From Scam to Safety: Participatory Design of Digital Privacy and Security Tools with International Students from Global South

Sarah Tabassum, Narges Zare, and Cori Faklaris
Department of Software and Information Systems, University of North Carolina at Charlotte, USA
{stabass2, nzare, cfaklari}@charlotte.edu

***Abstract*—In today's digital world, migrants stay connected to family, institutions, and services across borders, but this reliance on digital communication also exposes them to unfamiliar risks when they enter new technological and cultural environments. Educational migrants *(also known as international students)* depend on online platforms to manage admission, housing, work, and everyday life in the United States. Yet this transition often introduces an unfamiliar and fragmented digital ecosystem where they encounter privacy and security threats such as phishing, identity fraud, and cross-channel scams. Existing security tools rarely consider the situated vulnerabilities of newcomers who must interpret these threats without local knowledge or culturally familiar cues. To investigate these challenges, we conducted participatory design sessions with 22 educational migrants from Global South countries studying in the United States. Using inductive open coding within a reflexive thematic analysis framework, we identified seven themes of desired features. Participants proposed a range of support mechanisms, including transparent reporting and verification workflows, scam filtering, migrant-focused scam databases, and university-integrated safety tools Participants also mapped their concepts to high-level AI capabilities, emphasizing detection, identification, and interpretable explanations. Our findings highlight the need for transparent, culturally grounded, and context-aware digital safety supports for newcomers during their early experiences in the U.S. digital ecosystem.**

I. Introduction

Global mobility for higher education has expanded substantially in recent decades, with over 1.2 million international students studying in the United States during the 2024–25 academic year [32], [42]. Students from the Global South now constitute a significant portion of this movement [15], [10], often relocating to pursue academic and professional opportunities. In this paper, we refer to these individuals as *educational migrants*: people who relocate primarily for academic purposes while maintaining ongoing social, cultural, and communicative ties to their home countries [37], [59].

Educational migrants depend extensively on digital infrastructures throughout their transition, using email, messaging apps, social media, institutional portals, and online marketplaces for admissions, housing, banking, healthcare, and everyday coordination [43], [67], [5]. Yet this reliance exposes them to a wide range of security and privacy threats, including phishing, impersonation scams, fraudulent housing listings, identity theft, and data misuse that often unfold across multiple communication channels [20], [24], [70]. These risks are intensified for people in post-migration situation, who may be navigating unfamiliar institutional norms, legal frameworks, and threat landscapes while simultaneously adapting to new sociotechnical practices [53], [44], [27].

Despite growing interest in supporting international students, usable security solutions rarely account for the transitional, culturally mediated, and cross-channel nature of migrants' digital environments. Most existing mechanisms assume stable digital ecosystems, shared threat cues, and familiarity with local communication patterns [62], [66]. That is why, after moving to a new place, educational migrants need to navigate an opaque and fragmented digital environment that is often different than their mental model. Also, at the same time, they need to actively reconstruct the context, trust cues, and verification strategies with limited institutional scaffolding.

In addition, the current political situation in the U.S. has significantly affected students' mental health, increasing anxiety due to fears about travel bans and the potential loss of student status at various institutions [60], [36]. This atmosphere of uncertainty and chaos has created opportunities for scammers to exploit fear and confusion. As reported in several articles, fake immigration agents and I-9 form scams are occurring across the country [61], [63]. As usable privacy and security researchers, we need to talk more about how to protect these students and help them feel safe and secure from these scams and negative situations by promoting proper, trusted channels of communication.

Participatory design (PD) offers a promising approach for surfacing situated privacy and security needs. Prior PD research has generated nuanced design insights for browser warnings [65], interpersonal privacy conflicts [4], online dating risks [17], and AI literacy [16]. However, these studies typically focus on a single platform or device ecosystem. While this can create domain-specific insights, it fails to address how educational migrants navigate *interdependent*, cross-channel digital threats: an ecosystem where email, SMS, phone calls,

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23009
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

social media messaging, and institutional portals frequently intersect. For this population, a spoofed call may reinforce a phishing email purporting to be from a university, or an SMS scam may leverage personal data scraped from public student profiles. As recent research shows, cybercriminals exploit platform-specific affordances such as, Telegram's real-time messaging or dark web marketplaces' reputation systems to distribute fraud at scale across channels [38], [64], [2]. These interlinked threat vectors are especially challenging during early post-migration periods, when people are adapting to unfamiliar digital infrastructures, norms, and institutional communication practices. Yet, their voices and lived experiences remain underrepresented in security design research. A participatory design approach is needed to reveal how this group understands, prioritizes, and responds to cross-platform risks embedded in the migration experience.

This gap motivates our core research question:

- **RQ:** How can participatory design with international students surface context-aware security and privacy features for mitigating cross-channel scams during digital ecosystem transitions?

To address this question, we conducted participatory design sessions with 22 educational migrants from Global South countries studying in the United States. Unlike prior PD work constrained to a specific interface or technology, our study intentionally left the design space open across privacy, security, trust, and digital communication practices. This ecosystem-oriented approach aligns with calls in usable security to incorporate contextual, cultural, and situational factors into threat modeling and security design [59]. It also responds to critiques that security interventions often fail because they overlook real-world complexity and the cognitive demands placed on users navigating unfamiliar systems [65]. We further reflect on the limitations of this open-ended approach in the discussion.

Our work contributes to growing efforts to situate usable security within diverse lived experiences by documenting cross-channel digital risks among educational migrants, examining how migrants themselves conceptualize and design safety tools, and exploring how they envision the role of AI in supporting detection, verification, and decision-making during digital transitions. To our knowledge, this study is one of the first participatory design investigations with educational migrants from the Global South that examines their post-migration digital privacy and security challenges and explores how they envision supportive safety technologies. This paper makes the following contributions:

- Empirical insights into how educational migrants from the Global South experience cross-channel privacy and security threats during their post-migration digital transitions.
- A set of migration-grounded design directions based on participant-created concepts, showing what safety features educational migrants want and how they imagine system and AI support in making safer decisions.
- Higher-level design implications and considerations for migration-responsive, ecosystem-level safety interventions that move beyond platform-specific solutions in usable security.

II. Background and Related Work

A. Educational Migrants from the Global South and Digital Vulnerability

Digital infrastructures across different regions are shaped by diverse regulatory regimes, institutional arrangements, and communication norms [44], [49]. When people move across these differently organized digital ecosystems, they often encounter mismatches in expectations around digital safety, data protection, and institutional communication norms [9]. Despite making up a substantial share of international student mobility, students from the Global South are underrepresented in security and privacy design research [1]. Many participants described prior digital environments organized around different trust cues, authority relationships, and everyday communication practices. Entering a differently regulated setting like the United States can introduce discontinuities in privacy expectations, institutional trust cues, and everyday security practices [37], [62].

This transitional period is particularly demanding, as newcomers have to manage critical administrative tasks such as housing, immigration compliance, or university onboarding through channels like email, SMS, social media, and phone calls [5], [27]. These same channels are commonly exploited for impersonation scams [18]. Yet, this population remains largely absent in security design research. Their perceptions of digital risk, responses to unfamiliar warning cues, and coping strategies during migration remain underexamined [59], [43].

B. Cross-Channel Scams and Multi-Platform Threats

In the field of usable privacy and security, it is increasingly evident that digital fraud campaigns are not only technologically sophisticated but also socially engineered to exploit specific populations. Many attacks like, phishing, smishing, and vishing are deliberately designed to manipulate trust, authority cues, and urgency [34], [58], [45]. These threats often converge across multiple communication channels, creating the illusion of legitimacy through repetition and coordination. For example, a phishing email may be reinforced by a follow-up SMS or spoofed phone call, forming a coherent but fraudulent narrative [21].

These tactics are common in impersonation scams involving universities, immigration offices, delivery services, or financial institutions, sectors that educational migrants regularly interact with during transitional periods [50], [3]. Such targeting is not coincidental: attackers often adapt their strategies to the vulnerabilities and information-seeking behaviors of specific user groups. Yet, most users do not interpret these messages as part of a coordinated effort. Research shows that people often evaluate messages individually, without recognizing patterns across platforms [46], [24]. This fragmentation is amplified in mobile-first environments, where interface constraints reduce

the visibility of risk cues and limit users' ability to verify sender identity or detect anomalies [69], [59].

Recent studies conceptualize these fraud operations as part of a broader digital ecosystem—one in which different platforms serve distinct functions. For instance, Telegram is used for wide dissemination and recruitment, while dark web forums support skill development, trust-building, and service exchange [38], [64]. Broader research on digital and mobile ecosystems also suggests that low-barrier, asynchronous channels are often leveraged in underregulated or transitional contexts, making them ideal for scalable fraud [6], [56], [57], [1].

Despite this growing body of evidence, most consumer-facing security systems treat threats in isolation focusing on email, SMS, or app fraud independently. Few systems are designed to recognize or explain threats that move across platforms, or that target users undergoing cultural, linguistic, or situational shifts. This limits both detection and user awareness, especially among groups like educational migrants who must make trust decisions under uncertainty, pressure, and unfamiliar digital norms.

C. Usable Security and the Role of Participatory Design

Research in usable security consistently shows that people interpret security warnings in context—that is, their effectiveness depends on users' cognitive load, emotional state, prior experience, and familiarity with the system [14], [52], [69]. When users are stressed, multitasking, or unfamiliar with a digital interface, they are more likely to misread, dismiss, or ignore warnings [24], [46]. Risk cues are most effective when they align with user expectations and situational awareness [22], [29].

However, many security signals are poorly adapted across cultural and linguistic contexts. Standardized warnings often reflect assumptions rooted in dominant digital norms, leading to misinterpretation or misplaced trust among users unfamiliar with local threat models or communication styles [70], [67], [29]. These gaps are amplified when threat cues differ across platforms leaving users unsure which signals are meaningful or trustworthy. Recent advances in AI-assisted security systems, such as phishing detection and anomaly flagging, emphasize technical accuracy but rarely consider how users interpret or act on automated outputs. These tools often lack contextual explanations, making them difficult to use especially for individuals navigating unfamiliar or transitional digital environments [46], [11], [25], [62]. Few systems support users in recognizing cross-channel attacks, and even fewer address the needs of populations adjusting to new privacy and security expectations, such as educational migrants [59], [37].

Participatory design (PD) offers a valuable methodology for addressing these gaps by foregrounding users' lived experiences and culturally situated reasoning [8], [28]. Prior PD work in security and privacy has surfaced design insights around browser warnings, AI literacy, and interpersonal privacy management by centering user knowledge and social context [65], [4], [16], [17], [47]. These studies show that users often identify risks and design needs that system-centric approaches overlook.

However, most PD studies focus on single platforms or stable user contexts, limiting their relevance for populations dealing with fragmented or evolving digital environments. To date, to the best of our knowledge, no PD research has explored how educational migrants conceptualize cross-channel security threats or AI-augmented tools during digital transition. This gap leaves open questions about how participatory methods might support the design of more context-aware, migration-responsive security systems.

III. Methodology

To explore educational migrants' experiences and design preferences regarding digital safety tools in the post-migration context, we conducted a series of participatory design (PD) sessions. Our methodological approach is grounded in PD practices in usable security and privacy research, emphasizing the collaborative creation of design artifacts with affected communities, accessible artifact creation, and qualitative synthesis through thematic and artifact-centered analysis [4], [31], [48].

The participatory design sessions were conducted both in person and virtually via Zoom. Local participants were invited to attend in-person sessions, while individuals outside the area were given the option to join remotely. These sessions were held during August and September 2025. The study received approval from the university's Institutional Review Board (IRB), and informed consent was obtained from all participants prior to participation. Participants received a $20 Amazon e-gift card as compensation for taking part in the design session.

This section provides an overview of our recruitment process, participant demographics, details of the PD sessions, and the data analysis methods employed in this study.

A. Recruitment

We conducted participatory design sessions with 22 international students, all of whom were educational migrants from countries commonly categorized within the Global South [19]. The participant group included 12 females and 10 males. Recruitment was carried out through multiple channels, including flyers and social media advertisements posted on Facebook, WhatsApp and LinkedIn. We additionally employed snowball sampling [7], encouraging participants to refer others within their networks. Recruitment materials specifically targeted international students studying in the U.S. who had migrated for educational purposes from Global South regions. To verify eligibility, the advertisements included a brief screening survey; only respondents who met the study criteria were invited to participate. Demographic information was collected, and informed consent was obtained prior to scheduling the participatory design sessions. Eligible participants were contacted via email to coordinate session times and confirm whether they preferred an in-person or virtual format.

B. Participants

We recruited 22 educational migrants from the Global South, all aged 18 or older (Table I). All participants identified as first-generation migrants, meaning they were the first members of their families to migrate to the United States for educational purposes. Our participants represented 15 different universities across the U.S., including public institutions, private universities, and community colleges. The sample included 12 females (54.5%) and 10 males (45.5%), distributed across three age groups: 8 participants aged 18–24, 13 aged 25–34, and 1 aged 35–44.

Participants came from diverse academic disciplines. Eleven participants had background in Computer Science or Information Technology, while four of them studied Social Sciences, three participants from Engineering, two from Business or Management. We also had one participant from Natural Sciences, and one from Humanities. This disciplinary diversity allowed us to capture digital security perspectives shaped by varying levels of technical exposure rather than assuming uniform security expertise among international students.

TABLE I
PARTICIPANT DEMOGRAPHICS: THE TABLE PROVIDES A DETAILED OVERVIEW OF PARTICIPANTS' AGE GROUP, GENDER, COUNTRY OF ORIGIN, DURATION OF STAY IN THE USA

ID	Age	Gender	Origin Country	Duration in the U.S.
P1	25–34	Male	Bangladesh	1–3 years
P2	25–34	Female	Pakistan	1–3 years
P3	18–24	Male	Tanzania	1–3 years
P4	25–34	Female	Rwanda	1–3 years
P5	18–24	Male	India	6 mo.–1 yr
P6	25–34	Female	Ghana	<6 months
P7	25–34	Female	India	>3 years
P8	18–24	Male	Algeria	1–3 years
P9	25–34	Female	Ghana	1–3 years
P10	18–24	Male	South Africa	1–3 years
P11	18–24	Female	Angola	1–3 years
P12	25–34	Female	China	>3 years
P13	25–34	Male	Uganda	1–3 years
P14	25–34	Male	China	1–3 years
P15	18–24	Male	India	6 mo.–1 yr
P16	25–34	Female	Bangladesh	> 3 years
P17	35–44	Female	Pakistan	1–3 years
P18	18–24	Female	India	6 mo.–1 yr
P19	25–34	Male	Uganda	1–3 years
P20	18–24	Male	Uganda	1–3 years
P21	25–34	Female	Bangladesh	1–3 years
P22	25–34	Female	Nigeria	>3 years

Regarding educational background, 10 participants (45.5%) had completed a Master's degree, 9 (40.9%) held a Bachelor's degree, 2 (9.1%) had earned a Doctoral degree, and 1 participant (4.5%) had completed a higher secondary (HS) qualification and was currently enrolled as an undergraduate student in the U.S. Participants represented 12 countries. The distribution included 4 from India (18.18%), 3 from Bangladesh (13.64%), 3 from Uganda (13.64%), and 2 each (9.1%) from Pakistan, China, and Ghana. Additionally, one participant each (4.5%) came from Algeria, Angola, Nigeria, Tanzania, Rwanda, and South Africa.

Fig. 1. Scenario primer storyboard used to establish common ground during participatory design sessions, showing a newcomer's early digital experiences and a phishing scam encounter

Participants' durations of stay in the U.S. ranged from less than six months to over three years, allowing us to explore whether privacy-related needs shift with time, as noted in prior research [12], [26]. In our sample, 4 participants (18.18%) had lived in the U.S. for more than 3 years, 14 (63.6%) for 1 to 3 years, 3 (13.6%) for 6 months to 1 year, and 1 participant for less than 6 months.

C. Participatory Design Sessions

We used participatory design rather than interviews because the study aimed not only to understand participants' experiences, but also to collaboratively envision and critique design solutions with them instead of designing on their behalf [31], [48], [4]. We conducted nine small-group participatory design (PD) sessions with two to four participants per session, each lasting about 83 minutes on average. Sessions were held either in person or via Zoom. Small-group formats are commonly used in PD because they support inclusive discussion and allow deeper exploration of concepts [4], [31]. All sessions were facilitated by the first author, who adopted a collaborative stance to help minimize power asymmetries in line with PD principles [48].

In-person sessions used low-barrier materials such as sticky notes, markers, pencils, blank paper, and design templates featuring mobile, tablet, and desktop screen outlines. Remote sessions were conducted on Miro, and participants were free to sketch on paper and upload images of their work. Providing flexible, easy-to-use materials is recommended in PD to support different drawing preferences and expression styles [4], [17].

Each session followed a structured sequence. Participants first received an overview of the study and provided verbal consent. They were then introduced to a storyboard featuring a Tanzanian student's arrival in the United States and her encounter with a scholarship phishing scam (Fig. 1).

Scenario primers help establish common ground while still preserving open design possibilities [4], [48]. We used a single scenario as a generative grounding prompt rather than as a comprehensive threat model, to evoke participants' own memories of early post-migration digital uncertainty. Participants were told the scenario was only an example and were encouraged to adapt, critique, or move beyond it to reflect any privacy or security concern they had experienced across

platforms. Participants were invited to relate the scenario to their own experiences across any platforms.

Next, participants shared privacy and security challenges they had faced post-migration, followed by a design ideation phase in which they sketched potential tools or features on paper or digital canvases. Consistent with inclusive PD practice, participants could choose their preferred sketching medium [4], [16]. After ideation, participants presented their concepts and engaged in peer feedback discussions focused on usability, cultural fit, and perceived value, a common PD mechanism for refining emerging design ideas [16], [17], [4].

Finally, participants were invited to map their concepts onto eight predefined AI capability roles (detect, estimate, act, forecast, identify, generate, compare, discover), which we used as an abstract scaffold to help articulate and compare desired system behaviors [4], [16], [17]. This step was inspired by prior work showing that people often describe intelligent systems in overly broad or unrealistic terms when discussing future technologies [68]. By introducing these capability roles, we aimed to support more concrete and grounded discussion of what kinds of system functions participants were envisioning, without assuming or requiring that their designs must use AI. Participants were explicitly told that this activity was optional and that AI-based solutions were neither required nor assumed. Sessions concluded with brief reflections and final comments.

We collected three forms of data: (1) audio recordings of the PD sessions; (2) participant-created artifacts, including sketches, Miro board outputs, and sticky-note contributions; and (3) researcher field notes and memos taken during and immediately after each session. All data were de-identified after collection.

While the core protocol remained consistent across sessions, in-person sessions used physical materials, whereas remote sessions primarily relied mainly on shared Miro boards. However, some remote participants *(P7, P11, P19, and P21)* preferred to sketch on paper and share photos of their drawings instead, and this was fully supported to maintain low barriers to participation and accommodate individual comfort with different tools.

D. Data Analysis

We employed a qualitative analysis strategy grounded in inductive open coding within a reflexive thematic analysis framework [13]. All audio recordings were manually transcribed, and transcripts, participant-created artifacts, and field notes were treated as a unified dataset. Through iterative, inductive cycles of open coding [35], we identified salient experiences, concerns, and design rationales across participants' accounts. Codes captured concepts such as experiences with digital threats, scams across multiple channels, culturally shaped interpretations of risk, decision-making cues, and expectations for safety and support.

To analyze participant-generated design ideas, we conducted lightweight affinity clustering of sketches, and sticky-note comments. Similar design concepts were grouped to reveal recurrent patterns in participants' proposed features and to support the emergence of early design groupings, consistent with affinity diagramming practices in PD [30]. These clusters were examined alongside transcript-based codes to ensure alignment between expressed experiences and proposed design solutions.

Throughout analysis, the research team met periodically for peer debriefing, discussing emerging interpretations and refining analytic focus. Through these iterative conversations, initial codes and artifact clusters were developed into higher-level themes characterizing how educational migrants navigate unfamiliar digital environments and express their needs for clear, culturally grounded, and context-aware safety support. Finally, we integrated insights across transcripts, artifacts, and affinity clusters to generate design implications showing how future systems might assist educational migrants across email, SMS, phone calls, and institutional communication platforms. The first and second authors led the coding process, meeting regularly to discuss code definitions and resolve disagreements through consensus. Additional team discussions supported reflexive interpretation rather than inter-rater reliability metrics [39].

E. Ethical Considerations

Because this study involved discussing scams, digital risk, and post-migration experiences in a small-group setting, we designed the protocol to minimize potential discomfort and privacy risks. Participants were informed in advance about the study activities, recording practices, and their right to skip any question without penalty or stop participation at any time. They were not asked to share sensitive personal information such as visa details, financial credentials, or legal documentation. To reduce privacy risks, no video was recorded, no third-party or automated transcription services were used, and Zoom AI features were disabled; audio recordings were manually transcribed by the research team and de-identified prior to analysis. Participants were reminded that group discussions cannot guarantee complete confidentiality, and an anonymous feedback form was provided after each session for anything they preferred not to share in the group. Recordings were deleted after transcription and verification, and all study data were stored on access-controlled, university-managed systems. Beyond procedural protections, we also attended to ethical considerations in how this study was designed and how participants' experiences are represented. We used participatory design to treat participants as co-designers rather than as subjects being evaluated. We focus our analysis on contextual and structural factors shaping digital risk instead of on individual users.

F. Researcher Positionality

This work's lens has been shaped by the researchers' identities and lived experiences. The first author migrated to the United States for education. Moreover, both the first and second authors have remained actively engaged with international student communities *(i.e., university organizations for international students from Bangladesh, Iran, India, Pakistan)*.

Through these experiences, the authors have observed how newly arrived students often rely on peer networks to navigate unfamiliar digital environments and institutional systems. In particular, the first author has observed that seeking advice about scams, institutional communication, and online safety practices is often an unanticipated challenge for newcomers, especially when expectations about scam categories, legitimacy cues, and trusted communication channels differ from those in their prior contexts. Developing an accurate mental model of local scam patterns and institutional processes takes time, and during this early period of transition, uncertainty about whom to trust or where to seek guidance can increase exposure to targeted scams. At the same time, all authors are affiliated with a U.S. academic institution; while the authors recognize the important role that international student offices play in supporting students, the first author has also observed that many newly arrived students are often unsure whether such offices are the appropriate or safe place to seek advice about digital security concerns, contributing to confusion about where to turn for trusted guidance. To mitigate potential power asymmetries, sessions were facilitated using participatory design principles that positioned participants as co-designers rather than research subjects, and participants were explicitly encouraged to critique existing technologies, institutions, and proposed design ideas.

IV. Results

This section presents our findings, organized into three parts. First, we describe the digital privacy and security challenges that educational migrants encountered after arriving in the United States. Next, we outline the design ideas and proposed features generated by participants during the participatory design sessions. Finally, we describe how participants explored and incorporated AI capabilities into their envisioned tools for supporting newcomers' digital safety.

A. Digital Privacy and Security Challenges Encountered After Migration

Across sessions, participants described encountering a range of unfamiliar privacy and security risks shortly after arriving in the United States. These challenges occurred across communication channels such as phone calls, SMS, email, social platforms, and housing or job-related interactions. Participants noted that the volume and nature of threats differed substantially from what they experienced in their home countries, contributing to confusion, stress, and difficulty recognizing legitimate communications. The following themes summarize challenges that emerged from the data.

1) Cross-channel scams and impersonation: All of our participants described receiving fraudulent calls, emails, or messages after moving to the United States, often impersonating government agencies or service providers. For example, P17 explained: *"I have been receiving non-stop calls from IRS… the revenue department. And like they are not from them, because the codes … I don't know what countries plus six two. So they are not even from America, but I'm receiving them non-stop every day."*

Another participant (P15) encountered a threatening impersonation attempt, stating: *"I received a call… pretending to be a Homeland Security officer and asking for my personal information."*

These incidents created stress and uncertainty, particularly because newcomers lacked familiarity with U.S. institutional communication norms and struggled to determine whether such communications were legitimate.

2) Housing and job-related information requests: Eleven participants reported confusion regarding what information is appropriate to share with housing companies or employers, especially when asked for sensitive identifiers. For instance, P4 described: *"One [housing company] was asking for the SSN number, and I was confused, should I share or not?... It's very personal."*

Six of them specifically mentioned about uncertainty in job-related interactions. As P6 explained: *"I'm looking for internship for next summer. So I just shared all those details when I'm applying for a job on some website, but they, uh, I don't know if they're fake or real. And so, yeah, the number of scam calls have been increased since I started job searching."*

These examples illustrate how unfamiliarity with U.S. housing and employment processes creates hesitation and potential vulnerability for newcomers navigating early-stage digital interactions.

3) Financial fraud and unauthorized transactions: Several participants (8) described experiences with financial fraud and unauthorized activity on their accounts. P2 recounted: *"Someone was taking out my money… the scammer started with a very small amount… then increased the amount slowly."*

The same participant expressed shock upon learning the origin of the attacker: *"The scammer… was from the Middle East. I was shocked how the person… came to know about my credit card number."*

These incidents created both financial and emotional strain during an already stressful transition period.

4) Social media and identity-related concerns: Five participants expressed concern about how easily personal information could be gleaned or misused through social media. For example, P1 stated: *"It's really easy to get scammed or get our privacy leaked… there are social media [where] you can get birthdate or location… it's really easy."* Two participants described experiencing or nearly encountering marketplace fraud. P16 recounted a laptop scam attempt on Facebook Marketplace: *"The owner… kept asking them for money in advance… she insisted that they do it today itself… This sense of urgency then triggered something… I realized that it's a scam."*

These concerns highlight the challenges newcomers face while managing multiple unfamiliar platforms and attempting to maintain personal security online.

5) General confusion about U.S. digital and institutional expectations: Three participants described uncertainty about determining which communications, requests, and digital in-

teractions were legitimate. As P1 explained: *"This is kind of confusion happening to me every day in USA... we have some kind of indecision like this in most of the cases."*

Taken together, these challenges reflect not a lack of care or effort by participants, but the difficulty of navigating unfamiliar institutions, communication norms, and cross-channel digital environments during a period of transition. In the next section, we show how participants' design ideas directly respond to these situational challenges and reframe them into concrete forms of support.

B. Designs and Ideas Proposed by Participants

When we asked participants to imagine tools or features that could help address the challenges described above, they proposed a variety of design ideas grounded in their lived post-migration experiences. These ideas reflected what they wished they had during their early transition and what they believed would support other newcomers facing similar challenges.

Our analysis produced seven thematic categories that represent how international students envisioned digital safety support during their adaptation to the U.S. digital ecosystem. These themes reflect cross-channel vulnerabilities (email, SMS, phone), gaps in contextual understanding, and a desire for both institutionally grounded and personalized assistance. Below, we present each theme along with illustrative participant insights.

1) Theme 1: Reporting, Verification, and Investigative Feedback: In response to their frustration with opaque reporting processes and uncertainty about what is legitimate, six participants expressed strong interest in tools that allow them to *report*, *verify*, and *track* suspicious activities. Many described frustration with existing reporting systems that feel opaque or unresponsive. Participants wanted features that not only submit a report but also communicate status updates and outcomes.

For example, P1 proposed an app that would allow users to "report a scam and actually see what happens after," while P4 described a tool that could "copy–paste conversations or links and tell me if this is real, and what I should do next." Several participants emphasized the emotional reassurance provided by feedback loops. As P21 put it, *"If I report something, I want to know someone looked at it. Otherwise I feel ignored."* Figure 2 shows example design concepts created by P1 and P9.

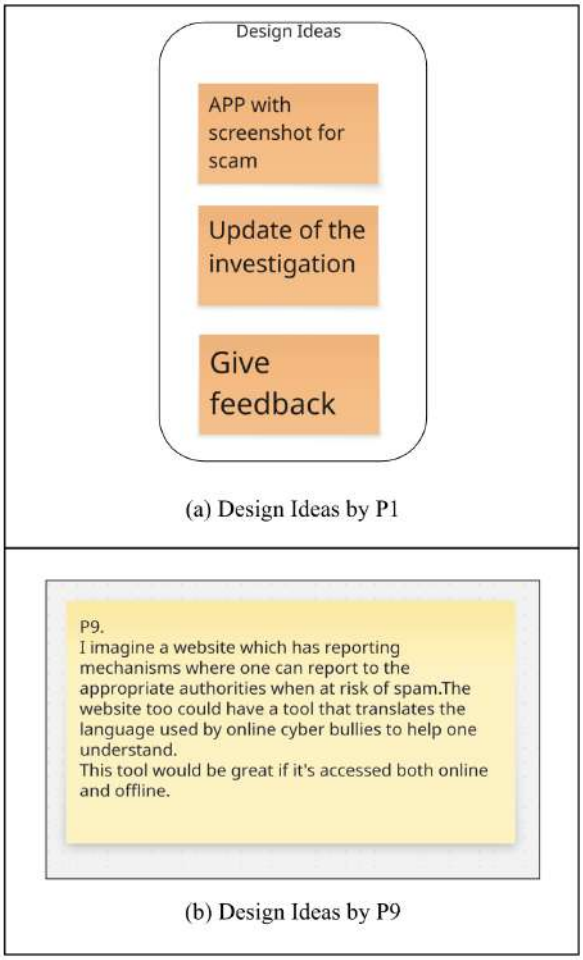


Fig. 2. Participant-generated design concepts for reporting, verification, and investigative feedback

These ideas show a desire for transparent, accountable reporting channels that offer verification, follow-up, and clear next steps.

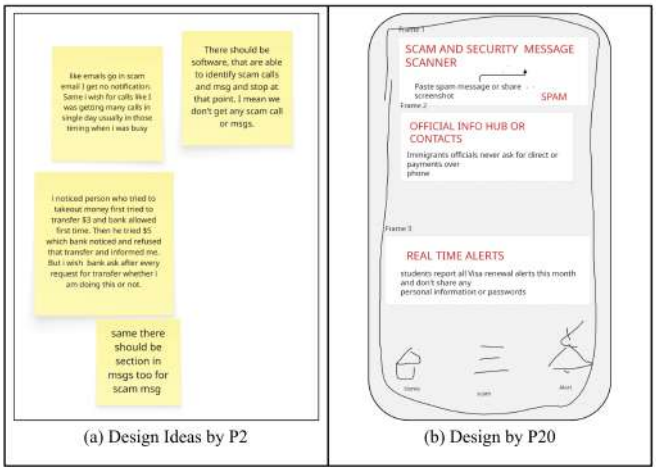
2) Theme 2: Cross-Channel Scam Filtering for SMS and Phone Calls: Because of the volume of scam calls described earlier, a second cluster of design ideas proposed by five participants focused on **SMS and call filtering** to address the high volume of phone-based scams targeting newcomers. Participants described receiving frequent fraudulent messages or calls impersonating banks, government agencies, or employers.

P2 noted, *"I get scam calls every day. I wish my phone could just filter them like email spam."* Others envisioned clearer visual cues or explanations. P6 proposed a tool that would *"highlight messages in red or green based on danger so you don't panic."* As shown in Figure 4, P14 also emphasized that filters should *"explain why it is suspicious, not just block it."* Figure 3 shows example design concepts created by P2 and P20.

These suggestions underline the need for intelligent, explainable mobile-based protection that helps users avoid social engineering tactics over SMS and phone calls.

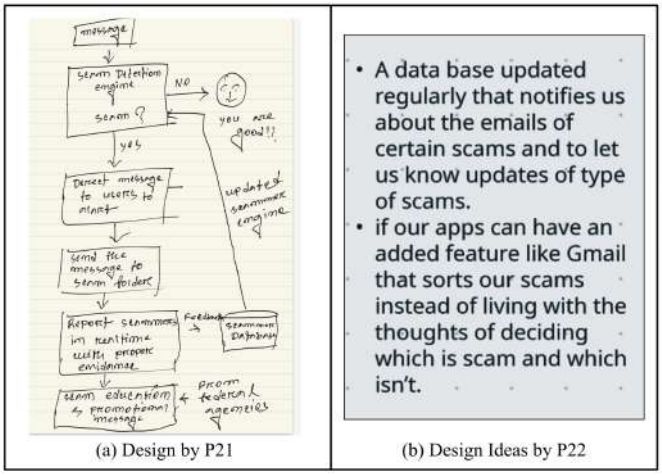
3) Theme 3: Migrant-Focused Scam Databases and Trend Tracking: Four participants expressed interest in a **centralized, migrant-aware scam database** that could help newcomers identify and understand emerging threats in the United States. They envisioned a resource where users could browse real scam examples, observe trends, and learn from the experiences of other migrants.

P4 described an online platform where *"people share their scam stories anonymously so others can avoid them."* Similarly, P22 proposed a service that *"updates you regularly about the latest scams happening in your area or targeting*



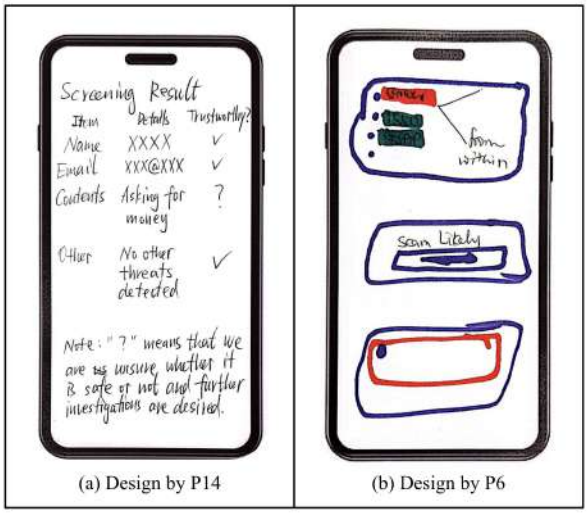
(a) Design Ideas by P2 (b) Design by P20

Fig. 3. Designs by P2 and P20 highlighting participants' desire for tools that scan suspicious SMS messages and phone calls



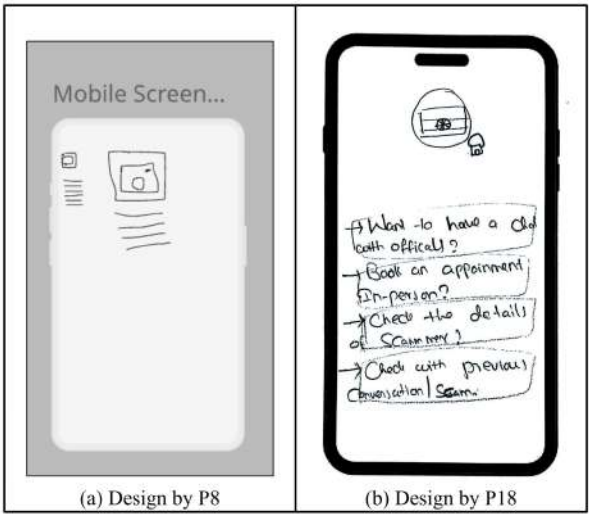
(a) Design by P21 (b) Design Ideas by P22

Fig. 5. Design concepts by P21 and P22 showing ideas for a migrant-focused scam database



(a) Design by P14 (b) Design by P6

Fig. 4. Detailed design ideas from P14 and P6 on the expected behavior of scam-filtering tools



(a) Design by P8 (b) Design by P18

Fig. 6. Design concepts by P8 and P18 with tools for guidance and verifying actions

international students." As shown in Figure 5, P21 emphasized the importance of collective knowledge, explaining that *"when newcomers land here, they don't know the types of scams. A shared database would help us quickly learn what to avoid."*

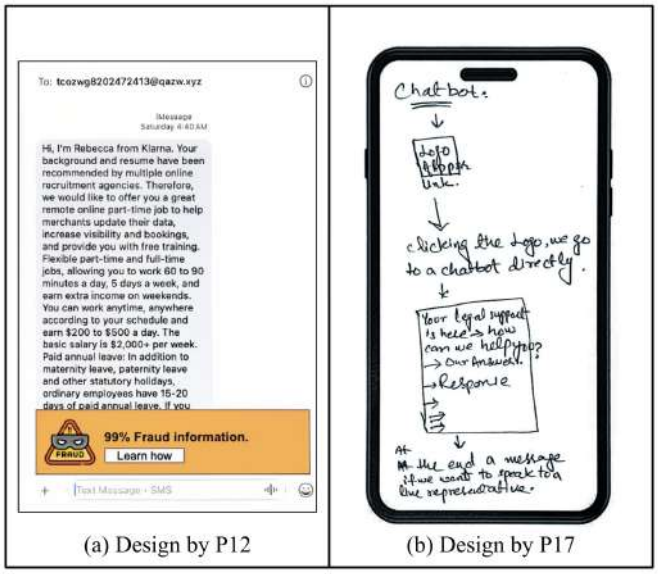
This theme highlights a desire for collective knowledge infrastructures that support rapid adaptation to local threat ecologies.

4) Theme 4: Guidance and Decision Support (Cues, Explanations, and What-Not-to-Share): Because participants described uncertainty about norms and expectations, eight participants proposed tools that offer ongoing guidance about what information to share online, how to interpret suspicious content, and how to make safe decisions during everyday digital interactions. These ideas emphasized lightweight support features that surface warning cues, explain red flags, and provide situational advice when users feel uncertain.

As shown in Figure 6(a), P8 envisioned a feature that provides *"tips on what not to post online because sometimes you don't know what is sensitive here."* Similarly, P12 proposed a warning system that *"summarizes the cues and tells me, here is why this message is risky."* P11 described a "smart scam detector" designed to *"tell you the warning signs before you click."*

P18 extended this idea by designing a feature that connects users with trusted resources or officials before taking action, as illustrated in Figure 6(b). Participants described such tools as especially helpful during moments of uncertainty or stress. As P17 noted, *"When you are new, you don't know the culture. Even small guidance helps a lot."*

5) Theme 5: Risk Assessment and Just-in-Time Support: Four participants expressed the need for tools that assess the risk of messages or interactions *in the moment*, offering timely warnings or nudges when users are rushed, tired, or emotionally overwhelmed. These ideas emphasized support



(a) Design by P12 (b) Design by P17

Fig. 7. Design concepts for risk assessment and just-in-time guidance

during moments when newcomers felt most vulnerable to making mistakes.

As shown in Figure 7(a), P12 shared an example of a fraudulent SMS from their phone and sketched a design illustrating how a risk assessment feature could flag suspicious content. P7 proposed a broader feature that performs *"risk assessment and orientation training so students know what to expect after arrival."*

P17 emphasized the importance of just-in-time interventions, envisioning a chatbot-based warning system (Figure 7(b)): *"Sometimes I'm sleepy or busy, and that's when I make mistakes. The system should warn me before I act."*

These ideas highlight the situational and temporal context of scam vulnerability, suggesting that digital safety tools must adapt to cognitive load and stress.

6) Theme 6: Protective Technical Capabilities: As participants wanted stronger ways to verify authenticity, they proposed a set of technical protections that support privacy and safety at a deeper infrastructural level. Their ideas focused on mechanisms that help newcomers **verify authenticity**, **interpret unfamiliar communications**, and **guard against hidden risks**.

P15 envisioned **encryption and stronger authentication features**, including a verification key that would allow users to confirm the identity of anyone contacting them. P9 emphasized the need for **automatic translation** and **warning systems** for messages written in unfamiliar or hostile languages, explaining that *"If someone sends you a scam in another language, you can't even understand the threat. It needs to translate and warn you."* Similarly, P15 argued for more robust identity verification, stating that *"There should be a universal key or authentication so you know who is contacting you."*

These ideas highlight participants' interest in cryptographic, linguistic, and verification-oriented capabilities that can help

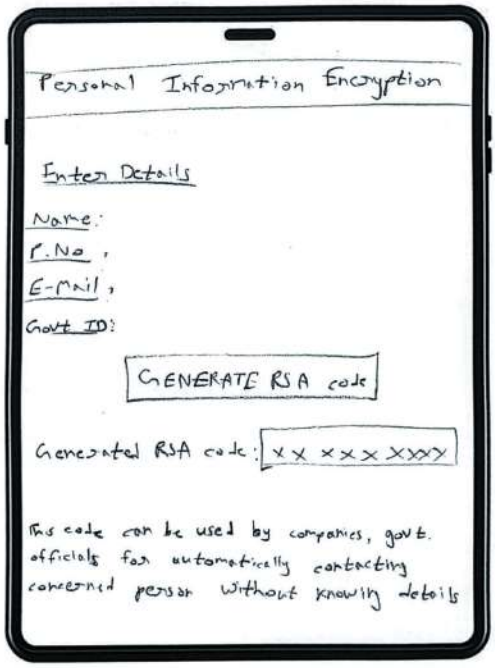


Fig. 8. Design by P15 showing proposed authentication and verification features

newcomers navigate unfamiliar digital ecosystems with greater confidence.

7) Theme 7: University-Integrated Digital Safety Support: Two participants proposed integrating digital safety functionality directly into university systems, reflecting their view that institutions serve as trusted anchors during the early stages of migration. P13 sketched a chatbot integrated into the university website (Figure 9) that would allow students to ask questions such as *"is this email real?"* P13 also suggested adding a dedicated portal section where newcomers could *"learn what to expect after moving here, like common scams or what not to share with housing companies."*

Participants described universities as uniquely positioned because *"students trust school websites more than random apps"* (P16). This theme highlights institutional integration as a critical pathway for supporting newcomers during their most vulnerable moments.

Taken together, these themes show that participants do not think of security as a single feature or platform-level fix. Instead, they envision a migration-responsive safety ecosystem that combines orientation, cross-channel sensemaking, institutional anchoring, and just-in-time support across moments of uncertainty.

C. Exploring AI Roles in Participants' Design Concepts

After articulating concrete design ideas, the AI capability activity served as a reflective step to help participants describe and reason about what kinds of system behaviors their concepts implied. The participants were introduced to

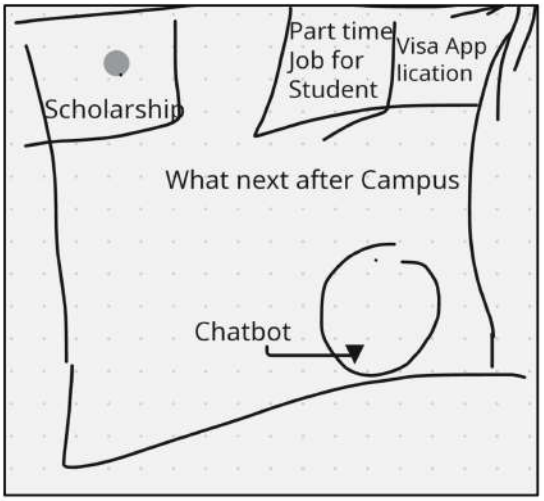


Fig. 9. Design concept by P13 with university-integrated safety support

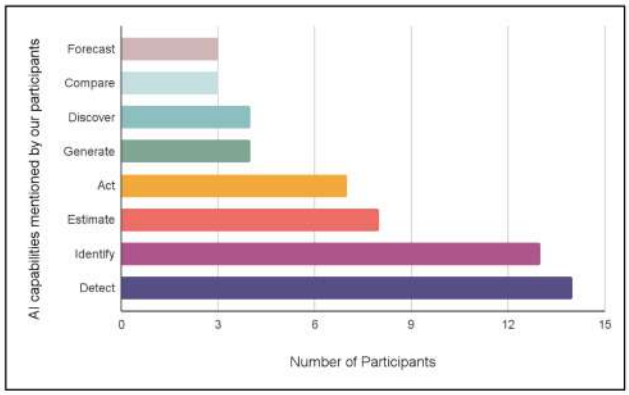


Fig. 10. Frequency of AI capabilities selected by participants

eight high-level AI capabilities drawn from Yildirim et al. [68]: *detect, identify, act, estimate, generate, discover, compare,* and *forecast*. As described in our PD protocol, these capabilities were used as an abstract, optional scaffold to support discussion, not as a requirement that participants design AI-based systems. They were selected because they represent broad, conceptual "roles" that AI systems can play in supporting user tasks, without requiring technical expertise or knowledge of specific algorithms. This activity was included to help participants reflect on how such capabilities might complement, extend, or constrain the tools they had already envisioned. The goal was not to assess feasibility, but to understand how newcomers imagine responsible and useful system support within unfamiliar digital ecosystems.

Overall, participants linked their design ideas to multiple AI roles. The most frequently selected capabilities were **detect** (14 participants) and **identify** (13 participants), reflecting a strong desire for systems that surface suspicious patterns, highlight red flags, and reduce cognitive burden. Participants also associated their concepts with *estimate* (8), *act* (7), *generate* (4), *discover* (4), *compare* (3), and *forecast* (3), demonstrating nuanced expectations for how AI could support judgment and contextualize digital risks. Figure 10 visualizes the frequency of each capability selected by participants.

Participants emphasized that these capabilities must be transparent and supportive rather than autonomous. P6 noted that AI could "*detect and warn me, but I still want the final say with some suggestions*," while P11 explained that estimation tools should "*explain why something looks risky so you can learn for next time*." Others highlighted scenario-specific uses, such as P17's suggestion that AI could "*discover patterns in migrant-targeted scams and generate examples to help new students understand how they happen*" and P20's idea that AI might "*predict which scams are trending right now and flag similar ones for students*."

Across sessions, participants framed AI *not as a replacement for human judgment*, but as a contextual layer of support that can surface cues, evaluate risks, translate unfamiliar content, connect reports to resources, and highlight emerging scam patterns. These views align with their broader emphasis on *transparency*, *cultural grounding*, and *human-in-the-loop decision-making*.

V. Discussion

We synthesize our findings to derive design implications for migration-responsive, ecosystem-level security and privacy support that move beyond platform-specific interventions.

A. Context-Aware Security and Privacy for Educational Migrants from the Global South

Our findings demonstrate that educational migrants from the Global South navigate digital risk under conditions that differ markedly from populations typically examined in usable security research. Prior work shows that newcomers need to navigate unfamiliar digital norms, shifting privacy expectations, and unfamiliar institutional communication patterns when entering a new country [41], [59], [37]. Participants in our study similarly struggled to interpret legitimacy across email, SMS, phone calls, and messaging apps, especially when messages appeared urgent, authoritative, or procedurally unfamiliar. Several participants described how situational pressures such as housing deadlines, visa requirements, and academic onboarding increased cognitive load, which in some cases made plausible but deceptive messages harder to evaluate [14].

In addition to these *migration* and *situational* factors, participants' cultural and political backgrounds shaped how they evaluated authority, formality, and trust. As shown in cross-cultural usable security research, individuals rely on culturally informed mental models when judging legitimacy [29], which can conflict with host-country communication styles or warning conventions. Participants also carried expectations from their home countries about how institutions communicate, what counts as an "official" channel, or how quickly authorities respond. Scammers leveraged these expectations

through impersonation and cross-channel reinforcement [23], [50].

Taken together, these findings point to the need for context-aware, culturally grounded security and privacy approaches that respond to migration stage, situational pressure, and the cross-channel nature of newcomers' digital ecosystems. Rather than assuming users who are already familiar with local digital norms, context-aware systems should help migrants connect signals across channels, interpret unfamiliar institutional communication patterns, and make sense of ambiguous cues during a period of sociotechnical transition. Such grounding is essential for designing security interventions that align with educational migrants' lived experiences and support safer navigation of complex digital environments.

B. Design Needs and Migration-Responsive Features Across the Scam Ecosystem

Our findings reveal that educational migrants require security support that spans the full scam ecosystem rather than isolated channels or platforms. Participants routinely encountered scams that moved fluidly between email, SMS, phone calls, and messaging apps, mirroring broader evidence that contemporary fraud operates as a coordinated, multi-channel process [64], [51]. Because newcomers often interpreted each message independently, they expressed the need for features that help them recognize connections across communications. Examples included alerts that identify repeated sender patterns, conflicting information, or unexpected switches from one channel to another.

Participants also described the challenges of interpreting institutional communication during moments of high cognitive load, such as housing searches, visa appointments, or university onboarding. Prior work shows that stress and divided attention significantly reduce users' ability to notice or act on security cues [14], [24]. To address these constraints, participants envisioned designs that provide clear, concise, and actionable guidance, including migration-specific orientation tools, examples of legitimate institutional communication, and step-by-step verification workflows (Fig.11). These ideas align with calls for ecosystem-level safety interventions that move beyond platform-specific alerts [22].

Beyond detection, participants emphasized the importance of low-effort reporting and help-seeking features tailored to newcomers' unfamiliarity with local institutions. They sought ways to quickly flag suspicious messages, compare communications across channels, and request assistance without fear of making mistakes. These participant-generated concepts highlight the need for migration-responsive design approaches that integrate orientation, detection, reporting, and verification within a unified, cross-channel safety experience. Participants wanted university-integrated portals that combined verification tools, scam education, and advisories customized for the newcomers.

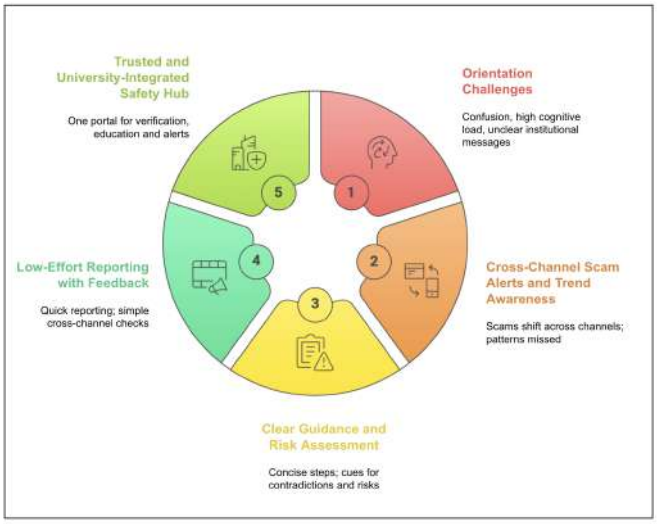


Fig. 11. Orientation challenges experienced by educational migrants (Point 1) and the four migrant-centered security features they identified as necessary for safer digital navigation (Points 2–5). Together, these elements illustrate how post-migration difficulties shape participants' visions for supportive, context-aware privacy and security tools.

C. AI-Assisted Security: Opportunities, Capabilities, and Human-in-the-Loop Cautions

Because we used AI capability roles as a reflective scaffold during the participatory design sessions, rather than as a requirement to design AI systems, participants' discussions of AI reveal how they imagine automated assistance fitting (or not fitting) into their existing sensemaking and verification practices. In our study, participants associated their design ideas with multiple AI roles such as, detection, translation, guidance, and pattern discovery but emphasized clear boundaries around autonomy, transparency, and user control. They viewed AI as a potentially valuable resource for detecting inconsistencies across messages and supporting them as they navigate unfamiliar host-country communication norms. Their ideas echo emerging work on AI-supported phishing detection and anomaly identification [55], but extend it to the cross-channel ecologies that shaped their lived experiences. Participants imagined AI tools that could compare message content across email and SMS, identify deviations from legitimate institutional patterns, highlight suspicious sender behavior, or provide contextual explanations about typical procedures. For newcomers navigating a period of transition and uncertainty, such capabilities could offer meaningful support.

However, our findings also reveal critical cautions. Participants expressed concern about misunderstanding AI judgments or relying on them too heavily. This reflects prior evidence that users struggle when AI explanations do not match their mental models [24], [40], [33]. Several worried about false positives that might increase stress or undermine trust in legitimate institutional communication. These concerns underscore the importance of human-in-the-loop approaches where AI surfaces anomalies but users remain the final decision

makers, supported by transparent, culturally accessible, and migration-aware explanations. Participants stressed that AI should detect and contextualize suspicious content but leave the final decision to the user.

Moreover, AI systems that ignore cultural, linguistic, or situational context may misinterpret benign variations in communication style or fail to recognize threats that exploit migration-specific circumstances and transitional pressures. Prior work shows that security cues often carry different meanings across cultural backgrounds [54], [33]. As such, AI-assisted security for educational migrants must be designed with caution: emphasizing interpretability, minimizing unnecessary alarms, and embedding safeguards that allow users to question, override, or request clarification about system outputs. These considerations are essential for developing AI tools that enhance, rather than complicate, newcomers' navigation of complex cross-channel scams.

Together, our work suggest that future AI-assisted security tools for educational migrants should prioritize explainability, cultural grounding, and human-in-the-loop control rather than automation-first approaches.

VI. Limitations and Future Work

While this study contributes new insights into the digital security experiences of educational migrants from the Global South and their design visions for protective technologies, several limitations should be acknowledged. Our sample of 22 participants, though intentionally composed of students navigating early-stage migration, does not capture the full heterogeneity of international student populations. Digital practices and threat exposures may differ by socio-economic background, academic discipline, institutional support structures, language proficiency, or migration pathway. Future work could expand to larger and more varied samples, including students in community colleges, intensive English programs, or migrants outside formal higher education systems. Moreover, further work could formalize these findings into a migration-situated threat model that captures impersonation pathways, cross-channel reinforcement patterns, and institutional trust exploitation strategies.

Our data were collected through participatory design sessions and self-reported accounts, which may be shaped by recall bias, selective disclosure, or participants' uncertainty about which experiences "count" as security threats. In addition, we used a single storyboard scenario as a generative grounding prompt rather than a comprehensive coverage of the threat landscape. Although participants were encouraged to move beyond the scenario and draw on any relevant experience, different scenarios (e.g., housing, employment, financial services, or government communication) might elicit different design priorities. Complementary methods such as diary studies, ecological momentary assessment, or analyses of real-world scam exposures could provide more granular insight into how threats unfold and how newcomers assess and respond to risk in situ.

Because we focused specifically on educational migrants, our findings may not generalize to other migrant groups (such as work-based migrants, refugees, and asylum-seekers) whose sociotechnical constraints and threat ecologies may differ substantially. Future research should examine how security challenges vary across migration types, cultural backgrounds, and stages of settlement, and how context-aware security needs evolve over time.

Finally, while we used AI capability roles only as a conceptual scaffold to help participants articulate desired system behaviors, rather than to evaluate or propose specific AI systems, participants' responses highlight important directions for future work. In particular, further research is needed to explore how explainable, human-in-the-loop, and culturally grounded AI-assisted security tools might be designed, evaluated, and governed in ways that support migrants without undermining trust, agency, or institutional understanding. Longitudinal studies could also examine how perceptions of risk, trust in such tools, and expectations of human-centered automation change over the course of migrants' adaptation processes.

VII. Conclusion

This study examined how educational migrants from the Global South encounter and interpret digital threats during their early transition into the U.S. sociotechnical environment and demonstrated how participatory design can surface migration-responsive security needs. Our findings show how unfamiliar communication norms, limited local knowledge, and cross-channel scam practices shape newcomers' vulnerability, and how participants envision tools that provide clearer verification, cross-channel detection, migrant-focused orientation resources, contextual guidance, and protective capabilities integrated into institutional systems. Participants also articulated opportunities for AI-assisted features, emphasizing detection, anomaly identification, and interpretable explanations that reduce uncertainty while preserving user control. By centering newcomers' lived experiences and design contributions, this work highlights the importance of transparent, culturally grounded, and context-aware digital safety support during periods of adjustment and points toward the need for human-in-the-loop, migration-aware, ecosystem-level security interventions that better support educational migrants navigating unfamiliar digital environments.

Acknowledgments

The authors are grateful for their participants' ideas and engagement, without which this paper would not be possible, and to Heather Richter Lipford and the other members of the Human-Centered Computing Lab at UNC Charlotte, who provided feedback on early stages of this research. This project was supported by a 2024 Google Research Award. Faklaris was also partially supported by U.S. National Science Foundation (NSF) Grant No. 2346281, DOD Department of the Army (DA) Grant No. W911NF2410189, and BasisTech founder Carl Hoffman. Zare was also partially supported by a FS-ISAC Future Leaders in Cyber Scholarship.

REFERENCES

[1] Z. J. Acs, E. Lafuente, and L. Szerb. The digital ecosystem around the world: A composite indicator analysis. *Journal of Platform Economics*, page 2150001, 2021.

[2] M. A. Al Montaser and M. Bannett. Beyond anomaly detection: Redesigning real-time financial fraud systems for multi-channel transactions in emerging markets. *Baltic Journal of Multidisciplinary Research*, 2(3):1–17, 2025.

[3] A. Algarni, Y. Xu, and T. Chan. Social engineering in social networking sites: the art of impersonation. In *2014 IEEE International Conference on Services Computing*, pages 797–804. IEEE, 2014.

[4] H. K. Aljasim and D. Zytko. Foregrounding women's safety in mobile social matching and dating apps: a participatory design study. *Proceedings of the ACM on Human-Computer Interaction*, 7(GROUP):1–25, 2023.

[5] R. M. Allen and K. Bista. Talented, yet seen with suspicion: Surveillance of international students and scholars in the united states. *Journal of International Students*, 12(1):175–194, 2022.

[6] R. G. Aricat. Mobile ecosystems among low-skilled migrants in singapore: An investigation into mobile usage practices. *The Electronic Journal of Information Systems in Developing Countries*, 68(1):1–15, 2015.

[7] R. Atkinson and J. Flint. Accessing hidden and hard-to-reach populations: Snowball research strategies. *Social research update*, 33(1):1–4, 2001.

[8] L. Bannon, J. Bardzell, and S. Bødker. Introduction: Reimagining participatory design—emerging voices, 2018.

[9] M. R. Bartolomei and A. Cava. Vulnerability, digital technologies and international law: Reflections on contemporary migration flows. *Law, Technology and Humans*, 6(2):16–28, 2024.

[10] K. Bell, B. Cash, H. Boetto, and K. Thampi. International study abroad programmes: Exploring global south student perspectives, reciprocity and sustainability. *Social Work Education*, 40(4):492–504, 2021.

[11] V. Bello. Virtual belongings, dual identities and cultural discomforts: The role of mediaspaces and technospaces in the integration of migrants. *Crossings: Journal of Migration & Culture*, 5(2-3):213–229, 2014.

[12] J. Bhatia and T. D. Breaux. Empirical measurement of perceived privacy risk. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 25(6):1–47, 2018.

[13] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[14] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: Designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS)*, SOUPS '13, 2013.

[15] A. C. Campbell and E. Neff. A systematic review of international higher education scholarships for students from the global south. *Review of educational research*, 90(6):824–861, 2020.

[16] A. Dangol, M. Newman, R. Wolfe, J. H. Lee, J. A. Kientz, J. Yip, and C. Pitt. Mediating culture: Cultivating socio-cultural understanding of ai in children through participatory design. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference*, pages 1805–1822, 2024.

[17] I. Datey and D. Zytko. " just like, risking your life here": Participatory design of user interactions with risk detection ai to prevent online-to-offline harm through dating apps. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW2):1–41, 2024.

[18] Department of Homeland Security. International students: Be aware of potential scammers. *Study in the States*, Jun 2022. Accessed: November 02, 2025.

[19] E. Díaz Gras. The global south: What's in a name?, Oct 2024.

[20] Editorial Staff. Cyberattacks are targeting immigrants. *Brilliance Security Magazine*, Jan 2024. Accessed: November 10, 2025.

[21] C. Faklaris, L. Dabbish, and J. I. Hong. A framework for reasoning about social influences on security and privacy adoption. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2024.

[22] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo. Rethinking Connection Security Indicators. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 1–14, Denver, CO, USA, 2016. USENIX Association.

[23] P. Fischer, S. E. Lea, and K. M. Evans. Why do individuals respond to fraudulent scam communications and lose money? the psychological determinants of scam compliance. *Journal of Applied Social Psychology*, 43(10):2060–2072, 2013.

[24] K. R. Fulton, R. Gelles, A. McKay, Y. Abdi, R. Roberts, and M. L. Mazurek. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 79–95, 2019.

[25] H. GHORASHI*. How dual is transnational identity? a debate on dual positioning of diaspora organizations. *Culture and Organization*, 10(4):329–340, 2004.

[26] A. Goldfarb and C. Tucker. Shifts in privacy concerns. *American Economic Review*, 102(3):349–353, 2012.

[27] T. Guberek, A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub. Keeping a low profile? technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–15, 2018.

[28] K. Halskov and N. B. Hansen. The diversity of participatory design research practice at pdc 2002–2012. *International journal of human-computer studies*, 74:81–92, 2015.

[29] F. Herbert, S. Becker, L. Schaewitz, J. Hielscher, M. Kowalewski, A. Sasse, Y. Acar, and M. Dürmuth. A World Full of Privacy and Security (Mis)conceptions? Findings of a Representative Survey in 12 Countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*, pages 1–23, New York, NY, USA, April 2023. Association for Computing Machinery.

[30] K. Holtzblatt and H. Beyer. *Contextual design: defining customer-centered systems*. Elsevier, 1997.

[31] A. S. Hwang, K. N. Truong, and A. Mihailidis. Using participatory design to determine the needs of informal caregivers for smart home user interfaces. In *2012 6th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops*, pages 41–48. IEEE, 2012.

[32] Institute of International Education. United States hosts 1.2 million international students at colleges and universities, totaling 6% of U.S. higher education. *PR Newswire*, Nov 2025. Accessed: December 04, 2025.

[33] N. Jain, R. S. Dubey, L. N. Yadav, G. Poongodi, N. Kumar, and S. S. Thavara. Artificial intelligence in personalization and its impact on consumer trust: A cross-cultural study of digital purchases. *Advances in Consumer Research*, 2:4328–4336, 2025.

[34] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, and Y.-K. Lim. What instills trust? a qualitative study of phishing. In *International Conference on Financial Cryptography and Data Security*, pages 356–361. Springer, 2007.

[35] S. H. Khandkar. Open coding. *University of Calgary*, 23(2009):2009, 2009.

[36] L. Knox. New ice policy puts international students at greater risk.

[37] S. J. Lipura and F. L. Collins. Towards an integrative understanding of contemporary educational mobilities: a critical agenda for international student mobilities research. *Globalisation, Societies and Education*, 18(3):343–359, 2020.

[38] V. Lymishchenko, E. Kamar, E. V. Botchkovar, and D. Maimon. Comparative analysis of cyber fraud ecosystems: Telegram and dark web platforms in digital criminal landscapes. *Available at SSRN 5722747*, 2025.

[39] N. McDonald, S. Schoenebeck, and A. Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on human-computer interaction*, 3(CSCW):1–23, 2019.

[40] T. Nazir. Bridging the gaps: Exploring ai-driven emotional, academic, and social support for international students. *International Journal of Human–Computer Interaction*, pages 1–9, 2025.

[41] C. Y. Oh and B. S. Butler. Newcomers from the other side of the globe: International students' local information seeking during adjustment. *proceedings of the Association for Information Science and Technology*, 53(1):1–6, 2016.

[42] Open Doors Internatinal Student Data. International Students Enrollment Trends. *IIE Open Doors*, Nov 2025. Accessed: December 04, 2025.

[43] C. Pyle, N. B. Ellison, and N. Andalibi. Social media and college-related social support exchange for first-generation, low-income students: The role of identity disclosures. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2):1–36, 2023.

[44] M. Ragnedda and A. Gladkova. Understanding digital inequalities in the global south. In *Digital inequalities in the global south*, pages 17–30. Springer, 2020.

[45] M. L. Rahman, D. Timko, H. Wali, and A. Neupane. Users Really Do Respond To Smishing. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy (CODASPY '23)*, pages 49–60, Charlotte, NC, USA, 2023. Association for Computing Machinery.

[46] E. M. Redmiles. " should i worry?" a cross-cultural examination of account security incident response. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 920–934. IEEE, 2019.

[47] T. Roy, L. F. Hodges, S. B. Daily, and J. McClendon. Secondlook: Participatory design process to create a phone app that detects digital dating abuse. In *2016 IEEE International Conference on Healthcare Informatics (ICHI)*, pages 320–327. IEEE, 2016.

[48] K. Salehzadeh Niksirat, E. Anthoine-Milhomme, S. Randin, K. Huguenin, and M. Cherubini. "i thought you were okay": Participatory design with young adults to fight multiparty privacy conflicts in online social networks. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference*, pages 104–124, 2021.

[49] N. N. Schia. The cyber frontier and digital pitfalls in the global south. *Third World Quarterly*, 39(5):821–837, 2018.

[50] T. Sharma, S. Kaushik, Y. Yu, S. I. Ahmed, and Y. Wang. User Perceptions and Experiences of Targeted Ads on Social Media Platforms: Learning from Bangladesh and India. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*, pages 1–15, New York, NY, USA, April 2023. Association for Computing Machinery.

[51] M. Sleeper, W. Melicher, H. Habib, L. Bauer, L. F. Cranor, and M. L. Mazurek. Sharing personal content online: Exploring channel choice and multi-channel behaviors. In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pages 101–112, 2016.

[52] B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman. Security fatigue. *IT Professional*, 18(5):26–32, 2016.

[53] I. M. Stepnov, P. I. Kasatkin, and T. V. Kolesnikova. Digital divide: Understanding the disparities between global north and global south. In *Polycrisis and Economic Development in the Global South*, pages 171–183. Routledge, 2024.

[54] E. Strandt and J. Murnane-Rainey. Cross-cultural differences in ai acceptance among leaders: A utaut-based study of western and eastern perspectives. *Journal of Leadership Studies*, 19(2):e70017, 2025.

[55] A. Suresh and A. C. Jose. Detection of malicious activities by ai-supported anomaly-based ids. In *Artificial Intelligence for Intrusion Detection Systems*, pages 79–93. Chapman and Hall/CRC, 2023.

[56] H. Susanto, L. F. Yie, D. Setiana, Y. Asih, A. Yoganingrum, S. Riyanto, and F. A. Saputra. Digital ecosystem security issues for organizations and governments: Digital ethics and privacy. In *Web 2.0 and cloud technologies for implementing connected government*, pages 204–228. IGI Global, 2021.

[57] F. Sussan and Z. J. Acs. The digital entrepreneurial ecosystem. *Small business economics*, 49(1):55–73, 2017.

[58] S. Tabassum, C. Faklaris, and H. R. Lipford. What drives smishing susceptibility? a u.s. interview study of how and why mobile phone users judge text messages to be real or fake. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 393–411, 2024.

[59] S. Tabassum, N. Mathew, and C. Faklaris. Privacy on the move: Understanding educational migrants' social media practices through the lens of communication privacy management theory. In *Proceedings of the ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies*, pages 1–18, 2025.

[60] The California Student Journalism Corps. International students in california grapple with fear of deportation, visa applications, Oct 2025.

[61] F. Thompson. Fbi warns of "scammer" immigration agents targeting wa foreign students, Jun 2025.

[62] M. Tran, C. W. Munyendo, H. S. Ramulu, R. G. Rodriguez, L. B. Schnell, C. Sula, L. Simko, and Y. Acar. Security, privacy, and data-sharing trade-offs when moving to the united states: Insights from a qualitative study. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 617–634. IEEE, 2024.

[63] U.S. Citizenship and Immigration Services. Common scams: Uscis, Nov 2025. Accessed: December 29, 2025.

[64] M. Verhaar. From chat to crime: Telegram's secrets! TU Delft Repository, 2025.

[65] S. Weber, M. Harbach, and M. Smith. Participatory design for security-related user interfaces. *Proc. USEC*, 15, 2015.

[66] T. Weber and C. Van Mol. The student migration transition: an empirical investigation into the nexus between development and international student migration. *Comparative Migration Studies*, 11(1):5, 2023.

[67] K. C. Yang, A. Pulido, and K. Yowei. Exploring the relationship between privacy concerns and social media use among college students: A communication privacy management perspective. *Intercultural Communication Studies*, 25(2), 2016.

[68] N. Yildirim, C. Oh, D. Sayar, K. Brand, S. Challa, V. Turri, N. Crosby Walton, A. E. Wong, J. Forlizzi, J. McCann, et al. Creating design resources to scaffold the ideation of ai concepts. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, pages 2326–2346, 2023.

[69] N. Zare, C. Faklaris, S. Tabassum, and H. R. Lipford. Improving Mobile Security with Visual Trust Indicators for Smishing Detection. In *2025 IEEE World AI IoT Congress (AIIoT)*. IEEE, May 2025.

[70] M. B. Zorica, I. O. Biškupić, T. Ivanjko, and S. Špiranec. Students and privacy in the networked environment. In *2011 Proceedings of the 34th International Convention MIPRO*, pages 1090–1094. IEEE, 2011.

APPENDIX

This appendix provides supplementary materials to support methodological transparency, including recruitment text, consent procedures, and the participatory design protocol used in the study.

A. Recruitment Email Script

The following text was used for recruitment via social media posts and flyers:

Receive $20 if Selected for Our Research Study on Designing Privacy & Security Features for International Students

Researchers at UNC Charlotte (UNCC) are conducting a research study on the digital privacy and security needs of international students in the United States. We are seeking participants to help us designing better privacy and security tools through participatory design (PD) sessions.

Who are International Students? For this study, international students are defined as individuals who have moved from another country to the U.S. primarily for educational purposes.

About the Study: This study explores how international students manage digital privacy and security during post-migration transitions and collaboratively designs features to better support their needs across digital platforms.

Participant Criteria:

- Aged 18 or older
- Moved to the U.S. primarily for educational purposes
- Able to attend an in-person PD session at UNCC or a virtual session via Zoom

Study Details: Participants will take part in a participatory design session involving group discussion and collaborative design activities. Sessions will last no more than two hours and will be audio recorded. Participants may create sketches or design artifacts. Upon completion, participants will receive a $20 Amazon e-gift card.

How to Get Involved: If you are interested in participating, please complete a brief eligibility survey to determine your eligibility and provide your contact information.

If you have any questions about the study, please contact the researchers via the provided email addresses. Thank you for your time and help!

B. Consent Process

The study followed a two-stage consent process:

Consent 1: Eligibility Survey Consent. Before completing the eligibility survey, individuals reviewed an online consent form describing the study purpose, voluntary nature of participation, confidentiality, and the absence of compensation for completing the survey alone. Only non-sensitive demographic information was collected. Identifying information from individuals not selected for the PD sessions was deleted.

Consent 2: Participatory Design Session Consent. Selected participants received a detailed consent form prior to the PD session. This form described session activities, recording procedures, potential risks, compensation, and participants' rights. Verbal consent was reconfirmed at the start of each session.

C. Participatory Design Protocol

Participatory design sessions were conducted in small groups of two to four participants and lasted approximately 83 minutes on average. Sessions were held either in person at UNCC usability lab or remotely via Zoom.

Each session followed a consistent structure:

1) Introduction to the study and confirmation of consent
2) Discussion of participants' post-migration digital experiences, including privacy and security concerns using the storyboard
3) Reflection on past encounters with scams or digital threats
4) Design activity in which participants sketched or described desired privacy and security features
5) Group discussion and feedback on proposed design ideas
6) Exploring the AI capability roles (detect, estimate, act, forecast, identify, generate, compare, discover) for their design ideas

In-person sessions used paper-based materials (e.g., pens, markers, and paper), while remote sessions used a shared Miro board. Audio was recorded for all sessions; no video was recorded. **As each session involved a small group discussion, an anonymous Google Form was provided after each session to allow participants to share additional feedback privately if desired.** Participants who completed a full participatory design session received a $20 Amazon e-gift card as compensation for their time

D. Code Book

TABLE II
CODEBOOK FOR DIGITAL PRIVACY AND SECURITY CHALLENGES AFTER MIGRATION

Theme	Description	Representative Quotes
Cross-channel scams and impersonation	Participants received fraudulent calls, emails, or messages impersonating government agencies or service providers, often across multiple channels.	"I have been receiving non-stop calls from IRS... they are not even from America." (P17); "I received a call pretending to be a Homeland Security officer." (P15)
Housing and job-related information requests	Confusion about what personal information is legitimate to share with housing providers or employers, especially sensitive identifiers such as SSN.	"One [housing company] was asking for the SSN number, and I was confused, should I share or not?" (P4); "Since I started job searching, the number of scam calls increased." (P6)
Financial fraud and unauthorized transactions	Experiences with unauthorized charges and gradual financial theft.	"Someone was taking out my money... the scammer started with a very small amount... then increased the amount slowly." (P2)
Social media and identity-related concerns	Concerns that personal information from social media or marketplaces is used to target scams or fraud.	"It's really easy to get scammed... social media shows birthdate or location." (P1); "They kept asking for money in advance... that urgency triggered something... I realized it's a scam." (P16)
General confusion about U.S. digital and institutional expectations	Ongoing uncertainty about which communications and requests are legitimate in the U.S. context.	"This confusion is happening to me every day in USA... we have indecision in most cases." (P1)

TABLE III
CODEBOOK FOR PARTICIPANT-GENERATED DESIGN THEMES

Theme	Design Goal	Representative Quotes
Theme 1: Reporting, Verification, and Investigative Feedback	Make reporting visible, transparent, and actionable.	"I want to report a scam and see what happens after." (P1); "Copy–paste and tell me if this is real, and what I should do next." (P4)
Theme 2: Cross-Channel Scam Filtering for SMS and Phone Calls	Reduce scam overload and explain why messages are suspicious.	"I wish my phone could filter them like email spam." (P2); "Explain why it is suspicious, not just block it." (P14)
Theme 3: Migrant-Focused Scam Databases and Trend Tracking	Support collective learning about scams targeting migrants.	"People share scam stories so others can avoid them." (P4); "Update about the latest scams happening in your area." (P22)
Theme 4: Guidance and Decision Support (Cues, Explanations, and What-Not-to-Share)	Provide lightweight guidance about safe actions and red flags.	"Tips on what not to post online." (P8); "Summarizes the cues and tells me why this message is risky." (P12)
Theme 5: Risk Assessment and Just-in-Time Support	Warn users during moments of stress, fatigue, or urgency.	"Sometimes I'm sleepy or busy, and that's when I make mistakes." (P17)
Theme 6: Protective Technical Capabilities	Support verification, translation, and authentication at a technical level.	"There should be a universal key or authentication so you know who is contacting you." (P15)
Theme 7: University-Integrated Digital Safety Support	Embed safety support into trusted university systems.	"Students trust school websites more than random apps." (P16)