		Perceived low personal risk and data value	Users underestimated personal risk, believing their data had little value.	29
		Low visibility of SIM-related damage	Consequences of SIM hacking are perceived as abstract and unlikely due to lack of direct experiences.	26
Response	Psychological reactions	Low trust	Low trust in the company's security measures.	27
		High trust	High trust due to compensation or visible measures.	6
		Low relevance to self	Users feel the issue does not affect them.	25
		High relevance to self	Users feel personally affected or at risk.	8
	Behavioral reactions	Full compliance (SIM replacement + services)	Most SKT users replaced their SIM as recommended, sometimes adding optional services (e.g., roaming block, spoofing block, protection service).	9
		Partial compliance (service only)	Some enrolled only in the protection service, citing time, cost, and effort.	2
		No action	Several participants took no action, often due to fatigue, indifference, or the absence of visible threats.	5
		Self-initiated coping	Few went beyond carrier guidance, such as learning about SIM security or changing everyday practices.	2

4.2.1 Psychological Response: Changes in trust. Overall, participants expressed **low trust** toward the company and its reported security measures. Many criticized the firm for prioritizing profit and doubted that SIM replacement alone could resolve what they perceived as a system-level issue. P12 (SKT) said, "*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.*" Others emphasized structural management failures. P16 (non-SKT) remarked, "*This didn't happen because something was wrong with my SIM. It happened because the company failed to manage SIMs properly.*"

In contrast, some participants expressed **high trust** due to compensation or visible security measures. P21 (SKT) stated, "*I trust them a lot. They're a big company. They give more data and discounts because of the accident.*" P27 (non-SKT) felt reassured by physically replacing the SIM, saying, "*I'd feel safer with the physical SIM replacement. At least I can see it being done.*" P18 (SKT) trusted software-based SIM protection more, stating, "*The SIM protection service feels like a more reliable, ongoing safety measure. I didn't even replace my SIM.*"

These trust patterns showed a modest demographic tendency. Low trust was most common among participants in their 20s and 30s, while high trust appeared more frequently among older age groups in their 40s and above. Gender, carrier type, and education level were more evenly distributed across trust groups and did not show clear differences. Overall, age-related expectations about institutional responsibility and visible protection measures seemed to shape participants' trust more than other demographic characteristics (see Appendix B).

4.2.2 Psychological Response: Relevance to self. Directly affected SKT users often treated the incident as distant, adopting a detached stance. P2 (SKT) said, "*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.*"

Non-SKT users showed mixed attachment and detachment. Attachment was more situationally contingent, reflecting factors such as perceived personal vulnerability and concern for others. For example, P11 (non-SKT) noted, "*It never really felt like someone else's problem. SKT got hit big this time, but other carriers have had even more hacks before.*" Some non-affected participants described concern for family members who used SKT, even when their own accounts were not at risk. P10 (non-SKT) reported, "*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.*" Others explained that they checked whether their parents or older relatives needed to replace their SIM cards, contacted the carrier on their behalf, or advised them to switch providers, reflecting worry about family members' limited awareness of SIM-related risks and their potential vulnerability. Some treated it as someone else's problem, saying, "*As soon as I checked I'm not the target, I just deleted the news.*" (P22, non-SKT).

4.2.3 Behavioral Response: SIM replacements and changes in mobile usage. Following psychological responses, we asked participants whether they had taken any behavioral measures after the incident. Among SKT users, most replaced their SIM card as recommended (N = 9), some opted only for the protection service (N = 2), and others took no action (N = 5). Across all participants, including those from other carriers, a small number engaged in self-initiated behaviors, such as studying SIM-related security or adjusting mobile practices. Overall, compliance patterns varied: full compliance among SKT users reflected both relief and lingering insecurity, partial compliance was often driven by cost or convenience, and non-compliance stemmed from fatigue, indifference, or the lack of visible threats. Self-initiated practices were rare and typically short-lived, indicating that most participants relied primarily on the carrier's recommendations.

Full compliance (SIM replacement + services): Most SKT users replaced their SIM as recommended, sometimes adding optional services. P23 (SKT) said, "*Yes, I replaced my SIM. I also signed up for services. Even after all this, I'm still not sure if I'm secure enough.*"

Partial compliance (service only): Some enrolled only in the protection service due to time, cost, or effort. P12 (SKT) noted, "*Replacing it takes time and money. Instead, I signed up for the protection service. It feels like the best safety net I have for now.*"

No action: Several participants took no action, often due to fatigue, indifference, or lack of visible threats. P31 (SKT) said, "*When you get old, it takes way more effort to understand what's going on. I'm just tired.*"

Self-initiated coping: When asked about any self-initiated coping behavior out of privacy concerns, few participants (including non-SKT users) went beyond carrier guidance, such as learning about SIM security or changing everyday practices. P29 (non-SKT) explained, "*I started using the automatic password-saving feature less often. It could be a security risk.*"

Overall, users' psychological and behavioral responses suggest that emotional trust and actual behavior can diverge, reflecting an awareness-action gap [22]. Many assume that large corporations manage security, which fosters passive behaviors even when incidents occur. While emotional trust may decline after a breach, this does not necessarily lead to proactive action. Users appeared to recognize that the system is highly centralized around a few major providers, limiting the scope of individual influence. This perception, combined with a sense of learned helplessness, seems to constrain behavioral change even when confidence in the provider is reduced.

4.3 Mental Models: SIM Operation and Authentication (RQ3)

Lastly, we answer RQ3, "*How do users conceptualize the operation of SIM cards and SIM-based authentication in everyday smartphone use?*" To assess participants' general understanding of SIM, we asked participants to explain the role of SIM in mobile phones and the types of information stored within them to illustrate their mental models through a drawing exercise. The responses revealed varying levels of understanding. A few participants recognized the SIM as a critical security component responsible for communication, authentication, and identification. However, most participants had limited or incomplete knowledge about its functions, with only a small number demonstrating accurate mental models of SIM operations.

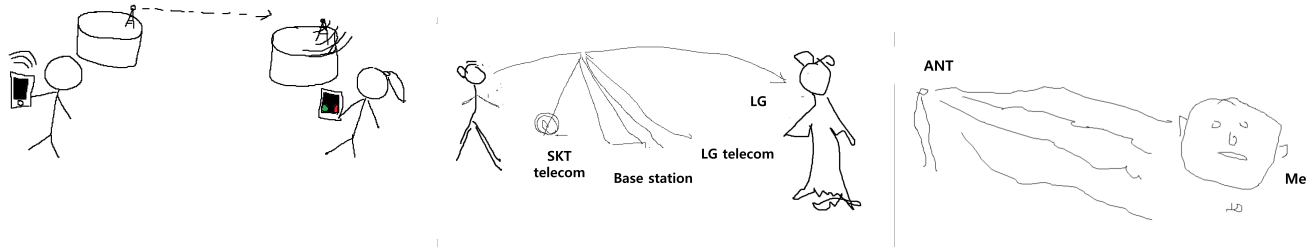
4.3.1 Conceptual Understandings of SIM Cards. Prior to the drawing exercise, the research team asked participants to describe what a SIM card is and how it functions. More than half of the participants (N = 17) acknowledged that the SIM is essential and related to personal information, but their understanding of its specific functions and stored data was limited. P19 (non-SKT) said, "*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.*" Some mistakenly believed that sensitive personal data, such as social security numbers, passport numbers, or financial records, were stored on the SIM. Overall, participants consistently recognized the SIM's importance and association with personal information, but their technical understanding of its role was often vague or inaccurate.

A smaller group demonstrated either very high (N = 7) or very low (N = 9) comprehension. Highly understanding participants often used metaphors such as a car key or ID card; for example, P13 (non-SKT) likened the SIM to a car key that enables the phone to operate. In contrast, those with very low understanding were either unaware of the SIM's existence or saw it merely as a chip for communication abroad, as P26 (non-SKT) put it, "*I think SIM is not necessarily related to personal data. It's just a card for data usage when going abroad.*"

4.3.2 Diversity in Mental Model Representations. Differences in understanding became more pronounced in the drawing task, where participants were asked to illustrate two representative SIM use cases: (1) call setup and (2) authentication for mobile application usage (e.g., mobile banking). Drawings ranged from detailed technical sketches to simple marks, and several participants avoided the task altogether. Based on the level of detail and reasoning style in these sketches, participants' mental models could be interpreted along a continuum from minimal to increasingly functional and partially structural. In this sample, participants in their 20s–40s more often demonstrated mid- to high-level models, while those in their 50s and older were more commonly found in the low-level group. Other demographic factors did not show consistent patterns (see Appendix C).

Low-level models showed minimal or pre-functional reasoning. Sketches were highly abstract, often limited to a SIM card icon, arrows, or brief labels such as "connects to carrier," without articulating how calls or authentication occur. These drawings lacked process flow, dependencies, or identifiable system actors, reflecting limited understanding among younger participants with no prior exposure and older adults with restricted digital experience.

Mid-level models reflected functional reasoning but without structural precision. Participants in this group captured general ideas such as the SIM "verifying identity," "routing calls," or "connecting to the network," yet their diagrams oversimplified procedures or omitted major components. Their sketches focused on sequential flow but did not depict how the SIM interacts with backend systems or authentication services, a pattern common among



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

Figure 2: Participant-generated mental models of the call process across three levels of understanding: (a) high, (b) mid, and (c) low. (Original Korean handwriting has been translated into English and typeset for readability and anonymization.)

participants with extensive banking experience but limited technical familiarity.

High-level models combined functional flow with partial structural elements. Drawings included network entities such as base stations, carrier servers, or authentication paths, showing how SIM credentials participate in call setup or app-based verification. While not fully expert-level, these sketches were logically reasoned and internally consistent, typically produced by younger adults with technical training or prior security experience.

Despite these differences, even some high-level participants struggled to correctly connect SIM functions to mobile application authentication. Several could verbally describe what the SIM "does," yet still failed to situate the SIM within real-world communication and authentication processes. These gaps illustrate that participants' mental models were often fragmentary even when individual components appeared well understood.

Scenario 1: Call process In the call process scenario, only a small number (N = 6) systematically depicted key components such as the base station, carrier servers, and authentication procedures, recognizing that the SIM card handles authentication, identification, and network access (See Figure 2a, high level). For example, P1 (SKT) explained, "*The signal is delivered to the telecom operator via SIM, then passed through the base station and finally to the recipient's phone.*"

Most participants (N = 18) showed a medium-level understanding, identifying the caller, receiver, telecom operator, and base stations, but focusing mainly on the relay of voice signals rather than the SIM's role. P10 (non-SKT) drew a simple connection between these components and remarked, "*I don't think any other information is transmitted. Probably just the voice signal*" (Figure 2b).

A smaller subset (N = 9) including several older adults and participants in their early twenties demonstrated minimal or misconceived interpretations of the SIM's function (Figure 2c). One older adult, P21 (SKT), even imagined the SIM as "digesting" signals inside the ear and sending them to the brain: "*The SIM in my ear absorbs the signals and delivers them to the brain. That way we communicate.*" These responses reflect how far their conceptual models diverged from the SIM's actual technical role.

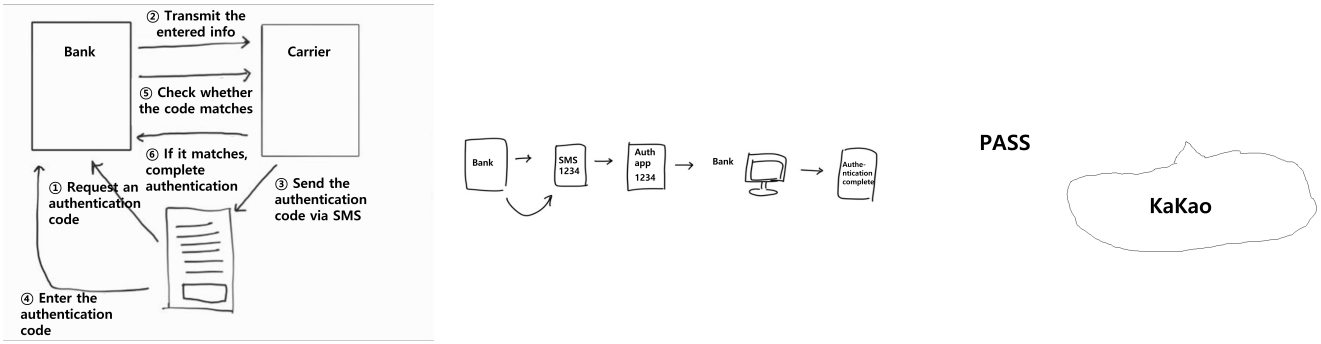
Scenario 2: Authentication Participants also showed varied and often limited understandings of SIM-based authentication. A small number (N = 6) demonstrated a high-level grasp by clearly separating the roles of the user, bank, and mobile carrier. P29 (non-SKT), for example, described the full sequence of entering information, the bank requesting verification, the carrier issuing and delivering a code via SMS, and the bank validating it, reflecting an accurate understanding of SIM-mediated code delivery (Figure 3a, high level).

Most participants (N = 16) held medium-level or incomplete mental models. Some believed the entire process – from issuing to verifying authentication codes – was handled solely by banks. P2 (SKT) noted, "*I think there's a department at a bank fully dedicated to authentication… they issue and verify the code.*" Others attributed responsibility to third-party apps or public agencies, or assumed that the SIM itself performed verification, conflating the SIM's routing function with server-side checks (Figure 3b, medium level).

Participants with low-level understanding (N = 11) either omitted key steps or entirely separated authentication from the SIM. P26 (non-SKT), for instance, referred only to familiar services like PASS (a mobile carrier–based identity verification app widely used in Korea) or Kakao (a widely used messaging platform) and concluded, "*This is authentication done on the site, so it is possible without a SIM*" (Figure 3c, low level). These responses indicate that many participants viewed authentication as a service-level action rather than a process dependent on the SIM for message delivery and device linkage.

4.3.3 Post-Session Reflection. After exploring participants' overall mental models of SIM cards, sessions concluded with a short instructional video explaining SIM functionality. Following the video, participants were asked a small set of reflective questions, such as whether any part of the explanation differed from their prior assumptions, what they learned from the video, and whether they would consider changing their mobile usage to be more protective. These questions were intended to capture participants' reflections on understanding and perceived risk, not to measure actual learning outcomes or behavioral change.

Based on interview responses, 20 reported gaining new insights while 7 reported no new learning, and 6 indicated that they were unsure. Women were more likely than men to report learning (12 of 20 learners were female). All participants in their 20s and 60s reported learning, while participants in their 30s and 50s showed more mixed results. Participants with prior CS experience (3 of 3 respondents) were among those less likely to report learning. Education level did not strongly predict learning, as even highly



(a) High level (P29) **(b) Medium level (P2)** **(c) Low level (P26)**

Figure 3: Participant-generated mental models of the authentication process across three levels of understanding: (a) High, (b) Mid, (c) Low. Original Korean handwriting has been translated and typeset for readability and anonymization.

educated participants often reported gaps in understanding. Carrier type, SIM type, and prior SIM replacement showed no clear association with reported learning.

Participants with initially limited understanding often provided more detailed descriptions after the video, moving beyond seeing SIMs merely as communication chips. For example, P24 (non-SKT) reflected, "*I used to think they were simply for storing my information, but I realized they connect to base stations, contain a lot of information, and that the leakage incident was more serious than I had imagined.*" Misconceptions, such as believing SIMs store resident registration numbers, were occasionally clarified. P28 (non-SKT) emphasized the need for easy-to-use security measures for older adults and children.

Although participants gained awareness and understanding, this did not uniformly translate into intention to act. Among the 20 who reported learning, 8 participants, particularly women in their 50s, indicated little or no intention to change their mobile security behaviors, with statements like P10 (non-SKT), "*Nothing will change even if I try*," and P4 (SKT), "*Telecom providers should handle it.*"

5 Discussion

We summarize the major findings by examining how Korean end-users perceived and made sense of the recent SKT SIM authentication key breach, and by outlining the current landscape of users' mental models of SIM and SIM-based authentication. We highlight the gaps between technical mechanisms and user perceptions, and discuss how these gaps shape risk awareness, security behaviors, and broader trust in digital services.

5.1 The Paradox of High Dependency and Passive Response in the Korean Context

Contrary to our hypothesis that affected and non-affected users would exhibit distinct levels of awareness or behavioral responses, findings revealed minimal disparities. Most users conceptualized the incident broadly as "being hacked," with few capable of specifying the exact nature of the compromised data. Participant concerns were primarily directed toward financial fraud and identity theft. This reflects South Korea's digital ecosystem, where online authentication infrastructure is tightly coupled with the *Resident Registration Number (RRN)* and carrier-based identity verification services (e.g., PASS) [31]. In this context, a mobile phone number functions not merely as a communication tool but also as a core credential for banking, government services, and online payments. Therefore, many regarded the breach less as a technical SIM failure and more as a threat to the stability of their digital identity.

Despite the high-stakes environment, concerns rarely translated into concrete actions. Even among affected users, SIM replacement was inconsistent. These findings resonate with the privacy paradox [22], illustrating the disconnect between user attitudes and actual behaviors, particularly where users weigh security risks against the costs of taking action. Users recognize the potential security risks (e.g., SIM card vulnerability, data breaches) but are often deterred by the associated costs (e.g., time, effort, inconvenience of SIM replacement). The perceived benefits—such as the decreased likelihood of a breach—may not outweigh these costs in users' assessments. We attribute such passive responses to cognitive biases, specifically optimistic bias (e.g., "it won't happen to me") and an illusion of control (e.g., users assuming that as long as their phone "works normally," the underlying SIM credentials must also be safe, even when this assumption has no technical basis) [23, 54, 59]. These biases likely shape participants' mental models, reinforcing surface-level interpretations and limiting their sense of urgency or vulnerability. In this context, users may underestimate the long-term benefits of enhanced security due to the perceived high immediate costs of implementing protective measures [2].

This awareness-action gap also reflects the broader cultural context of South Korea, where strong reliance on centralized institutions often reduces the sense of individual responsibility for personal security. Although structural trust in the mobile carrier

remained stable, psychological trust declined, and this shift did not lead to more proactive behavior. Such observation aligns with prior studies in information security that show that the degree of trust is a leading factor affecting risk perception and following actions [28, 35]. The combination of structural lock-in and a learned sense of limited agency appears to weaken protective actions even when users are aware of potential risks. In addition, constant exposure to news about phishing and ransomware contributed to a feeling that such threats are unavoidable. Many participants, especially older adults, perceived these incidents as part of everyday digital life, a view reinforced by the "invisible" nature of SIM technology once it becomes embedded in the device [30].

Taken together, these structural, cognitive, and cultural constraints highlight why user-driven protective actions remain limited and underscore the need for design strategies that work with, rather than against, these everyday realities.

5.2 Mental Models and Knowledge Gaps Around SIM Security

Interview findings revealed that most participants had a limited understanding of SIM functionalities and their relation to personal information. Participants' mental models varied. Some highly articulate users drew detailed diagrams and employed diverse metaphors, such as comparing SIM to a car engine or a key, seeing the smartphone as mere hardware, or equating the SIM to the heart or an ID card. Most participants had intermediate understanding, recognizing that SIM contained personal information but unable to explain the underlying mechanisms, typically adults in their 30s to 40s who actively used banking or authentication services. A smaller group had minimal awareness, often younger or older adults, who saw SIM as a chip swapped during travel or phone replacement. This spectrum of mental models reflects a behavioral pattern seen in the literature, where users often struggle to understand the technologies they engage with [60, 61]. Even participants with detailed diagrams could not explain the connection between SIM and authentication, limiting their perception of its functional importance. This contributed to the belief that SIM compromise would not disrupt phone functionality or personal data, reinforcing passive responses. Cognitive biases and reliance on institutional infrastructure further constrained proactive behavior. In post-session reflections after a short instructional video on SIM functionality, many participants reported gaining new insights, particularly about SIM connectivity and potential data exposure. However, these insights did not consistently translate into intentions to change behavior. Some participants, particularly women in their 50s, expressed limited motivation to act, emphasizing the responsibility of telecom providers and that protective actions would have little effect. These findings indicate that limited mental models, structural reliance, and cognitive biases shape user responses, while brief educational interventions may improve understanding but are insufficient to consistently induce behavioral change [32, 52].

5.3 Design Implications

5.3.1 Perceptible Security Touchpoints. SIM security largely operates at a low-level system layer, and most users do not need to understand all technical mechanisms to use mobile services safely. Functional mental models are typically sufficient for correct use, and exposing full structural details could increase cognitive load without meaningful benefit [25, 60, 61]. To foster these functional models, interfaces can employ accessible metaphors (e.g., depicting the SIM as a 'network access key' or 'subscriber identity card') that better articulate its active security role while aligning with users' intuitive understanding [13, 51]. Design can then highlight critical touchpoints throughout the device lifecycle. For instance, visualizing the SIM's role during initial insertion can establish a mental model of security, while indicating when SIM-based authentication occurs or clarifying the data flow between the service and carrier during requests can reinforce it. This approach makes key processes perceptible without overloading users or turning them into security experts. Findings from our study align with prior work showing that users often rely on surface-level cues and operational continuity as proxies for security [30]. Because critical authentication events occur invisibly, users may misattribute safety to device functionality rather than underlying mechanisms, reinforcing an inflated sense of control [43]. Interfaces that make these touchpoints perceptible can recalibrate user expectations by foregrounding when sensitive operations occur and what data is involved, without requiring detailed technical comprehension [17].

5.3.2 Targeted and Reflective Education. Brief interventions such as short video tutorials were most helpful for participants with a very limited understanding of SIM functionality. These activities clarified basic connectivity and potential data exposure, supporting the formation of functional mental models [5, 11, 13]. However, these gains did not consistently translate into behavioral change, and most users remained reliant on mobile carriers. This underscores that education should focus on filling specific knowledge gaps rather than exposing all structural details or attempting to train every user as a security expert. This pattern is consistent with work showing that security education is effective only when it aligns with users' pre-existing interpretations and everyday practices [34]. To achieve this, security education should emphasize real-world scenarios, demonstrating how SIM compromises could intersect with banking, messaging, or identity verification. Reflective framing that helps users articulate these connections may increase perceived relevance and encourage protective behavior [50]. By aligning security education with users' everyday practices and providing clear touchpoints, users can better understand potential risks and take proactive steps to safeguard their data.

5.3.3 Behavioral Nudges and Cultural Framing. Even when participants recognized the severity of the incident, proactive measures were rare. Interventions combining default protections and behavioral nudges can encourage everyday security practices: SIM PIN locks, automatic SIM replacement notifications, or just-in-time prompts (e.g., "one-click SIM replacement") can explain why an action is needed and what risk it mitigates [15, 20, 63]. This aligns with broader research showing that default-centric interventions reduce *cognitive burden* and reliably promote secure behavior in settings where the perceived locus of responsibility is externalized [3]. These nudges work best when paired with education that itself serves as a nudge, guiding users to understand risks and underlying processes in a way that prompts action. Furthermore, cultural and social framing can increase motivation. In the Korean context,

nudges may be more effective when paired with motivational framing that resonates with local social norms, since increasing the perceived relevance of action is essential for activating behavior. Such culturally tailored framing is particularly essential in contexts marked by institutional trust and structural dependency, as it can address motivational gaps that purely informational interventions fail to resolve [58]. Collectively, these strategies can narrow the action–awareness gap by lowering behavioral friction while resonating with local social norms and expectations.

6 Limitation

Our qualitative investigation (N = 33) examined a single SIM security incident in South Korea, limiting cross-cultural generalizability but providing insight into a highly digitized context where phone-based authentication underpins banking, government, and commerce. To capture diverse perspectives, we purposefully sampled participants across ages (20s–60s), occupations, technical backgrounds, and incident exposure (SKT vs. non-SKT). While mechanisms such as learned helplessness, corporate reliance, and technical invisibility emerged, our cross-sectional design cannot establish causal relationships. Additionally, since interviews were conducted months after the incident, findings rely on participants' retrospective self-reports, which may be subject to recall bias or differ from actual behavioral logs. Future work could employ longitudinal or experimental methods to track how mental models evolve after a breach and evaluate interventions aimed at closing the awareness–action gap.

7 Conclusion

This study examined how mobile users in South Korea perceived and responded to a nationwide SIM authentication key breach. We found a clear gap between awareness of the breach and protective action. Participants often held incomplete or incorrect mental models of SIM authentication, perceived little personal risk, and placed strong trust in mobile carriers, resulting in limited behavioral change. A brief educational intervention improved conceptual understanding but did not lead to sustained protective practices, showing how technical invisibility and psychological factors jointly inhibit protective action. These results highlight opportunities for more effective security design, such as making core SIM processes more visible, providing contextual explanations for security decisions, and reducing the effort required to replace or secure SIM cards.

Acknowledgments

Corresponding authors of this work are Hyoungshick Kim and Uichin Lee. This research was supported by the Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (RS-2025-02305801,RS-2024-00438686,RS-2024-00459638)

References

[1] 2025. SIM Security Tutorial. YouTube, ChannelName. https://www.youtube.com/watch?v=ChNE2XhRfosXXX Accessed: 2025-09-12.
[2] Alessandro Acquisti, Leslie K John, and George Loewenstein. 2013. What is privacy worth? *The Journal of Legal Studies* 42, 2 (2013), 249–274.
[3] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.
[4] Abu Shohel Ahmed, Aleksi Peltonen, Mohit Sethi, and Tuomas Aura. 2024. Security analysis of the consumer remote sim provisioning protocol. *ACM Transactions on Privacy and Security* 27, 3 (2024), 1–36.
[5] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *International Journal of Human–Computer Interaction* 33, 11 (2017), 927–942.
[6] Nuril Anwar, Imam Riadi, and Ahmad Luthfi. 2016. Forensic SIM card cloning using authentication algorithm. *International Journal of Electronics and Information Engineering* 4, 2 (2016), 71–81.
[7] Jason Aten. 2019. SIM Swapping Is the Biggest Security Threat You Face, and Almost No One Is Trying to Fix It. *Here's Why It Matters. Inc. Sept* 17 (2019).
[8] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. 2021. What breach? Measuring online awareness of security incidents by studying real-world browsing behavior. In *Proceedings of the 2021 European Symposium on Usable Security*. 180–199.
[9] Eric Blancaflor, Drizzle Joy Caberto, Charlene Grazielle lara, and l Mancilla, Danielle Franchesca. 2024. Guarding Against Phone Scammers: An Examination of Gaining Access to Phone Contacts through Smishing Social Engineering Exploits. In *Proceedings of the 2024 10th International Conference on Computing and Artificial Intelligence*. 365–372.
[10] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology* 18, 3 (2021), 328–352.
[11] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2010. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy* 9, 2 (2010), 18–26.
[12] Builtin. 2024. What is a SIM Card and how does it work? https://builtin.com/hardware/what-is-a-sim-card
[13] L Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and society magazine* 28, 3 (2009), 37–46.
[14] Prakriti Dumaru, Ankit Shrestha, Rizu Paudel, Cassity Haverkamp, Maryellen Brunson McClain, and Mahdi Nasrullah Al-Ameen. 2024. "… I have my dad, sister, brother, and mom's password": unveiling users' mental models of security and privacy-preserving tools. *Information & Computer Security* 32, 3 (2024), 282–303.
[15] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1065–1074.
[16] Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. 2023. *5G Wireless Network Security and Privacy*. John Wiley & Sons.
[17] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14.
[18] Casey Fiesler and Blake Hallinan. 2018. "We Are the Product" Public Reactions to Online Data Sharing and Privacy Controversies in the Media". In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.
[19] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–24.
[20] Alisa Frik, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. 2019. A promise is a promise: The effect of commitment devices on computer security intentions. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.
[21] Sarah Abdelwahab Gaballah, Lamya Abdullah, Ephraim Zimmer, Sascha Fahl, Max Mühlhäuser, and Karola Marky. 2025. "It's Not My Data Anymore": Exploring Non-Users' Privacy Perceptions of Medical Data Donation Apps. *Proceedings on Privacy Enhancing Technologies* (2025).
[22] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* 77 (2018), 226–261.
[23] Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries, and Max Mühlhäuser. 2012. Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing: Advances, Systems and Applications* 1, 1 (2012), 19.
[24] Zahra Hassanzadeh, Robert Biddle, and Sky Marsen. 2021. User perception of data breaches. *IEEE Transactions on Professional Communication* 64, 4 (2021), 374–389.
[25] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*. 133–144.
[26] Felix Hillmann, Tim Klauenberg, Lennart Schroeder, and Till Ole Diesterhöft. 2023. A User-centric View on Data Breach Response Expectations.. In *CIISR@ Wirtschaftsinformatik*. 19–37.

[27] Hsiao-Ying Huang, Soteris Demetriou, Muhammad Hassan, Güliz Seray Tuncay, Carl A Gunter, and Masooda Bashir. 2023. Evaluating user behavior in smartphone security: a psychometric perspective. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 509–524.

[28] Sirkka L Jarvenpaa, Noam Tractinsky, and Michael Vitale. 2000. Consumer trust in an Internet store. *Information technology and management* 1, 1 (2000), 45–71.

[29] Ji-hye Jun. 2025. Credit card firms exit ID verification services amid dominance of telecom-led authentication. The Korea Times. https://www.koreatimes.co.kr/business/banking-finance/20250425/credit-card-firms-in-south-korea-exit-id-verification-services-amid-dominance-of-telecom-led-authentication Accessed: 2025-09-12.

[30] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. {"My} data just goes {Everywhere:"} user mental models of the internet and implications for privacy and security. In *Eleventh symposium on usable privacy and security (SOUPS 2015)*. 39–52.

[31] Jongbae Kim. 2024. Personal Identity Proofing for E-Commerce: A Case Study of Online Service Users in the Republic of Korea. *Electronics* 13, 19 (2024), 3954.

[32] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. 2009. " When I am on Wi-Fi, I am fearless" privacy concerns & practices in eeryday Wi-Fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1993–2002.

[33] Brian Krebs. 2018. Busting SIM Swappers and SIM Swap Myths. *Krebs on Security. Nov* 7 (2018).

[34] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M Angela Sasse. 2015. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. *arXiv preprint arXiv:1501.04434* (2015).

[35] Hyunsoo Lee, Soowon Kang, and Uichin Lee. 2022. Understanding privacy risks and perceived benefits in open dataset collection for mobile affective computing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2 (2022), 1–26.

[36] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, and Arvind Narayanan. 2020. An empirical study of wireless carrier authentication for {SIM} swaps. In *Sixteenth symposium on usable privacy and security (soups 2020)*. 61–79.

[37] Peter Mayer, Yixin Zou, Byron M Lowens, Hunter A Dyer, Khue Le, Florian Schaub, and Adam J Aviv. 2023. Awareness, intention,(In) action: individuals' reactions to data breaches. *ACM Transactions on Computer-Human Interaction* 30, 5 (2023), 1–53.

[38] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J Aviv. 2021. " Now I'm a bit {angry:}" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *30th USENIX Security Symposium (USENIX Security 21)*. 393–410.

[39] Ahmed A Moustafa, Abubakar Bello, and Alana Maurushat. 2021. The role of user behaviour in improving cyber security management. *Frontiers in Psychology* 12 (2021), 561011.

[40] S Murugalakshmi, D Doreen Hepzibah Miriam, and CR Rene Robin. 2023. Advancements in Mobile Security: A Comprehensive Study of SIM Card Swapping and Cloning-Trends, Challenges and Innovative Solutions. *i-manager's Journal on Mobile Applications and Technologies* 10, 1 (2023), 23.

[41] Prajwol Kumar Nakarmi. 2021. "Cheatsheets for Authentication and Key Agreements in 2G, 3G, 4G, and 5G". *arXiv preprint arXiv:2107.07416* (2021).

[42] Boann News. 2025. [SKT Hacking Incident] SIM Card Replacement vs. SIM Card Protection... Is SIM Card Protection Service Enough for Peace of Mind? https://m.boannews.com/html/detail.html?idx=137022&tab_type=1

[43] Don Norman. 2013. *The design of everyday things: Revised and expanded edition*. Basic books.

[44] Donald A Norman. 2014. Some observations on mental models. In *Mental models*. Psychology Press, 7–14.

[45] Ministry of Science and ICT. 2025. SK Telecom Announces Final Investigation Results of Breach Incident. https://www.msit.go.kr/bbs/view.do?sCode=user&mPid=208&mId=307&bbsSeqNo=94&nttSeqNo=3185964

[46] Ministry of Science and ICT (South Korea). 2025. MSIT Releases Final Investigation Results on SK Telecom Data Breach. Press release, Ministry of Science and ICT. https://www.msit.go.kr/eng/bbs/view.do;jsessionid=hkKV7Gza1mcXySBSv1IJ6e9aM8mgmP8PU6Q6FqvH.AP_msit_1?sCode=eng&nttSeqNo=1139&bbsSeqNo=42&mId=4&mPid=2 Accessed: 2025-09-12.

[47] Okta. 2020. What is SMS authentication and is it secure? https://www.okta.com/blog/identity-security/sms-authentication/

[48] Rebecca Panskus, Max Ninow, Sascha Fahl, and Karola Marky. 2023. Privacy mental models of electronic health records: a German case study. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 525–542.

[49] Cyber Peace. 2025. SIM Cloning: The Silent Cyber Threat Putting Users at Risk. https://www.cyberpeace.org/resources/blogs/sim-cloning-the-silent-cyber-threat-putting-users-at-risk

[50] Alessandro Pollini, Tiziana C Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. 2022. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work* 24, 2 (2022), 371–390.

[51] Fahimeh Raja, Kirstie Hawkey, Steven Hsu, Kai-Le Clement Wang, and Konstantin Beznosov. 2011. A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In *Proceedings of the seventh symposium on usable privacy and security*. 1–20.

[52] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. 2014. Why doesn't Jane protect her privacy?. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 244–262.

[53] Reuters. 2025. SK Telecom shares plunge after data breach due to cyberattack ? https://www.reuters.com/sustainability/boards-policy-regulation/sk-telecom-shares-plunge-after-data-breach-due-cyberattack-2025-04-28/

[54] Hyeun-Suk Rhee, Young Ryu, and Cheong-Tag Kim. 2005. I am fine but you are not: Optimistic bias and illusion of control on information security. *ICIS 2005 proceedings* (2005), 32.

[55] Thomson Rreuters. 2025. A deep dive into the growing threat of SIM swap fraud. https://www.thomsonreuters.com/en-us/posts/corporates/sim-swap-fraud/

[56] Security Scorecard. 2025. SIM Card Hacking: What It Is, How It Works, and How to Protect Yourself. https://securityscorecard.com/blog/sim-card-hacking-what-it-is-how-it-works-and-how-to-protect-yourself/

[57] Statista. 2024. "Mobile Banking in South Korea – Statistics & Facts". https://www.statista.com/topics/8085/mobile-banking-in-south-korea/. Accessed 2025-11-28.

[58] Harry C Triandis. 1993. Cultures and Organizations: Software of the Mind.

[59] Katinka Waelbers. 2009. Technological delegation: Responsibility for the unintended. *Science and Engineering Ethics* 15, 1 (2009), 51–68.

[60] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 1–16.

[61] Rick Wash and Emilee Rader. 2011. Influencing mental models of security: a research agenda. In *Proceedings of the 2011 New Security Paradigms Workshop*. 57–66.

[62] Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J Aviv, and Florian Schaub. 2024. Encouraging users to change breached passwords using the protection motivation theory. *ACM Transactions on Computer-Human Interaction* 31, 5 (2024), 1–45.

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

Appendix

A Interview Questionnaire

1. Awareness and Threat Perception

- Were you aware of the recent incident involving SKT's SIM authentication key leakage?
- When and how did you first hear about it (e.g., news, SNS, acquaintances)?
- What do you remember about the incident? Please describe it in your own words.
- What kinds of information did you think were exposed?
- When you first heard about the incident, what aspects (if any) felt concerning or risky to you?
- Have you heard of attacks such as SIM swapping or SIM cloning? If yes, could you explain what you understand about them?

2. Psychological and Behavioral Responses

- Did you feel that the incident could potentially affect you personally? Why or why not?
- Are you aware of any protective actions recommended by SKT (e.g., SIM replacement)?
- How much do you trust these measures?
- (For SKT users) Did you replace your SIM card? If yes, what motivated your decision? If not, why did you choose not to replace it?
- (For non-SKT users) Did the incident influence your broader mobile usage or security behaviors?

3. Mental Model Elicitation

- How would you describe the role of a SIM card in everyday smartphone use?
- What kinds of information do you think are stored inside a SIM card?

Drawing Task Instructions. In this activity, we would like to understand how you think a SIM card works in two everyday scenarios. There are two short scenarios, and for each one, we ask you to draw what you believe is happening. This is not a test, and there are no right or wrong answers. You may use simple shapes, arrows, text labels, or any symbols that make sense to you.

Scenario 1: Person A calls Person B. Please draw how you think their phones connect and how the call goes through. After drawing, please explain the main steps and describe the role you think the SIM card plays. You may consider:

- What steps happen after Person A dials Person B?
- How does Person B's phone receive the call?
- What components might be involved (e.g., phones, SIM card, cell towers, mobile carrier)?
- What types of information might be exchanged between them?

Scenario 2: Person A is logging into a mobile banking app. To finish logging in, they tap "Send verification code" and receive an SMS code. Please draw how you think this verification process works—from requesting the code to completing the login. After drawing, please explain your diagram and describe the role of the SIM card in this verification process. You may consider:

- What happens right after Person A taps "Send verification code"?
- Who sends the SMS code?
- How is the entered code checked?
- What components are involved (e.g., phone, SIM card, mobile carrier, bank server)?
- What types of information may be exchanged?

4. Post-session Reflection

- After watching the video, was there anything that differed from what you previously assumed about SIM cards?
- Did the new information change your perception of mobile security or personal-data protection?
- Do you feel motivated to change any part of your mobile usage to be more secure? If yes, what kinds of changes would you consider?

B Trust Levels by Participant Demographics

Table 3 presents the distribution of participants' trust levels across demographic groups, mobile carriers, and education levels.

Table 3: Trust levels by demographics factors.

Trust Level	Age Group	Male	Female	Carriers	Education Level
Low	20s	P3	P15, P20, P24	SKT: P15, P20 / LG U+: P3, P24	HS: P3 / Undergrad: P15, P20, P24
	30s	P4, P8, P11, P12	P18, P29	SKT: P4, P12, P18 / KT: P8 / LG U+: P29	Bachelor: P8, P11, P12, P18, P29 / Master: P4
	40s	P6	P22, P26	SKT: P6 / LG U+: P22, P26	Bachelor: P6, P22, P26
	50s	P13	P28	LG U+: P13, P28	Bachelor: P13, P28
	60+	P30	P16	LG U+: P30 / KT: P16	Bachelor: P30 / HS: P16
High	30s	P17	P23	KT: P17 / SKT: P23	Master: P17 / Bachelor: P23
	40s	P27, P25	-	LG U+: P27 / SKT: P25	Bachelor: P27 / Master: P25
	50s	-	P10	LG U+: P10	Bachelor: P10
	60+	P21	-	SKT: P21	Bachelor: P21
Neutral / Uncertain	20s	P1, P7	P2, P14	SKT: P1, P2, P7 / KT: P14	Undergrad: P1, P2, P7, P14
	40s	-	P5	SKT: P5	Master: P5
	50s	P19, P33	P9, P32	SKT: P9, P32, P33 / KT: P19	HS: P32, P33 / Bachelor: P9, P19
	60+	-	P31	SKT: P31	Bachelor: P31

C Mental Model Levels by Participant Demographics

Tables 4 and 5 present the distribution of participants' mental model levels across demographic factors.

Table 4: Mental model levels for the call process scenario by demographic factors.

Demographic Factor	High (n=6)	Mid (n=18)	Low (n=9)
Age Group	20s: P1, P3 30s: P23 40s: P22, P27 50s: P19	20s: P2, P7, P14, P15, P20, P24 30s: P8, P11, P12, P18, P29 40s: P5, P25, P27, P6 50s: P9, P10, P28 60+: P30	30s: P4 40s: P17, P26 50s: P13, P32, P33 60+: P16, P21, P31
Gender	M: P1, P3, P19, P27F: P22, P23	M: P7, P8, P11, P12, P14, P30, P6 F: P2, P5, P9, P10, P15, P18, P20, P24, P25, P28, P29	M: P4, P13, P17, P21, P33 F: P16, P26, P31, P32
Education	HS: P3 Undergrad: P1 Bachelor: P19, P22, P23, P27	Bachelor: P9, P10, P11, P12, P14, P15, P18, P20, P24, P28, P29, P6 Master+: P5, P7, P8, P30	HS: P4, P16, P17, P32, P33 Bachelor: P13, P26, P31
IT Experience	Yes:– No: P1, P3, P19, P22, P23, P27	Yes: P8, P11, P18 No: P12, P25, P9, P7, P2, P5, P14, P10, P15, P20, P24, P28, P29, P30, P6	Yes:– No: P13, P4, P16, P21, P26, P31, P33, P32, P17
Carrier	SKT: P1, P22, P23 KT: P19 LG U+: P27	SKT: P2, P5, P7, P12, P18, P25, P6 KT: P8, P14, P15, P20, P24 LG U+: P9, P10, P11, P28, P29	SKT: P13, P21, P26, P31, P32, P33 KT: P17 LG U+: P4, P16

Table 5: Mental model levels for the authentication scenario by demographic factors.

Demographic Factor	High (n=6)	Mid (n=16)	Low (n=11)
Age Group	20s: P1, P14, P24 30s: P7, P29 40s: P22	20s: P2, P3, P15, P20 30s: P5, P8, P11, P12, P18, P23, P27 40s: P25, P30 50s: P9, P13, P28, P19	20s: P4 30s: P18, P26 40s: P17 50s: P10, P32, P33 60+: P16, P21, P31
Gender	M: P1, P7, P14 F: P22, P24, P29	M: P3, P5, P6, P8, P11, P12, P19, P27, P30 F: P2, P9, P13, P15, P18, P20, P23, P25, P28	M: P4, P17, P21, P33 F: P10, P16, P18, P20, P26, P31, P32
Education Level	Bachelor: P1, P7, P14, P22, P24, P29	HS: P3 Bachelor: P6, P9, P13, P19, P23, P25, P28, P5, P12, P27, P30 Master/PhD: P8, P11, P18	HS: P4, P16, P17, P32, P33 Bachelor: P10, P13, P18, P20, P31
IT Experience	Yes: – No: P1, P29, P7, P22, P24, P14	Yes: P8, P11 No: P3, P5, P6, P12, P23, P25, P2, P15, P19, P27, P30, P9, P13, P28	Yes: P18 No: P4, P10, P16, P17, P20, P21, P26, P31, P32, P33
Carrier	SKT: P1, P22 LG U+: P29 KT: –	SKT: P2, P5, P12, P18, P25, P6 KT: P8, P15, P19, P20 LG U+: P3, P9, P11, P23, P27, P28, P30	SKT: P21, P26, P31, P32, P33 KT: P17, P18, P20 LG U+: P4, P10, P16