"I Wonder if These Warnings Are Accurate": Security and Privacy Advice in Nine Majority World Countries

Collins W. Munyendo[1,2], Veronica A. Rivera[2,3], Jackie Hu[2,4], Emmanuel Tweneboah[2], Amna Shahnawaz[5], Karen Sowon[6], Dilara Keküllüoğlu[7], Marcos Silva[2,8], Yue Deng[2,9], Mercy Omeiza[10], Gayatri Priyadarsini Kancherla[11], Maria Rosario Niniz Silva[12], Abhishek Bichhawat[11], Maryam Mustafa[5], Francisco Marmolejo-Cossio[13], Elissa M. Redmiles[14†], and Yixin Zou[2†]

[1]*The George Washington University, USA,* [2]*Max Planck Institute for Security and Privacy, Germany,* [3]*Georgia Institute of Technology, USA,* [4]*University of Michigan, USA,* [5]*Lahore University of Management Sciences, Pakistan,* [6]*Indiana University, USA,* [7]*Sabanci University, Türkiye,* [8]*Federal Center for Technological Education of Minas Gerais, Brazil,* [9]*The Hong Kong University of Science and Technology, China,* [10]*University of Ibadan, Nigeria,* [11]*Indian Institute of Technology Gandhinagar, India,* [12]*The College of Michoacán, Mexico,* [13]*Boston College, USA,* [14]*Georgetown University, USA*

***Abstract*—Security and privacy (S&P) advice plays a crucial role in how people stay safe online. While prior work shows that the plethora of advice from varied sources makes it difficult for users to prioritize advice, the insights are primarily based on studies conducted in Western contexts. Other work shows that users outside the West have different S&P needs and thus, we cannot simply rely on advice curated in the West to generalize to the majority world—regions of Africa, Asia, Latin America, and the Middle East, where most of the world's population lives. We fill this gap by investigating S&P advice across nine majority world countries via 70 semi-structured interviews with *local experts*: cybercafe operators, tech repair specialists, and other community figures that people commonly rely on for tech support and S&P advice. We find that the advice provided by local experts in the majority world largely matches the advice they provide to their constituents and the advice from the West. However, we surface various significant barriers that hinder majority world users from implementing advice, including economic constraints, language barriers, and social friction from taking protective measures. Our findings further show how factors such as social norms and gender shape advice practices, e.g., by driving gendered advice-seeking. We discuss how S&P advice in the majority world can be improved and reflect on how the S&P community can better engage with local communities in conducting similar research.**

1. Introduction

Security and privacy (S&P) advice plays a critical role in how users learn to stay safe online [64], [65]. Prior work shows that users get S&P advice from various sources, including the web [67], social media [5], [8], [20], [79], [100], entertainment media [27], friends and family [28], [33], [35], [56], among others. However, the wide variety of advice and perceived inconvenience of following the advice makes it difficult for both experts and non-experts to prioritize advice to follow [9], [37], [67]. Further research has shown that advice sources and willingness to follow advice are strongly influenced by the perceived trustworthiness of advice [66], convenience/security trade-offs [2], [22], and socio-demographic factors [14], [38], [64], [65], [97].

While most of this work has focused on Western users, internet users outside the West have unique S&P needs and threat models due to different cultures [74], infrastructure [53], and socioeconomic backgrounds [52], [65]. Thus, we hypothesize that S&P advice developed in the West is likely to fail when used in other places in the world, potentially leaving users at risk. For instance, while using two-factor authentication is a commonly suggested advice [9], [37], cultural expectations in South Asia dictate that women share their phones with other family members, rendering this advice impractical [74]. Similarly, to protect accounts, users are often encouraged to select strong passwords across accounts [9], [37]. However, previous work in Kenya [53] finds that people often rely on public computers, e.g., at cybercafes, and the managers at those facilities to manage their passwords. To ease their workload in helping many users remember passwords, cybercafe managers encourage users to select simple passwords such as their names or ID numbers, contradicting advice from the West [9], [37].

To create a safe online experience for people in the majority world,[1] it is imperative to investigate how they are advised to stay safe and gaps in the provided advice. Prior work in Western [64] and majority world contexts [32], [35], [53] finds that people rely on others for S&P advice. These

[†]*Elissa M. Redmiles and Yixin Zou co-advised this work equally.*

1. Majority world refers to the countries that contain the majority of the world's population, and has been proposed to describe countries in Africa, Asia, and South America. It's an alternative to terms such as "developing countries" and "third world" which might come across as being pejorative.

trusted sources include friends and family [32], [35], work colleagues [32], and community figures like cybercafe owners [53]. Our study examines S&P advice in the majority world through the perspectives of "local experts" i.e., individuals who offer tech support or guidance within their communities, including cybercafe operators, phone and computer repair technicians, communication technology trainers, digital freelancers, tech-savvy teachers, among others. We seek to address the following three research questions:

RQ1: What security and privacy advice is prioritized by local experts in the majority world?

RQ2: What are the sources of this advice and what concerns inform the advice provided?

RQ3: What barriers do local experts and their constituents face in implementing the advice?

To answer these questions, we conducted 70 semi-structured interviews with local experts in a variety of occupations, e.g., cybercafe operators, tech repair shop owners, teachers, and computer and phone sellers (more details in Table 2). We focus on local experts because they assist a broad range of people in their communities, providing a first look at the S&P concerns community members raise and the advice these experts offer them. The local experts we interviewed are from nine majority world countries spanning four continents: Africa (Ghana, Kenya, and Nigeria), Latin America (Brazil and Mexico), Asia (China, India, and Pakistan), and the Middle East (Türkiye). Collectively, these nine countries account for close to 50% of the world's population [103], and are highly diverse in their geographic locations, internet penetration rates, smartphone ownership rates, internet freedom, cultures, religion, and gender (in)equality rates (see Table 1).

Our study surfaces advice prioritization challenges in the majority world due to the broad range of S&P advice offered, similar to prior work in the West [37], [67]. While the advice that local experts provide to their constituents mostly matches the advice they prioritize for their own S&P, we find some differences. For instance, while local experts use VPNs, they advise their constituents to use trusted experts and memorable passwords. When we compare local experts' advice to advice from the West, we once again find significant overlap but with notable differences. For example, password managers and regular software updates are frequently encouraged in the West, but less so by local experts in our study. Importantly, users face significant barriers in implementing advice, including not knowing benefits of the advice (e.g., no visible UI changes after security updates), economic constraints (e.g., inability to afford expensive authentic software), and social frictions that are caused by taking protective S&P measures such as using an unlock PIN or password on a mobile phone.

While prior work has quantified correlations between sociodemographic factors and S&P practices [99], our study contributes in-depth insights into *how* gender, culture, and religion shape S&P concerns and advice in the majority world. For instance, collectivist cultures and religion compel people to share their devices, undermining privacy affordances from the West where device sharing is less common. Gender influences advice-seeking behaviors, with women preferring to seek advice from other women. Our work suggests the need for better advice prioritization and consideration of majority world users in tech and S&P design. We also advocate for better translation of tech tools and S&P advice. Lastly, our methodology shows how and why it is critical to engage local communities in conducting similar research.

2. Related Work

S&P advice studies. Previous studies conducted mostly with Western participants have explored where users get S&P advice from and the efficacy and actionability of that advice. Redmiles et al. [67] found that there are a lot of security imperatives on the web, making it difficult for users to prioritize important advice. Both Redmiles et al. and Reeder et al. [68] found that the security community lacks consensus on the most important pieces of advice for users to follow. Other research has identified factors that influence advice sources and adherence, including the trustworthiness of advice [66], convenience/security trade-offs [2], [22], and socio-demographic factors [14], [38], [64], [65], [97]. Recently, Rotthaler et al [71] have demonstrated that a mobile app can be effectively leveraged to provide S&P advice.

Prior work has also compared S&P advice between experts vs non-experts. Ion et al.'s US-based study [37] in 2015 noted how experts and non-experts prioritized different practices for staying safe online, e.g., experts prioritize installing updates, whereas non-experts focus on avoiding unknown links. A replication study with European participants in 2019 confirmed most findings [9]. An even more recent replication of Ion et al.'s study by Ortloff [58] in 2025 notes that both experts and non-experts are beginning to particularly focus on authentication practices such as two-factor authentication, while the use of anti-virus is becoming less popular. To enable comparison with these studies in the majority world, we similarly ask local experts in our study to list their top three advice for staying safe online to explore S&P advice prioritized in majority world countries.

Recent work has shown how social media is used to disseminate S&P advice, e.g., how TikTok is used to spread "anti-security" and "anti-privacy" advice [100] and facilitate cheating on proctored tests [79]. Other studies have featured Twitter's role in disseminating S&P advice during the Black Lives Matter protests [8] and the Russian invasion of Ukraine [77]. Other work has questioned user engagement of S&P advice on social media [5]. In our study, several participants also rely on social media for S&P advice.

S&P studies in the majority world. Recent research has increasingly focused on users in the majority world due to their unique S&P challenges. In South Africa [69] and Kenya [54], users of social messaging apps like WhatsApp are more concerned about interpersonal privacy than the S&P risks posed by the platforms; this explains the proliferation of WhatsApp mods in Africa despite their security risks [54]. In South Asia, women are culturally expected to share their

phones with others, forcing them to resort to techniques such as content deletion and the use of app locks to protect their privacy [74]. In Kenya [43], [52] and India [62], financial adversity often compels mobile loan app users to deprioritize their privacy concerns with these apps to procure loans. Kotut [43] shows how laxity in policy enforcement leaves loan app users in Kenya vulnerable to these apps. In Lebanon and Ghana, failing infrastructure often necessitates "infrastructuring" practices to overcome institutional and systemic failures [48], [90], e.g., technology users relying on intermediaries to charge their devices when they do not have access to electricity. As infrastructuring poses S&P risks to users, McClearn et al. [48] introduce the concept of "security patchworking" to describe practices that users subsequently adopt to protect their everyday security. Similar infrastructuring and patchworking practices have been noted in the majority world and beyond, for example among refugees [36], [72], activists [16], migrants [13], domestic workers [81], LGBTQ+ users [41], women [6], [86], [101], and low socioeconomic users [7], [32], [42], [53].

Other studies have compared multiple countries, showing that S&P needs vary across countries and cultures [4], [11], [34], [39], [63], [76], [78]. These differences are directly shaped by culture [15], [63], infrastructure [53], context [95], social isolation [40], local regulations, religion, among others. Accordingly, researchers have designed solutions that are more tailored to the needs and constraints of the majority world, including mHealth solutions designed to aid frontline health workers in India, Kenya, and Zimbabwe [45], redesigned privacy-preserving protocols for mobile money services in Kenya [82], and affordable contact-tracing wearables suitable to low and middle income countries [73].

Regarding S&P advice, while previous work in the West shows that many users rely on social contacts for advice [64], research in the majority world suggests that majority world users rely even more heavily on social connections [35] for S&P advice due to collectivist cultures compared to their Western counterparts from individualistic cultures [63]. For instance, low socioeconomic people in Pakistan heavily rely on community advice and support to protect their S&P [32]. Low-income users and older adults in India [55], [75] and Bangladesh [1], [85] rely on other more skilled users (e.g., from their families) to access technology while in Kenya, many users rely on cybercafe managers for technology access and S&P advice [53]. Crucially, the support and advice offered by local experts is helpful but can also inadvertently leave their constituents at risk. For instance, cafe managers in Kenya often advise customers to use simple passwords such as their names, leaving them vulnerable to password guessing attacks [53]. Therefore, our study systemically explores the S&P advice that local experts prioritize across various majority world countries and the potential impact of this advice on users' digital S&P and safety.

A closely related to ours by Umbach et al. [91] interviewed participants from five majority world countries, finding that users across these countries had similar concerns to those noted in Western contexts, including desires to protect private information. However, device sharing was a common practice that amplified privacy concerns. While Umbach et al. focus on S&P awareness and adopted practices, our study focuses on how people come to gain awareness of protective practices through S&P advice across nine majority world countries. Given that previous work in the West [64] and the majority world [32], [35], [53] shows that users rely on other people for advice, we focus on local experts across these countries to understand concerns these experts prioritize when supporting others, the advice they provide to them, sources of the advice, and barriers to advice implementation. Understanding the advice landscape is crucial for better supporting the digital S&P of users in the majority world.

3. Methodology

To explore S&P advice across nine majority world countries, we worked with local in-community contacts and collaborators to identify and interview 70 local experts. We chose interviews because (a) our research questions are exploratory, and interviews allowed deeper probes; (b) many of the countries we focus on lack survey infrastructure and are not covered by survey platforms such as Prolific.

Country selection. We selected nine majority world countries that are highly diverse in their geographic locations, internet penetration rates, smartphone ownership rates, internet freedom scores, cultures, religion, and gender (in)equality (see Table 1). Prior work [53], [65] suggests that these factors influence peoples' S&P concerns and practices. In particular, we selected countries from the following regions: Africa (Ghana, Kenya, and Nigeria), Latin America (Brazil and Mexico), Asia (China, India, and Pakistan), and the Middle East (Türkiye). On aggregate, these nine countries account for approximately 47.48% of the world's population [103] but remain understudied in S&P research [31].

Research personnel. To execute this large-scale study across multiple countries, we started with a core multidisciplinary team of five researchers. The core team has vast experience studying S&P in both Western and majority world countries, as well as engaging with at-risk populations. Three members are natives from two majority world countries, and the core team collectively speaks four languages spoken in the countries of study. After the core team ideated and designed the study, we expanded the team's diversity in lived experience, expertise, and language skills by building and collaborating with a distributed network of 13 additional researchers and contacts in the nine majority world countries. Our local contacts helped us identify and recruit suitable participants as well as conduct interviews in local languages.

We compensated our local contacts for their assistance in translating the interview protocol, moderating the interviews, and delivering the transcripts to us in English. We additionally included as coauthors all our contacts who engaged in data analysis and paper writing with our team. For quality control, our core team reviewed all prospective participants shortlisted by the local contacts to ensure they matched our criteria for local experts prior to conducting interviews. For our contacts

new to qualitative research, the core team trained them on how to effectively conduct interviews. We also invited them to listen in on interviews conducted in other countries. Where language permitted, a member of the core research team also participated in interviews conducted by our local contacts and asked follow-up questions where needed.

Recruitment and demographics. We define a local expert as anyone who provides tech (or related) services, support, or advice to members of their community. While prior work in the majority world has used terms like intermediaries [75] to describe individuals who assist others with technology, we use the term local experts to specifically refer to those who are frequently consulted and regarded as knowledgeable, often outside of the familial relationships typically associated with intermediaries. To meet our criteria, these experts had to be publicly-facing and directly supporting the general public regularly as part of their job. Their job roles can include tech/repair shop owners, operators at cybercafes or libraries, phone/sim card sellers, teachers, religious leaders, community leaders, and more.

As local expert profiles can vary across countries, we worked with local contacts to identify and recruit suitable participants who met our criteria. Working with local contacts helped us reach populations (e.g., indigenous communities in the case of Mexico) that would otherwise have been impossible to reach. We did not publicly advertise the study to avoid scammers attempting to participate without meeting our criteria [59]. Additionally, as the interview protocol touches on sensitive topics such as surveillance, we wanted to avoid attracting scrutiny from officials in countries with authoritarian regimes to minimize risk to participants. In the end, we recruited a diverse pool of 70 local experts across the nine majority world countries, with each country having at least five and up to ten experts. Table 2 in the Appendix has more details about local experts and their roles.

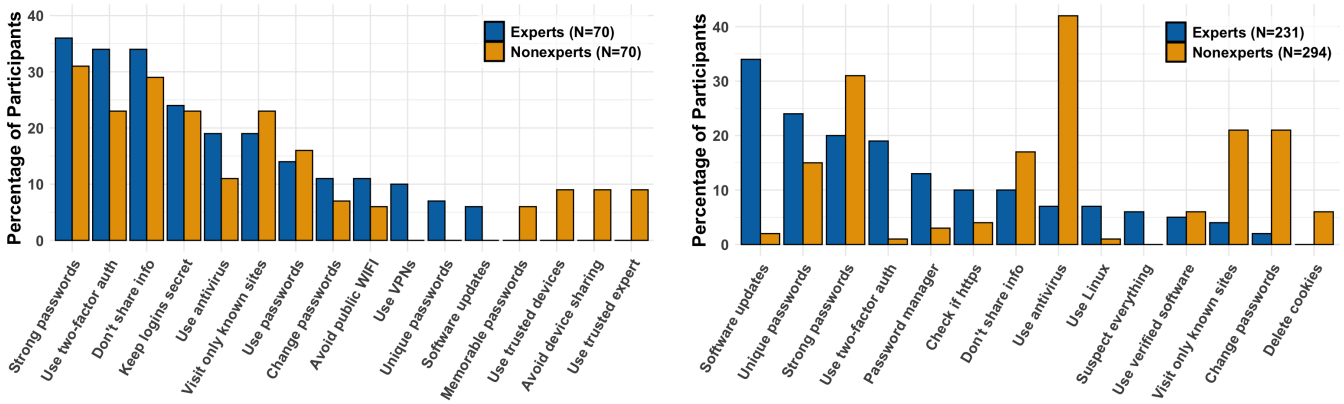
Interview procedure. We developed our interview guide around our research questions. Below is a summary of the interview procedure (see Appendix A for the full protocol).

- ***Local experts' background***: We first asked local experts about their background (**Q1** - **Q3**). Next, we asked them to indicate any technology challenges in their communities, followed by the support they provide others in resolving them (**Q4** - **Q5**). We additionally asked about the sources of this support or advice (**Q6**).
- ***S&P concerns***: Our next set of questions focused on concerns around technology and S&P. We first asked local experts about concerns they have about their own S&P and how they handle them (**Q7**), followed by the concerns people in their community come to them with and how they help them resolve these concerns (**Q8**).
- ***S&P advice***: We asked experts to provide their top three pieces of advice they currently (or would) follow to protect their S&P, following Ion et al. [37]. We probed where they learned the advice from, if they follow the advice, and challenges in following the advice (**Q9**). Following, we asked the experts for the top three pieces of advice they have provided (or would) to those they support (**Q10**). We also asked about advice people are likely to follow and advice gaps (**Q11** - **Q13**).
- ***Tech and S&P practices and challenges***: Next, we asked questions about local experts' personal technology use and practices (**Q14** - **Q16**), as well as those of other people they support in their local communities (**Q17** - **Q19**). We further probed about specific potential challenges in their communities such as common scams and phishing schemes (**Q21** - **Q23**).
- ***Other contextual factors***: To understand how S&P concerns and advice further vary, we next asked local experts whether they vary advice they provide based on their constituents' gender, religion, age, job type, as well as any other factor (**Q24**).
- ***Demographic questions***: Lastly, we asked local experts about their demographics including age, gender, and education (**D1** - **D5**). We also asked them to share any feedback they had about the study (**D6**).

Data collection. Due to the logistics involved in executing this study across nine countries, we started data collection in December 2023 and ended it in February 2025. We conducted pilots with two local experts, one from Kenya and another from China. We used the pilot feedback to refine our interview protocol and add more probes [12]. For example, when experts indicated they had not provided any advice, we asked them what advice they would provide if people asked. The interview guide was developed by our core team in English and translated to local languages by our contacts and collaborators. Most recruitment and interviews were conducted remotely and in local languages[2] by our collaborators, with the transcripts later translated to English for analysis. All interviews were audio-recorded. We compensated participants the equivalent of $40 based on the purchasing power parity of their countries [70]. For example, this translated to Ksh. 1,700 or $13.15 in Kenya. In some cases, we adjusted these rates as suggested by our contacts.

Data analysis. We qualitatively analyzed the interview transcripts using MAXQDA [47]. First, the lead researcher (serving as the primary coder for all transcripts) coded a few transcripts from Kenya to develop an initial primary codebook. Using this codebook, five secondary coders comprising in-community contacts or collaborators from Kenya, Ghana, China, Pakistan, and Turkiye performed secondary coding in their respective countries. As this was not possible for Nigeria, Brazil, Mexico, and India, our secondary coders with geographical proximity or familiarity with the culture in these countries assisted. For example, our Pakistani contact performed secondary coding for transcripts from India. In all the countries, at least half of the transcripts were double-coded and discussed by both coders. These discussions were used to refine codes and identify emerging themes, and thus there was no need to calculate inter-rater agreement [49].

2. As English is an official language in Ghana, Kenya, and Nigeria, interviews there were conducted in English. In Turkiye, one interview was conducted in English as the interviewee doubled as an English teacher.



(a) Top advice from our study.

(b) Top advice from Ion et al. [37]

Figure 1: Top advice for staying safe. Figure 1a has advice from our study while Figure 1b has advice from Ion et al. [37]. Since we only interviewed experts in our study, both expert and non-expert advice in Figure 1a was from experts' perspectives.

Limitations. Our study has several limitations. First, our sample size per country was relatively small. In Mexico, our engagement of indigenous students to recruit participants and conduct interviews might have biased our sample toward marginalized communities. Additionally, local experts across the nine countries were very diverse, with some countries having predominantly rural experts, while others had experts based in urban areas. However, the goal of our work is not to generalize to any of the countries but to surface common concerns and S&P advice. We also avoid making country-level comparisons as much as possible due to the diversity of experts across the nine countries. Further, as we conducted the interviews in countries that speak different languages and have different cultures, it is possible that some phrases or nuances might have been lost in translation. To mitigate this, we worked closely with local collaborators to ensure that our interview guide was appropriately translated and that interviews were conducted in local languages. We also involved our local contacts in analyzing the data and writing the results to ensure the local context was appropriately considered and respected throughout this study.

Ethics. Our study was reviewed and approved by five institutional ethics review boards. Where appropriate and possible, such as in Kenya, we also obtained local ethics approval. We took several measures to protect our study participants. In particular, participation was completely voluntary: participants could opt out anytime or decline to answer any question. As some of the questions (e.g., about surveillance) might put participants at risk, we worked with our local contacts and collaborators in each country to ensure it was both appropriate and acceptable to ask these questions. On three occasions during interviews, local experts were hesitant to discuss surveillance, and we thus did not probe any further. We minimized the collection of personally identifiable information (PII) from participants. Any PII shared by participants was removed from the transcripts before we conducted the analysis. In some cases, we collected participants' phone numbers for interview scheduling and payment; we deleted these details after interview completion.

Throughout the ideation, design, and execution of this study, we reflected on our goal for this work and made efforts to work with local collaborators and contacts from each country to ensure (a) local context is appropriately considered; and (b) research benefits can directly extend to local communities, in line with the research justice principle in the Belmont report [3].

4. Results

In this section, we discuss local experts' top three advice for their own S&P and that of their constituents, followed by the sources of this advice. We then discuss the concerns that this advice seeks to address, followed by reasons why both local experts and users follow the advice. Lastly, we discuss barriers and contextual factors that make it challenging for users to follow the advice. We refrain from reporting counts to avoid implying generalizability; those provided in Figure 1 show how the advice in our study compares to prior work; however, we caution against drawing any generalized findings. Finally, we focus on broader themes across the nine countries, and where possible, mention some country-specific themes.

4.1. Top Three S&P Advice

Overview. While the advice in our study overlaps with advice from the West—evidenced by the use of strong passwords and two-factor authentication—we also found several differences. For example, local experts often promoted general password use (including memorable passwords) among their constituents, prioritizing account access over security.

Top S&P advice. Figure 1 shows participants' top three advice for staying safe online. Figure 1a has advice mentioned by local experts (n=70) in our study for their S&P (experts) but also that of their constituents (nonexperts), while Figure 1b has the top three advice mentioned directly by both experts (n=231) and nonexperts (n=294) in an earlier US-based survey study conducted by Ion et al. [37]. While Busse et al. [9] recently replicated the study by Ion et al. in Europe, we compare our results only to the original work by Ion et al., as the findings from Busse et al. substantially overlap with those of the original study.

Expert vs. non-expert advice in the majority world. Overall, we find that local experts' top three personal advice for staying safe were mostly similar to the top three advice they provide to others in their community (Figure 1a). In particular, this advice revolved around the use of strong passwords, 2FA, not sharing personal information, keeping logins secret, using anti-virus software, avoiding clicking on unknown links, generally using passwords, frequently updating passwords, and avoiding public WI-FI. However, we also noted some differences. In particular, experts themselves additionally seemed to use VPNs and prioritize software updates, but less frequently recommended this advice to others. It appears that when advising others, experts prioritize advice that is simple for users but also affordable. Unfortunately, as software updates often require purchasing the Internet, this can often be seen as unnecessary cost for users, especially if they do not understand the benefits of the updates.

On the flipside, experts encourage their constituents to use trusted devices, avoid device sharing, consult trusted experts only, and use memorable passwords more compared to their own personal advice. We hypothesize that because users often need to share their sensitive data for assistance, local experts emphasize the need for trust, both on the device level as well as for consulted experts. For passwords, local experts recommend memorable passwords because their advisees frequently forget complex passwords. Thus, account access is often prioritized over account security.

Advice in the majority world versus in the West. When we compare advice from our study (Figure 1a) to Ion et al.'s (Figure 1b) study, we once again find many similar pieces of advice, but with some differences. In particular, strong passwords, unique passwords, use of 2FA, use of anti-virus, frequent password updates, avoiding unknown links, and not sharing personal information appear in both studies. However, the use of password managers is recommended frequently by experts in Ion et al, but not by experts in our study at all. This suggests that users (and even local experts) in the majority world might be less familiar with password managers in general. While software updates are the most frequently mentioned advice by experts in Ion et al.'s study, this advice is mentioned less frequently in our study. We hypothesize that local experts in the majority world might not really view the security benefits of these updates as a priority. Additionally, internet costs might make them less likely to recommend this advice to their constituents.

On the flip side, experts in our study frequently mention the use of passwords, avoiding public WI-FI, and regular backups; these are not among the top advice mentioned in Ion et al.'s study. While backups are a great piece of advice, using passwords alone is not sufficient for account security, especially if the passwords are weak, reused, or saved on shared devices. Avoiding public WI-FI is no longer important today, given that many websites have switched to using HTTPS. At the same time, however, local experts and their constituents do not always follow these pieces of advice, and we discuss reasons for that later in Section 4.5.1.

Main takeaway. Local experts in the majority world tailor their S&P advice to the practical needs of their constituents, prioritizing usability, account access, and affordability over strict adherence to what may be considered security best practices. Practices that are deemed costly, complex, or resource-intensive (e.g., software updates or VPNs) may be personally adopted by local experts but are not provided by local experts to their constituents. This directly shows how infrastructural and economic constraints shape S&P advice and practices in the majority world.

4.2. Sources of Advice

Overview. While sources of advice such as online platforms, past negative experiences, formal training, social circles, and traditional media have also been documented in Western contexts, we find that community ICT centers play a significant role in providing tech advice and support in the majority world. Additionally, many experts note a growing reliance on children as a trusted source of digital guidance.

Online sources. Similar to prior work in the West [8], [77], [79], [100], local experts across the nine majority world countries overwhelmingly pointed to online sources, including online searches and social media, as a source of advice for themselves and others in their communities. Different from those studies, some local experts indicated running social media pages, e.g., on Facebook as well as WhatsApp groups, to disseminate advice to their constituents. P56 (India) indicated that *"the Internet has all the answers these days"* while P02 (Kenya) runs *"several Whatsapp groups where I update them [people in their community]."* P58 (Pakistan) was overly trusting of advice on the Internet, stating that *"the Internet can not lie to you.* However, P41 (Brazil) was skeptical, stating that for their *"family, sometimes they share something in WhatsApp groups, and we say, no, it's not like that, you have to look for more reliable source[s] information.*

Previous negative incidents. Similar to prior work in the West [61], [64], we find that previous negative incidents are a common source of advice for experts and those they support. For instance, P04 (Kenya) uses strong passwords because *"a friend was using simple passwords and somebody came and guessed his information/passwords and entered into his accounts and messed up everything."* Regarding keeping logins secret, P55 (India) *"learned this from the mine and customers' experiences that we've had to deal with."* P44 (Brazil) *"learned the importance of backups through personal experience . . . This lesson hit home when I uninstalled WhatsApp while formatting my phone, not realizing I needed a backup, and ended up losing everything."*

Formal training. Similar to Redmiles et al. [64], some local experts pointed to some formal training as a source of their advice or expertise. This ranged from IT-related courses in school to courses taken online. For example, P23 (Ghana) *"was first introduced to VPN[s] by my teacher . . . in high*

school" while P44 (Brazil) *"learned about this [keeping passwords secret] in my technical course."*

Social circles. Another common source of advice for experts and their constituents was friends, partners, family, and colleagues, similar to previous work in the West [64]. In our study, however, local experts detailed how people increasingly rely on their children for advice. For instance, P55 (India) stated that people usually *"ask people around them, children around them, or someone who might be technically sound in their neighborhood."* Similarly, P67 (Türkiye) mentioned that parents rely a lot on their children: *"I think parents also use their children's, uh, support to . . . navigate through technology because our day and age children are really good."* The reliance on children for advice suggests that updates to school curriculum in the majority world to cover technology and security awareness could have widespread impacts.

Community ICT centers. Different from prior work in Western contexts [64], some experts pointed to local community ICT centers as places where people in their local communities seek advice or tech support. This included libraries (Türkiye), tech repair shops (Pakistan, Türkiye, Brazil, Ghana, Kenya), cybercafes (India, Kenya, Mexico), churches (Brazil), phone and computer sellers (Brazil, Ghana), government ICT centers (Kenya), and pharmacies (Türkiye). For example, P63 (Pakistan) stated that *"in Pakistan, it's very common to go to phone-repair shops to get technology support."* P43 (Brazil) pointed out how local churches also play an important role: *"The pastor . . . makes an ad about it, saying that on such and such a day, at such and such time, there will be a class, there will be a course for people to learn about computing."*

Official sources. While official sources are used more by users with more resources in the West compared to those with fewer resources [65], only a few experts in our study pointed to official sources, including customer care and government websites. While official sources are authoritative, users are hesitant to use them because of cost constraints. P11 (Nigeria) stated that there are *"premium services like people who go to Carlcare which are like the official companies/service representatives and so some people go to them because they believe that what comes for them is satisfactory."*

Traditional media. Lastly, a few experts mentioned getting advice from traditional media sources, including radio and TV. For example, P30 (Ghana) learned to avoid *"suspicious link[s] through education on the TV [and] on the radio"* while P44 (Brazil) said that *"in small towns, radio is still a big deal."* For rural areas in the majority world, traditional media could especially be a useful way to disseminate advice.

4.3. Concerns Addressed by Advice

Overview. We now discuss concerns that influence S&P advice provided by local experts. While most concerns, including account compromise and financial scams, have also been noted in the West, we find that most of the advice provided by local experts (see Section 4.1) protects users against account compromise, but less so against other concerns such as stalking and intimate partner violence. This potentially leaves users vulnerable to other S&P risks.

Account compromise. Described as "hacking" by local experts, account compromise occurs when an unauthorized individual gains access to a user's account [21], [94], allowing them to impersonate or take over the account. Throughout our study, local experts frequently mentioned account compromise—especially for social media accounts such as WhatsApp and Facebook—as a big concern for themselves and their constituents. P06 (Kenya) personally worried that *"we have hackers everywhere these days"* while P12 (Nigeria) mentioned that *"people complain to me that their social media accounts have been hacked, especially WhatsApp."*

Account compromise occurs in various ways, e.g., users forgetting to log out of public computers, inadvertently sharing one time passwords (OTPs) with attackers, or clicking on phishing links. P22 (Ghana) shared: *"Someone can guess your number and then try to log into your WhatsApp, but then you will surely receive a message and they will call you to ask you for a code. And when you mention the code to them, they get into your WhatsApp."* While experts shared ways to mitigate account compromise including not sharing OTPs or avoiding unknown links, they also mentioned that some users are unconcerned about account compromise, choosing to simply create new accounts, as elaborated by P38 (Brazil): *"The person says, okay, you hacked my social network, no problem, I'll create another account."*

Misuse of personal information. While account compromise involves unauthorized parties getting access to users' data, participants also worried about authorized parties using their data for purposes other than legitimate ones. P38 (Brazil) argued that *"there is no free lunch . . . all the applications that come for free have as a goal to watch us."* P44 (Brazil) was worried about their information being used for advertisements: *"If an app is free to . . . use, it means you're paying with your data in some way . . . They might not steal your data, but they do collect certain information and sell it to other apps."* This was echoed by P07 in Kenya, where mobile money is common: *"We mostly pay our bills using mobile phones but you find later those people whom you paid those funds they call you back like they are advertising their services . . . something that you never consented to."* While prior work in the West also notes privacy concerns, e.g., with online ads [104], [105], our results show how emerging technologies in the majority world, such as mobile money, introduce new privacy risks for users, suggesting design opportunities to improve the privacy of these technologies.

Financial scams. Financial scams are deceptive methods used to steal money from people [17]. Local experts mentioned being worried about financial scams targeting themselves and their local constituents. P54 (India) was concerned that *"a lot of scams are happening these days."* P49 (China) described two scenarios: *"In one, they've [people*

in their community] already been scammed and are stuck in an endless loop of transferring money, unsure of whether to continue. In the other, they're being blackmailed and don't know how to handle it." In most cases, social engineering [98] is used to trick victims as detailed by P06 (Kenya): *"I have a lady who was conned 2 million at Standard Chartered Bank and she was called by someone and they told her your account has some issues kindly give us your date of birth, your last transaction and the numbers they use are close to the actual numbers of the bank."*

Malware. Malware is malicious software designed to harm devices or data [87]. Because of the nature of websites they access, many local experts were concerned about viruses infecting their devices or those of people in their local communities. For instance, P69 (Türkiye) stated that they are *'interested in sports. I look at Fotomaç newspaper every day. You know, in order to look at a page there, maybe 10 or 15 advertisements come from there. Maybe you can get a virus."* This was echoed by P62 (Pakistan) for movies: *"There are websites where I usually go to watch certain shows. So I know for sure that, you know, there are a lot of things that can go wrong here, but there are no other options in Pakistan."* Similarly, P47 (China) said: *"When downloading certain apps . . . my phone's security system sometimes warns me that the app might have risks, like viruses or potential data breaches. But* ***I wonder if these warnings are accurate.*** *Despite the warnings, sometimes I have no choice but to download the app to complete a task."* Similar to prior work with refugees in the US [80] and loan app users in Kenya and India [52], [62], our results show how users de-prioritize S&P when faced with competing priorities. This is exacerbated by low socioeconomic conditions in the majority world.

Social harms. Social harms are the collective negative effects of behaviors or actions on an individual, community, or society [50]. Local experts were worried about the negative impact of access to pornography and gambling—made easy by technology—on their communities. P15 (Nigeria) worried that *"one of the things that technology has done, especially for young children, is it has made them addicted to technology and they have pornography and that sort of thing. And it has really made a lot of youths not focus on their education."* When doing repairs, P25 (Ghana) described how *"a lot of people . . . have pornography on the laptop . . . so some time you try to do back up for them [before repair] and when you go to the camera you will see things that you shouldn't see."* P58 (Pakistan) was worried that TikTok *"is mostly used to promote obscenity and vulgarity"* while P43 (Brazil) was concerned about gambling: *"I believe this is very harmful for people. It ends up taking their money."* We speculate that concerns around social harms might be more pronounced in the majority world due to collectivist values.

Intimate partner violence (IPV). IPV refers to physical or sexual abuse, stalking, and other forms of harm caused by an intimate partner [10]. Some experts recounted incidents where people in their communities had been targets of stalking via spyware and other forms of IPV. P25 (Ghana) detailed how *"most [targets] are the ladies. So what happens is that the guys will tap their WhatsApp and be reading their messages . . . one lady informed me that . . . she was beaten by her boyfriend; that she had been chatting with another man . . . So I went through the phone . . . and I asked her about many apps, but she said some were not installed by herself."* Sometimes this stalking was facilitated by device or account sharing, as elaborated by P49 (China): *"I have a friend who shares an Apple ID with his wife. Through the ID's tracking feature, she knows his every move."* While IPV has been extensively explored in the West [10], [23], [24], [25], [88], [89], [106], we note that factors like low digital literacy in the majority world make targets more vulnerable.

Image-based sexual abuse (IBSA). IBSA occurs when someone takes, shares, or threatens to share sexually explicit images or videos of another person without their consent [96]. It can take many forms, including nonconsensual distribution of consensually-created intimate content (NDII), nonconsensual creation of the images, or unsolicited sharing [60]. In our study, local experts were worried about some forms of IBSA, especially targeting women. For instance, P39 (Brazil) mentioned that *"[female] teachers, especially, were much more concerned with image leaks, with image manipulation, than men . . . because image manipulation is a relatively new threat, is much scarier to women than to men. And, of course, women are much more targeted."* P02 (Kenya) was worried about NDII: *"People who use technology for very dubious reasons to gain dubious things. We have someone who uses technology to download things like porn, part of it to sell."* P32 (Mexico) shared an incident where accounts were compromised and used to distribute images, causing emotional and physical abuse on targets: *"[Hacking] happened to a couple of young girls. One of them looked for me and told me that her Facebook profile had been hacked, they made a photomontage of her, and many people saw it, her father hit her and kicked her out of the house."* Some experts were particularly worried about how advances in AI have made it easy to create deepfakes.

Digital surveillance. Digital surveillance is the use of technology to monitor and track activities of other people [57], including their online communications, financial transactions, etc. When probed about this, local experts across all nine countries believed digital surveillance exists in their countries, and is conducted mostly by governments and tech companies. Many local experts and those they support were worried about this surveillance. For instance, P43 (Brazil) said: *"Some people do worry and are afraid of being watched. It even happens that people say something, and shortly after, they see advertisements related to what they talked about."* P36 (Mexico) added: *"There are people I have heard who believe that we are watched by the government or other non-governmental institutions and that we should be careful."*

Despite these concerns, many experts felt helpless in avoiding surveillance because they could not avoid using technology (for surveillance by tech companies) or because

the government is too powerful. Regarding the government, P67 (Türkiye) said that *"you can't really do much"* while P49 (China) added that *"in China, it's almost impossible"* to avoid surveillance. P38 (Brazil) stated that *"it's impossible to stop being watched. Because most of the applications that we are dependent on use the application as a form of surveillance. Facebook, WhatsApp, TikTok, and so on."*

4.4. Reasons for Following Advice

Overview. Local experts provided various reasons why they and those in their communities follow recommended S&P advice. While reasons including knowing benefits/risks, previous negative incidents, and simplicity of advice are consistent with previous work in the West, we find that trust between experts and users is critical in the majority world.

Understanding the benefits and risks. The most commonly cited reason for following advice was understanding both the benefits of the advice and the risks posed by not following it. For 2FA, P21 (Ghana) said that *"it is important because setting up that two-step verification, no one can hack your account."* This was echoed by P67 (Türkiye) who added that *"passwords can always be breached. But two-step verification uses your phone. It's harder to be breached."* For strong passwords, P32 (Mexico) stated that *"having a secure password is an important aspect of keeping the security and privacy of your online information."*

Trusting local experts. Previous work in the West [64] notes that users are more likely to follow advice if they trust the source. We extend this work to the majority world and show how local constituents trust advice from local experts because of the trust they have developed with the experts. This sometimes forces people to only seek help from certain experts, as P20 (Nigeria) recounted: *"I had a customer who wanted to print a personal document relating to her salary and all that, and she kept telling me that she cannot take it to any other cybercafe but mine because she trusts me."* We note that trust between users and the experts is important as local experts often access sensitive information when supporting their constituents; this has also been noted for case managers and refugees in the US [80], cybercafe managers and customers in Kenya [53], and repair shop owners and customers in India [51]. Further, this trust sometimes intersects with gender, as some users trust women experts more and consult them for sensitive transactions.

Negative incidents. Similar to prior work in the US [64], some local experts described previous negative incidents as a reason for following advice. P01 (Kenya) frequently changes their passwords due to *"the time someone used my password to borrow money on my behalf I felt humiliated and so I had to keep on changing."* P64 (Pakistan) protects their data because *"sometimes people use others' phones and start browsing their pictures, which is personal. I've seen people unlock phones, access contact numbers, and even extract numbers . . . So, I decided to secure my photos and numbers."* For P43 (Brazil), *"after having some of my social networks hacked, I started using MFA on almost all my accounts."*

Advice being simple. Lastly, some experts mentioned that people are more likely to follow recommended advice if it is simple to implement. For example, P59 (Pakistan) stated that *"people will prefer to follow simpler advice."* Similarly, P20 (Nigeria) said that people are more likely to follow their advice of generally using passwords *"because it is easy for them to follow compared to others."* Our findings support those of Redmiles et al. [64] about the need to make security imperatives simple for users to implement them.

4.5. Challenges and Contextual Factors

Finally, we discuss barriers and contextual factors that make it difficult for users to follow recommended advice.

4.5.1. Challenges to Implementing Advice.

Overview. While inconvenience has also been noted as a barrier for implementing advice in the West, we find socioeconomic factors, not knowing benefits, language barrier, and social frictions of taking protective measures as significant barriers for following advice in the majority world.

Inconvenience of implementing advice. Prior work in the US has noted inconvenience as a reason for users rejecting advice [64]. We confirm and extend these findings to the majority world, showing how such inconveniences can stem from poor connectivity or government-imposed Internet and network shutdowns in the case of 2FA. These inconveniences also lead experts to prioritize account access over security when creating passwords for their constituents. For example, P02 (Kenya) stated that *"some people still get challenges because you create a strong password for someone and someone forgets [it]."* Regarding 2FA, P59 (Pakistan) said that *"sometimes, you don't get the code when you activate two-factor authentication, or when the phone services are down in Pakistan."* These inconveniences lead to insecure practices such as reusing passwords or turning off 2FA.

Socioeconomic factors. Previous work in the West notes that users of lower socioeconomic status struggle to find information on the web [29], [30], [83], [93]. Further, these users lack access to more authoritative sources of S&P advice [64]. We extend these findings to the majority world to show how limited finances often inhibit people from implementing recommended S&P advice. P27 (Ghana) highlighted how internet costs prevent people from updating their software despite knowing the benefits: *"Most of them, I think for the Internet concerns, they are not willing to update phones because update takes a lot of Internet subscriptions . . . so most of them often frequently do not update knowing fully well the importance of these updates."* P70 (Türkiye) said that they *"do not update it [their OS] . . . for financial reasons. Since this is a cost, I don't see it necessary in Türkiye."* Similarly, P43 (Brazil) stated that *"some people*

lack the resources to get antivirus software" while P44 (Brazil) added *"they'd say, but you have to pay for antivirus, why should I get it?"* In Pakistan, P61 remarked that most people *"don't even try to spend their money on VPN. No one pays attention to safety. They want to save their money, even when it's compromising their security and privacy."* Despite discouraging their constituents from using public WI-FI, P70 (Türkiye) acknowledged that *"sometimes people may have to use public networks due to financial reasons."* These findings suggest opportunities to make S&P solutions more affordable for users in the majority world.

Performance degradation. Relatedly, some experts mentioned how following advice can degrade device performance. In particular, some experts indicated that installing anti-virus tools can slow down their resource-constrained devices, as elaborated by P37 (Mexico): *"There are antivirus software on computers that are very slow, well not very slow but they slow down the performance of the computer."* This was echoed by P40 (Brazil) who recalled *"back when I used Windows, I had Norton. Wow, man, for the love of God, that Norton took at least a third of your RAM."* Relatedly, P42 (Brazil) described how VPNs can slow down their connection: *"a VPN makes your connection much slower—five times slower, sometimes. Free VPNs often have limited speeds."*

Not knowing benefits. Another reason for not following advice was the fact that some people did not know the S&P benefits of following recommended advice. For instance, P44 (Brazil) said that *"it was common for them [people in their community] to say, oh, there's been this update notification for the past five months, and I can't get rid of it."* Similarly, P27 (Ghana) stated that *"most of these updates don't change much. So once they don't see much change after the update, they don't really see the need for updates often."* This was further complicated by the high costs of internet data, as described earlier. Similarly, P36 (Mexico) indicated that people do not use anti-virus because *"they don't know the importance or they simply don't have information about it."* P62 (Pakistan) emphasized the need to *"reject all besides the necessary cookies . . . So that I've told a lot of people, you know, all your data is going this and that, but you know, a lot of people just like, okay, whatever, we don't care!"*

Social friction due to protective behaviors. Social relations and norms in the majority world (highlighted particularly in Ghana and Pakistan) also inhibit people from following advice. For instance, P21 (Ghana) detailed how preventing people from inserting USBs into your devices can cause social friction and negative perceptions, stating that if you *"don't allow people to insert their pendrives to copy music or other kinds of things, they will just say you are being rude and arrogant."* Similarly, P29 (Ghana) described how it can be difficult not to share devices: *"The challenge is normally about our way of doing things. They feel people who need help, if you do not do it [help them], even the reason you give . . . to not share, they feel like you are denying others something."* P64 (Pakistan) narrated how it can be difficult for people in intimate relationships to protect privacy on their devices: *"Sometimes husbands even ask why you've enabled these [security] features. This also leads to issues . . . They themselves say that our family members will question why so many passwords are used."* P62 (Pakistan) added that *"I think since we live in a society where sharing a phone is very common, so . . . if they are sharing their phone a lot, and they have to share, then definitely it's not very feasible to, you know, keep putting in a password yourself every time."* We note that such tensions can dissuade people from taking S&P measures such as using a phone lock, and subsequently make them even more vulnerable to IPV via stalkerware.

Language barrier. Lastly, some experts described how some of their constituents struggle to use technology devices because they do not understand English. For instance, P54 (India) stated that *"since most of the errors are in English or not even errors, any problem alerts are in English, they do not know what is happening. Say there is some notification on the screen and they did not see what they changed or what they clicked on. For example, there is this do-not-disturb service, right? They might have clicked it, accidentally, which eventually leads to their calls being denied. Without them being notified. So stuff like that they don't understand."* Similarly, P65 (Pakistan) added that *" if it [the language on tech devices] is in English, they [people they support] don't understand at all."* This language barrier similarly extends to S&P, making it difficult for users to understand or configure appropriate privacy controls.

4.5.2. Contextual Factors.

Overview. Lastly, we saw different ways in which factors including gender identity, religion, digital literacy, infrastructural challenges, and device sharing practices shape S&P concerns, advice, and practices in the majority world.

Gender. A recent SoK found mixed results regarding the impact of gender on security behaviors in Western contexts [99]. While many quantitative studies find correlations between gender and S&P practices, they often fail to account for *why* these correlations exist. Through our qualitative study in the majority world, we find a multitude of ways in which gender identity intersects with S&P, particularly through perceived threats, barriers to resources and advice, social norms, and gendered seeking of S&P advice. For *perceived threats*, several experts mentioned that women are more vulnerable than men, especially to stalking, image-based sexual abuse, and account compromise. For instance, P27 (Ghana) stated that *"I find a lot of women falling victim to these social media hacks. So you find frequently a lady will call you that someone has hacked my WhatsApp."*

Social norms. Some of the reasons women are more concerned or vulnerable include cultural expectations to share their devices with others as well as patriarchal norms that disadvantage women, similarly noted in majority world countries like Bangladesh [85]. For instance, P10 (Kenya) said that in their rural place, *"women are not given priority*

when it comes to education and the job accessibility and opportunities and so they have little to no information."

Gendered seeking of advice. Gender also influences who people turn to for advice in the majority world. In Pakistan, women prefer to seek advice from other women, as detailed by P60: *"Since I am a girl, more women reach out to me."* In other cases, men experts are preferred for technical challenges, while women are often turned to for sensitive transactions as they are deemed more trustworthy. For instance, P03 (Kenya) said that when people's challenges *"involves some sensitive information, for example . . . their pay slips and all that information, they prefer a female [expert] . . . when it comes to the usual repairs, maybe the usual computers they would prefer a male."* P20 (Nigeria), a woman expert, said that *"even though they [people who seek help] want a male figure [to fix technical problems], I still try to make them understand that I can do this."* However, this does not always work as elaborated by P10 (Kenya): *"The place I am, the way you talk to women is not the way you talk to men . . . When talking to a man, for him to listen to you, another man has to be the one talking to him. [So it's hard to advise men because] they have this diminishing treatment when it comes to women."*

Digital literacy. When asked about common challenges in their communities, local experts overwhelmingly pointed to low digital literacy often caused by low literacy. For instance, P02 (Kenya) said that *"most of them [people in their community] are very illiterate and have very little knowledge about ICT."* This low digital literacy often amplifies other challenges, including users forgetting their logins, not understanding privacy controls, and sometimes being vulnerable to stalking. For instance, P08 (Kenya) mentioned how *"the first time someone has created [a] Facebook page or on social media and they end up posting and they might think they have posted for themselves while they have posted and so many other people are seeing it."* P25 (Ghana) described how low digital literacy can make people confuse the camera flashlight on their phones for just a flashlight, and end up unknowingly recording intimate videos of themselves: *"Sometimes the ladies, they give the phones to their children and then in an attempt to use the camera they sometimes walk around nakedly in the room . . . when there is lights out, they use the phone torchlight as a camera even if they go to the washroom . . . sometimes in an attempt to put the phone in a good place where they can get the lights they end up punching the video . . . they think they are using the camera light but they do not know that it is the video they have activated."* P25 (Ghana) added that *"some people even don't know how to delete things from their phones. When they delete, it go[es] straight to the recycle bin and they have no idea of the recycle bin."* These results show how low digital literacy can amplify S&P risks faced by users in the majority world. In fact, prior work in Kenya by Kotut et al. [44] shows that as users (especially non-literate ones) transition from feature phones to smartphones, they encounter issues using these devices, especially if they had memorized feature phone settings, forcing them to rely on other people for help.

Local experts further detailed that they vary their advice and delivery of advice depending on the target users' literacy, and especially digital literacy. For instance, P22 (Ghana) is hesitant to recommend phone locks to people with low digital literacy: *"There are some people who don't know anything at all so if you ask this people to put locks on their phone it will be a problem."* P24 (Ghana) recommends simple passwords for those with low technology skills: *"For those who don't know, I would not make the password very difficult to remember."* Some experts also mentioned not bothering to explain things to people with low literacy levels, instead directly performing the task for them, as elaborated by P58 (Pakistan): *"For uneducated people, we just do this for them. If the person is educated, we will guide him . . . and he will do it himself."* This was echoed by P54 (India): *"If the customer is not educated, then I prefer to solve the problem myself and tell them not to do anything."* Such practices further widen the digital divide between users.

Infrastructural challenges. Local experts further described various infrastructural challenges that amplify S&P challenges and concerns in the majority world. Many experts pointed to poor networks and a lack of access to electricity and personal devices that necessitate their constituents to devise workarounds. For instance, P21 (Ghana) stated that *"people that do not have access to electricity come here to charge their phones."* If these devices are not adequately protected, e.g., via a PIN, users' information could be accessed at these stations, as confirmed by a recent study in rural Ghana [90]. According to P32 (Mexico), *"the limited access to technology is due to the poverty that prevails in the P'urhépecha area; a good part of the indigenous population does not have a computer, internet or other technological devices at home."* These infrastructural challenges often disproportionately affect rural [90] and indigenous communities, leading to what McClearn et al. refer to as "infrastructuring" [48], i.e., practices such as device sharing and reliance on intermediaries for technology access and use. Due to the S&P tensions they introduce, users often resort to "patchworking" practices to protect their everyday security [48].

Device sharing practices. Another common theme in our study was device and account sharing. Local experts provided various contexts why they and their constituents share devices and accounts, including at workplaces and at home with trusted ones. P35 (Mexico) explained how device sharing is common in Mexico due to economic constraints: *"Sometimes there is only one device in a single family or worked by a team [adults, young people, and children]. Well, you have to do it on a single computer here. Here, a computer is shared by several people."* P66 (Türkiye) described how sharing is encouraged by their religion: *"If someone in the neighborhood has one [product], that is, if a man who has the means [to] buy it, the neighbors in the neighborhood can borrow it and benefit from it. This is also seen as good from a religious point of view."* However, device sharing can lead people to think they have been "hacked" when their accounts are accessed. In some cases, trust when sharing

accounts and devices can be abused, as elaborated by P44 (Brazil): *"The most common issue was with bank passwords. They'd usually share them with other people, like close relatives. Unfortunately, every family has at least one person who's a bit untrustworthy. These people would then make transfers using their name."* We note that these device and account sharing practices routinely lead to privacy tensions, as similarly noted in previous work [74], [91].

Religion. Religion also influences tech usage and S&P concerns in the majority world. Some experts described how religion can turn people away from technology, with P19 (Nigeria) stating that *"Muslims don't have time and they feel most of the things on the Internet are not morally right."* Some experts mentioned being cautious about the advice they give in relation to the advisee's religion. In Türkiye, photo-sharing on social media can be problematic due to religious beliefs as elaborated by P66: *"We had a lot of discussions about . . . whether it is right or permissible to share the picture of your wife, the picture of your daughter or the picture of your son . . . it doesn't matter in the end, if you take and share a picture of your wife, your wife's picture in a home environment that people can't normally see, it zooms in much closer. I mean, it counts your eyebrows, eyes, eyelashes. Is this permissible? It is not . . . It is like this in terms of privacy. In fact, it is also religiously impermissible."* In Pakistan, P59 expressed concern at the Internet blockage during religious holidays: *"My main concern is that the social media platforms should not be blocked at any time. For example, social media gets blocked during Muharram . . . it is harmful not only for our work, but for everyone."*

5. Discussion and Conclusion

In this study, we explored S&P advice prioritized by local experts (n=70) across nine majority world countries. While local experts' advice for their constituents largely matches advice for their own S&P and advice from the West, we surface various significant barriers to advice implementation in the majority world, including economic constraints, language barriers, and social frictions that can be caused by taking protective S&P measures.

In this section, we reflect on our findings and share recommendations to better support majority world users. We also share lessons for researchers looking to do similar work.

5.1. Main Takeaways

Advice in the majority world is mostly similar to the West. Previous research conducted mostly with Western participants finds that the web [67], social media [5], [8], [20], [79], [100], entertainment media [27], and friends and family [28], [33], [35], [56] are common sources of S&P advice. We confirm these findings in the majority world. In addition, we find that people in the majority world frequently turn to local experts for advice, with some local experts mentioning they run groups on social media platforms such as WhatsApp and Facebook to disseminate advice. Regarding the advice content, we similarly find that the advice provided (including the use of strong passwords and two-factor authentication) by local experts largely matches advice from the West [37], [67], with advice prioritization challenges [67] similarly extending to the majority world. However, we also noticed some differences. For example, some experts advise their constituents to use memorable passwords likely because their constituents often forget complex passwords. Others advise their constituents to only consult trusted experts. Collectively, these results suggest that recommendations made by previous work in the West around advice prioritization [67] may also be applicable in the majority world. However, without considering the context of the majority world, any such recommendations are likely to fail, and we discuss next why and how advice from the West fails in the majority world.

Western advice fails elsewhere for various reasons. While we also find that the trustworthiness of advice [66], convenience [2], [22], past negative incidents [64], and simplicity of advice [64] are critical for implementing advice, we surface factors that make it difficult for users in the majority world to implement advice. For example, our study shows how economic constraints and social frictions that arise because of protective S&P practices such as using passwords, inhibit people from following advice. Regular software updates are impractical for some users because of internet costs, while collectivist cultures compel people to share their devices, making it difficult for users to protect their privacy. Despite advising their constituents to use genuine software, some experts decried how people are unable to afford it, turning to pirated and potentially harmful software. Similarly, other experts mentioned how it is impractical for users to use the often resource-intensive anti-virus tools on their resource-constrained devices. In rural areas, SMS-based two-factor authentication sometimes fails due to poor connectivity. Overall, these results suggest the need for more consideration of users in resource-constrained settings in both the design and deployment of tech and S&P solutions.

Many concerns around account "hacking". Throughout our study, one frequently cited concern was account compromise (otherwise described as hacking by many local experts). Local experts recounted various incidents where their own accounts as well as those of other people in their communities had been compromised and taken over. The compromised accounts ranged from social media accounts including Facebook to social messaging apps such as WhatsApp. While the experts described this as hacking, we noted that these "hacks" often involved simple techniques. For instance, several experts detailed how people easily get tricked into giving away one-time authentication codes or clicking on unsuspecting links, resulting in their accounts getting compromised. Device sharing practices can also lead to inadvertent access by users who share the same device. In fact, a recent study focusing on cybercafes in Kenya [53] highlighted how some cybercafe operators encourage their customers to save their passwords in the public computers at the cafes to avoid forgetting them. However, this can result in unauthorized access to

user accounts by other cybercafe customers. These concerns point to a need for more educational interventions as well as redesigning technology and S&P tools to better serve device sharing contexts that remain prevalent in the majority world.

Low literacy amplifies S&P risks. Our study shows how low digital literacy in the majority world can particularly complicate security and privacy for users. While English is often the de facto language on tech devices and platforms, low-literate users in the majority world often do not understand English, making it challenging for them to even configure appropriate S&P settings. For example, local experts detailed how some users do not understand device update nudges presented in English, turning to the experts to help them to *dismiss* these nudges. Other experts mentioned that some users fail to understand privacy settings and configuration on social networks such as Facebook, leading them to overshare their data. Low literacy also seemed to directly connect with low digital literacy, with experts sharing how low digital literacy makes their constituents vulnerable to risks of being stalked. For example, the ability to log onto multiple WhatsApp accounts on one device can allow attackers to stalk others, especially if the victims do not understand how to check other devices they are logged to. These results suggest opportunities for better language translation for technology and prominent UI features that can provide users with better visibility and transparency into their S&P configurations.

5.2. Next Steps

Prioritizing advice in the majority world. In a previous study focusing on the US, Redmiles et al. [67] noted that there are too many security imperatives on the web, making it difficult for users to prioritize advice. The study recommends the prioritization of a few high-impact pieces of advice for end users. In our study focusing on the majority world, we similarly find a wide variety of S&P advice provided by local experts to users. Similar to Redmiles et al., we note that this plethora of advice makes it almost impossible for users to follow all these pieces of advice. Thus, future work can evaluate the efficacy and applicability of S&P advice from our work and prior work [64], [66], [67] against the threat models and possible adversaries in the majority world with the goal of prioritizing the most practical and highest impact advice for users in various majority world contexts. For example, in shared device contexts, advice such as logging out of accounts after use might arguably be more useful and practical than the use of strong passwords.

Better translation to local languages. Language barrier remains a significant challenge for users in the majority world when using technology, presenting opportunities for better translation from English to local languages. While smartphone brands like Android and Apple allow users to switch languages, these translations are often incomplete, leaving many menus and interfaces in English. Recent advances in AI could be used by tech designers to aid translations to local languages. However, many majority world countries have several local languages, and thus, it's impractical to immediately translate to all these languages. Nevertheless, proper translation to just the official languages would be a good start. Beyond devices, there is also potential to curate S&P advice in local languages, ensuring users can better understand and implement important S&P advice. As shared by some local experts, public gatherings offer a great avenue to disseminate S&P advice. However, adequate care must be taken when doing these translations as S&P terms can vary across languages and cultures. Thus, it is crucial to directly work with local communities to account for these nuances during the translation and dissemination of advice.

Designing tech and S&P for diverse contexts. Our study underscores the importance for designers to consider diverse contexts in the majority world when designing technology and S&P features. For example, password managers could greatly benefit from redesigns that accommodate multiple user profiles, each protected by user-specific vault passwords, to better support device-sharing contexts. This could also be beneficial for experts who manage passwords for other users, e.g., at public computing facilities. Additionally, clearer information about file deletion is needed; while iOS notifies users that deleted items remain in the recycle bin for 30 days, some Android devices do not, leading to misconceptions that deleted files are permanently removed. Nudging users about items in the recycle bin could address this. Similarly, nudges could enhance security in apps like WhatsApp by periodically notifying users of all devices and locations where they are logged in to alert users about potential stalking. For these designs and interventions to be effective, however, we recommend more research with the target users.

Making tech and S&P solutions more affordable. In our study, local experts mentioned that pirated software is commonly used by their constituents, despite their advice against using it. To discourage the use of this potentially harmful software, companies should make authentic solutions affordable. As economic conditions vary across countries, uniform pricing may be less accessible to users in low-income regions, prompting them to turn to pirated software. Instead, we argue that equitable pricing models, such as adjusting for purchasing power parity [70], could improve affordability and encourage the use of genuine and safer software.

5.3. Other Thoughts and Future Work

Lessons for the West from the majority world. Our results from the majority world show that local experts prioritize usability, affordability, and account access over strictly recommending what may be considered security best practices in Western contexts. Even measures they personally adopt, including software updates and the use of VPNs, are not recommended by experts to their constituents if they perceive them to be too costly or complex given the infrastructural and economic realities of their constituents. Local experts additionally emphasize trust and communal approaches to S&P, encouraging their constituents to use

trusted devices or consult trusted experts only, especially when conducting sensitive transactions. While they have limitations, we believe some of these practices can inform the design of S&P solutions that are useful not just in the majority world but also in Western contexts. For instance, making security solutions such as anti-virus less resource-intensive, and genuine software more affordable can also be helpful in Western contexts, especially among low-income groups. Communal approaches to technology access and S&P, especially in contexts where trust is essential, are also relevant in settings such as public libraries in the West [19], [46], or between refugees and their case managers [80]. Thus, designing S&P tools suited to these contexts in the majority world will likely be beneficial even in Western contexts.

Future work. Our study surfaced how contextual factors—ranging from gender, religion to infrastructural challenges and device sharing practices—shape both S&P concerns and advice. Given that S&P practices can be directly affected by local laws, political regimes, and regulations, future ethnographic work can explore more closely how these factors shape concerns and advice in the majority world, potentially developing a framework to theorize this relationship.

5.4. Study Reflections

Throughout this study, we made deliberate efforts to involve local communities in this work, ranging from recruitment to data collection, analysis, and paper writing. While this extended the timelines of the project, e.g., because we had to train some local contacts on research, our contacts provided invaluable contributions. They enriched our analysis with a lot of nuances and context that would otherwise have been impossible to capture. We left it up to our contacts to decide their level of involvement, offering various compensation options from payment to authorship and/or both. For payments, we took advantage of platforms including Wise and Remitly to wire payments to our contacts.

For other researchers looking to do similar work, we encourage them to involve local communities to ensure (a) the research benefits directly extend to local communities, and (b) local context is appropriately respected. While it might be easier and more convenient to use panel providers, we argue that the context and insights provided by local collaborators justify the efforts to involve them. We found it somewhat easier to contact local contacts by tapping into our own academic and personal contacts, an approach that could be beneficial for others looking to replicate our methods.

However, we also faced a few challenges. First, this project spanned multiple years because of all the logistics involved in navigating IRB processes, finding the right in-community contacts, handling translations, etc. It was also challenging to coordinate the project across multiple time zones. For others looking to do similar work, we suggest blocking out enough time (in the count of years) and having alternative countries in case others fail to materialize.

Acknowledgments

We thank Siying Hu, Pardis Emami-Naeini, Iman Alipour, Iman Mohammadi, Esdras Lins Bispo Junior, Amarildo Moreira Jr, Peter Mwangi, Daniel Omeiza, Abraham Mhaidli, Julio Poveda, David Cortes, Cristina Sánchez Osorio, Ofelia Lopez Mejia, Viridiana Camacho, Rob Reeder, and Lucy Simko for their help. We also thank the EAAMO working group on Equity and Justice for Indigenous Communities in the Americas (EJUCIAM) for their assistance in Mexico, as well as everyone that attended talks, asked questions, and provided feedback on this research. We are also grateful to the anonymous reviewers for their feedback, and all participants for their time and invaluable insights. This research was funded in part by the Stanford Internet Observatory, the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972, and the US National Science Foundation under Grant Number 1845300. Collins Munyendo was additionally supported by a Google PhD Fellowship.

References

[1] Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, MA Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. We Don't Give a Second Thought Before Providing Our Information: Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh. In *Proc. COMPASS*, 2020.

[2] Elham Al Qahtani, Yousra Javed, Heather Lipford, and Mohamed Shehab. Do Women in Conservative Societies (Not) Follow Smartphone Security Advice? A Case Study of Saudi Arabia and Pakistan. In *Proc. EuroS&PW*, 2020.

[3] Tom L Beauchamp et al. The Belmont Report. *The Oxford textbook of clinical research ethics*, pages 149–155, 2008.

[4] Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5):313–324, 2004.

[5] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. "Adulthood is trying each of the same six passwords that you use for everything": The Scarcity and Ambiguity of Security Advice on Social Media. In *Proc. CSCW*, 2022.

[6] Nicola J. Bidwell. Women and the Sustainability of Rural Community Networks in the Global South. In *Proc. ICTD*, 2020.

[7] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. When the Internet Goes Down in Bangladesh. In *Proc. CSCW*, 2017.

[8] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *Proc. CHI*, 2021.

[9] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Proc. SOUPS*, 2019.

[10] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The Spyware Used in Intimate Partner Violence. In *Proc. IEEE S&P*, 2018.

[11] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, 11(3):395–416, 2009.

[12] Deborah Cohen and Benjamin Crabtree. Qualitative research guidelines project, Jul 2006. http://www.qualres.org/.

[13] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In *Proc. CHI*, 2018.

[14] Kovila PL Coopamootoo and Magdalene Ng. "Un-Equal Online Safety?" A Gender Analysis of Security and Privacy Protection Advice and Behaviour Patterns. In *Proc. USENIX Security*, 2023.

[15] Sadie Creese, William H Dutton, and Patricia Esteve-González. The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and ubiquitous computing*, 25(5):941–955, 2021.

[16] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. Defensive Technology Use by Political Activists During the Sudanese Revolution. In *Proc. IEEE S&P*, 2021.

[17] Martynas Damulis. Investigations of Financial Fraud: Literature Analysis of Selected Financial Scams. *Theory and Practice of Illegitimate Finance*, pages 203–221, 2023.

[18] DataReportal. Digital 2023: Pakistan. https://datareportal.com/reports/digital-2023-pakistan, 2023.

[19] Samuel Dooley, Michael Rosenberg, Elliott Sloate, Sungbok Shin, and Michelle Mazurek. Libraries' Approaches to the Security of Public Computers. In *Proc. WIPS*, 2020.

[20] Paul Dunphy, Vasilis Vlachokyriakos, Anja Thieme, James Nicholson, John McCarthy, and Patrick Olivier. Social Media As a Resource for Understanding Security Experiences: A Qualitative Analysis of #Password Tweets. In *Proc. SOUPS*, 2015.

[21] Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Towards Detecting Compromised Accounts on Social Networks. *IEEE Transactions on Dependable and Secure Computing*, 14(4):447–460, 2015.

[22] Michael Fagan and Mohammad Maifi Hasan Khan. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. In *Proc. SOUPS*, 2016.

[23] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[24] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A Stalker's Paradise"': How Intimate Partner Abusers Exploit Technology. In *Proc. CHI*, 2018.

[25] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), 2017.

[26] Freedom House. Freedom on the net: Scores by country. https://freedomhouse.org/countries/freedom-net/scores, 2024.

[27] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. The Effect of Entertainment Media on Mental Models of Computer Security. In *Proc. SOUPS*, 2019.

[28] Susanne Furman, Mary Frances Theofanos, Yee-Yin Choong, and Brian Stanton. Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy*, 10(2):40–49, 2011.

[29] Eszter Hargittai. Second-level digital divide: Differences in people's online skills. *First Monday*, 7(4), 2002.

[30] Eszter Hargittai. The Digital Divide and What To Do About It. *New economy handbook*, 2003:821–839, 2003.

[31] Ayako A Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. How WEIRD is Usable Privacy and Security Research? In *Proc. USENIX Security*, 2024.

[32] Sumair Ijaz Hashmi, Rimsha Sarfaraz, Lea Gröber, Mobin Javed, and Katharina Krombholz. Understanding the Security Advice Mechanisms of Low Socioeconomic Pakistanis. In *Proc. CHI*, 2025.

[33] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. Digital Security—A Question of Perspective A Large-Scale Telephone Survey with Four At-Risk User Groups. In *Proc. IEEE S&P*, 2024.

[34] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. A World Full of Privacy and Security (Mis)Conceptions? Findings of a Representative Survey in 12 Countries. In *Proc. CHI*, 2023.

[35] Franziska Herbert, Collins W Munyendo, Jonas Hielscher, Steffen Becker, and Yixin Zou. Digital Security Perceptions and Practices Around the World: A WEIRD versus Non-WEIRD Comparison. In *Proc. USENIX Security*, 2025.

[36] Faheem Hussain, Abdullah Hasan Safir, Dina Sabie, Zulkarin Jahangir, and Syed Ishtiaque Ahmed. Infrastructuring Hope: Solidarity, Leadership, Negotiation, and ICT among the Rohingya Refugees in Bangladesh. In *Proc. ICTD*, 2020.

[37] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Proc. SOUPS*, 2015.

[38] Aarti Israni, Nicole B Ellison, and Tawanna R Dillahunt. 'a library of people' online resource-seeking in low-income communities. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–28, 2021.

[39] Margaret C. Jack, Pang Sovannaroth, and Nicola Dell. "Privacy is Not a Concept, but a Way of Dealing with Life": Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[40] Rikke Bjerg Jensen, Lizzie Coles-Kemp, Nicola Wendt, and Makayla Lewis. Digital Liminalities: Understanding Isolated Communities on the Edge. In *Proc. CHI*, 2020.

[41] Anne Jonas, Stefani Vargas, and Jean Hardy. 'Better than Google': Information Activism for LGBTQ+ Young Adults in a Rural Community. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW2), November 2024.

[42] Anastassija Kostan, Sara Olschar, Lucy Simko, and Yasemin Acar. Exploring digital security and privacy in relative poverty in Germany through qualitative interviews. In *Proc. USENIX Security*, 2024.

[43] Lindah Kotut. Terms and Conditions (Do Not) Apply: Understanding Exploitation Disparities in Design of Mobile-Based Financial Services. In *Proc. AfriCHI*, 2025.

[44] Lindah Kotut and Hummd Alikhan. "Things on the Ground are Different"': Utility, Survival and Ethics in Multi-Device Ownership and Smartphone Sharing Contexts. In *Proc. CHI*, 2024.

[45] Neha Kumar, Waylon Brunette, Nicola Dell, Trevor Perrier, Beth Kolko, Gaetano Borriello, and Richard Anderson. Understanding sociotechnical implications of mobile health deployments in india, kenya, and zimbabwe. *Information Technologies & International Development*, 11(4):pp–17, 2015.

[46] Alan F. Luo, Noel Warford, Samuel Dooley, Rachel Greenstadt, Michelle L. Mazurek, and Nora McDonald. How Library IT Staff Navigate Privacy and Security Challenges and Responsibilities. In *Proc. USENIX Security*, 2023.

[47] MAXQDA. https://www.maxqda.com/, 2024.

[48] Jessica Mcclearn, Rikke Bjerg Jensen, and Reem Talhouk. Security Patchworking in Lebanon: Infrastructuring Across Failing Infrastructures. *Proc. ACM on Human-Computer Interaction*, 8(CSCW1), 2024.

[49] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[50] Mohammad Basir Moqemi. The Interplay Between Social Harm and Education: Toward Preventing Societal Detriment. *Sprin Journal of Arts, Humanities and Social Sciences*, 2(12):82–90, 2023.

[51] Deepthi Mungara, Harshini Sri Ramulu, and Yasemin Acar. Security and Privacy Advice for UPI Users in India. In *Proc. USENIX Security*, 2025.

[52] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In *Proc. IEEE S&P*, 2022.

[53] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *Proc. IEEE S&P*, 2023.

[54] Collins W. Munyendo, Kentrell Owens, Faith Strong, Shaoqi Wang, Adam J. Aviv, Tadayoshi Kohno, and Franziska Roesner. "You Have to Ignore the Dangers": User Perceptions of the Security and Privacy Benefits of WhatsApp Mods. In *Proc. IEEE S&P*, 2025.

[55] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. In *Proc. CHI*, 2021.

[56] James Nicholson, Lynne Coventry, and Pamela Briggs. "If It's Important It Will Be A Headline"': Cybersecurity Information Seeking in Older Adults. In *Proc. CHI*, 2019.

[57] Anri Nishnianidze. Surveillance in the Digital Age. *ESI Preprints*, 24:80–80, 2023.

[58] Anna-Marie Ortloff, Jenny Tang, Arthi Arumugam, Daniel Huschina, Lisa Geierhaas, Florin Martius, Luisa Jansen, Kolja von der Twer, Lilly Jungbluth, and Matthew Smith. Replication: "no one can hack my mind"' - 10 years later: An update and outlook on experts' and non-experts' security practices and advice. In *Proc. SOUPS*, 2025.

[59] Aswati Panicker, Novia Nurain, Zaidat Ibrahim, Chun-Han Wang, Seung Wan Ha, Yuxing Wu, Kay Connelly, Katie A Siek, and Chia-Fang Chung. Understanding fraudulence in online qualitative studies: From the researcher's perspective. In *Proc. CHI*, 2024.

[60] Lucy Qin, Vaughn Hamilton, Sharon Wang, Yigit Aydinalp, Marin Scarlett, and Elissa M Redmiles. "Did They {F*** ing} Consent to That?": Safer Digital Intimacy via Proactive Protection Against {Image-Based} Sexual Abuse. In *Proc. USENIX Security*, 2024.

[61] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proc. SOUPS*, 2012.

[62] Divya Ramesh, Vaishnav Kameswaran, Ding Wang, and Nithya Sambasivan. How Platform-User Power Relations Shape Algorithmic Accountability: A Case Study of Instant Loan Platforms and Financially Stressed Users in India. In *Proc. FACCT*, 2022.

[63] Elissa M Redmiles. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *Proc. IEEE S&P*, 2019.

[64] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proc. CCS*, 2016.

[65] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. In *Proc. CHI*, 2017.

[66] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *Proc. IEEE S&P*, 2016.

[67] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *Proc. USENIX Security*, 2020.

[68] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security & Privacy*, 15(5):55–64, 2017.

[69] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp. In *Proc. USENIX Security*, 2020.

[70] World Population Review. Purchasing Power Parity by Country 2024. https://worldpopulationreview.com/country-rankings/purchasing-power-parity-by-country, 2024.

[71] Anna Lena Rotthaler, Harshini Sri Ramulu, Lucy Simko, Sascha Fahl, and Yasemin Acar. It's time. Time for digital security.": An End User Study on Actionable Security and Privacy Advice. In *Proc. IEEE S&P*, 2025.

[72] Dina Sabie and Syed Ishtiaque Ahmed. Moving into a technology land: exploring the challenges for the refugees in Canada in accessing its computerized infrastructures. In *Proc. COMPASS*, 2019.

[73] Kavous Salehzadeh Niksirat, Collins W Munyendo, Onicio Batista Leal Neto, Muswagha Katya, Cyrille Kouassi, Kevin Ochieng, Angoa Georgina, Bernard Olayo, Jean-Philippe Barras, Ciro Cattuto, et al. Reimagining Wearable-Based Digital Contact Tracing: Insights from Kenya and Côte d'Ivoire. In *Proc. CHI*, 2025.

[74] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proc. SOUPS*, 2018.

[75] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. Intermediated technology use in developing communities. In *Proc. CHI*, 2010.

[76] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proc. CHI*, 2017.

[77] Juliane Schmüser, Noah Wöhler, Harshini Sri Ramulu, Christian Stransky, Dominik Wermke, Sascha Fahl, and Yasemin Acar. Analyzing Security and Privacy Advice During the 2022 Russian Invasion of Ukraine on Twitter. In *Proc. CHI*, 2024.

[78] Sarita Schoenebeck, Amna Batool, Giang Do, Sylvia Darling, Gabriel Grill, Daricia Wilkinson, Mehtab Khan, Kentaro Toyama, and Louise Ashwell. Online Harassment in Majority Contexts: Examining Harms and Remedies across Countries. In *Proc. CHI*, 2023.

[79] Lucy Simko, Adryana Hutchinson, Alvin Isaac, Evan Fries, Micah Sherr, and Adam J. Aviv. "Modern problems require modern solutions"': Community-Developed Techniques for Online Exam Proctoring Evasion. In *Proc. CCS*, 2024.

[80] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer Security and Privacy for Refugees in the United States. In *Proc. IEEE S&P*, 2018.

[81] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "They Look at Vulnerability and Use That to Abuse You"': Participatory Threat Modelling with Migrant Domestic Workers. In *Proc. USENIX Security*, 2022.

[82] Karen Sowon, Collins W Munyendo, Lily Klucinec, Eunice Maingi, Gerald Suleh, Lorrie Faith Cranor, Giulia Fanti, Conrad Tucker, and Assane Gueye. Design and Evaluation of Privacy-Preserving Protocols for Agent-Facilitated Mobile Money Services in Kenya. In *Proc. SOUPS 2025*, 2025.

[83] Laura D Stanley. Beyond access: Psychosocial barriers to computer literacy. *The Information Society*, 19(5):407–416, 2003.

[84] Statista. Smartphone penetration worldwide by country. https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/, 2022.

[85] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. Design Within a Patriarchal Society: Opportunities and Challenges in Designing for Rural Women in Bangladesh. In *Proc. CHI*, 2018.

[86] Sharifa Sultana, Ilan Mandel, Shaid Hasan, S.M.Raihanul Alam, Khandaker Reaz Mahmud, Zinnat Sultana, and Syed Ishtiaque Ahmed. Opaque Obstacles: The Role of Stigma, Rumor, and Superstition in Limiting Women's Access to Computing in Rural Bangladesh. In *Proc. COMPASS*, 2021.

[87] Rabia Tahir. A Study on Malware and Malware Detection Techniques. *International Journal of Education and Management Engineering*, 8(2):20, 2018.

[88] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *Proc. USENIX Security*, 2020.

[89] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. Care Infrastructures for Digital Security in Intimate Partner Violence. In *Proc. CHI*, 2022.

[90] Emmanuel Tweneboah, Collins W Munyendo, and Yixin Zou. "No, I Can't Be a Security Personnel on Your Phone"': Security and Privacy Threats From Sharing Infrastructure in Rural Ghana. In *Proc. USENIX Security*, 2025.

[91] Rebecca Umbach, Anubha Singh, and Ashley Walker. "Your Protection is in Your Hands Only"': User Awareness and Adoption of Privacy and Security Practices in Five Majority World Countries. *Journal of Online Trust and Safety*, 2(1), 2023.

[92] United Nations Development Programme. Gender inequality index (gii). https://hdr.undp.org/data-center/thematic-composite-indices/gender-inequality-index/indicies/GII, 2024.

[93] Jan Van Dijk and Kenneth Hacker. The digital divide as a complex and dynamic phenomenon. *The information society*, 19(4):315–326, 2003.

[94] Courtland VanDam, Jiliang Tang, and Pang-Ning Tan. Understanding Compromised Accounts on Twitter. In *Proc. WI*, 2017.

[95] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining Security and Privacy Research in Developing Regions. In *Proc. COMPASS*, 2018.

[96] Victim Support. Image-based sexual abuse. https://www.victimsupport.org.uk/crime-info/types-crime/image-based-sexual-abuse/, 2025.

[97] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. "I Knew It Was Too Good to Be True"' The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–25, 2018.

[98] Zuoguang Wang, Limin Sun, and Hongsong Zhu. Defining Social Engineering in Cybersecurity. *IEEE Access*, 8:85094–85115, 2020.

[99] Miranda Wei, Jaron Mink, Yael Eiger, Tadayoshi Kohno, Elissa M Redmiles, and Franziska Roesner. SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors. In *Proc. USENIX Security*, 2024.

[100] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships. In *Proc. SOUPS*, 2022.

[101] Nicola Wendt, Rikke Bjerg Jensen, and Lizzie Coles-Kemp. Civic Empowerment through Digitalisation: The Case of Greenlandic Women. In *Proc. CHI*, 2020.

[102] World Bank. Individuals using the internet (% of population). https://data.worldbank.org/indicator/IT.NET.USER.ZS, 2024.

[103] Worldometer. Population by country (2024). https://www.worldometers.info/world-population/population-by-country, 2024.

[104] Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. What Makes a "Bad"' Ad? User Perceptions of Problematic Online Advertising. In *Proc. CHI*, 2021.

[105] Eric Zeng, Xiaoyuan Wu, Emily N Ertmann, Lily Huang, Danielle F Johnson, Anusha T Mehendale, Brandon T Tang, Karolina Zhukoff, Michael Adjei-Poku, Lujo Bauer, et al. Measuring Risks to Users' Health Privacy Posed by Third-Party Web Tracking and Targeted Advertising. In *Proc. CHI*, 2025.

[106] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *Proc. USENIX Security*, 2021.

Appendix A. Interview Script

Local Experts' Background

Q1 Please tell me a little bit about yourself and what you do.

Q2 Can you briefly describe the area you live in in [country x]?
- a) Is it rural or urban?

Q3 What is your experience with technology?
- a) How did you get started with technology?

Q4 Are there any general challenges around technology and/or its use in [country x] that you are aware of? Please elaborate.

Q5 What type of support do you provide people with their technology challenges or needs in [country x]?
- a) How would you characterize the people who come to you? [Prompts: axes of interest e.g., ethnicity/minority group; gender; location i.e. rural or urban; resource background]
- b) How do people get to know about you or come to find you?
- c) Why do you think they specifically come to you?
- d) What is the biggest challenge that most people you support face?
- e) What advice/support do you provide them to resolve them?
- f) Are these challenges always resolved? Which ones are hard?

Q6 What other sources do people in your area/country/community use to obtain technology support?

Experts' Personal Concerns

Q7 Personally, do you have any concerns relating to technology or how you use technology in general? Please elaborate.
- a) What factors do you think influence these concerns? Prompts: Type of technology you use, where you access the technology from etc.
- b) Do any of these concerns specifically relate to security and privacy?
- c) How do you handle these concerns?

Concerns of Others

Q8 What concerns relating to the usage of technology do people from your community or [country x] come to you with? Please elaborate.
- a) Why do you think they have these concerns?
- b) Have you noticed any patterns in terms of the types of people who express certain concerns more than others e.g, do older people tend to have different concerns than younger people? Gender?
- c) Are there other concerns people come to you, e.g., about S&P?
- d) How do you handle (or help them handle) these concerns?

Security and Privacy Advice

Q9 What are the 3 top things you do (or would do) to protect your digital security and privacy?
For each piece of advice:
- a) Where did you learn about this advice?
- b) Do you follow this advice?
- c) Have you faced any challenges following this advice? Elaborate.

Q10 Have you provided any advice to those in your local community or [country x] to protect their digital security and privacy?
If yes:

a) What are the top 3 pieces of advice you have provided to those you support in your local community or in [country x] to protect their security and privacy?
For each piece of advice:
i) Where did you learn about this piece of advice?
ii) Why do you think this advice is important for these users?
iii) What challenges do people face in following this advice?
iv) Do you vary this advice based on the target users? Prompts: different identities, skills, resources etc. Please elaborate

If no:

a) What are the top 3 pieces of advice you would give to those you support in your local community or in [country x] to protect their security and privacy?
For each piece of advice:
i) Where did you learn about this piece of advice?
ii) Why do you think this advice is important for these users?
iii) What challenges do you think people would face in following this advice?
iv) Would you vary this advice based on the target users? Prompts: different identities, skills, resources etc. Please elaborate.

Q11 Is there any advice you would love to give but cannot provide? Why?

Q12 What advice do you think people are most likely to follow? Why?
Q13 What gaps or opportunities for improvement do you see for security and privacy advice in your local community or [country x]? Elaborate.

Experts' Tech and S&P Practices
Q14 Personally, how do you most frequently access the Internet?
Q15 What are the technologies, devices or services that you regularly use? Prompts: smartphone, computer, social media, mobile money etc.
a) In what contexts/for what purposes do you use these devices or services? For example at work or at home?
b) Do you share any of these devices or services? With whom, why?
c) Do you have any concerns about other people having access to these devices or services? Why or why not?

Q16 For the mentioned devices, do you have any standard S&P practices?

a) How often do you update your OS? Why or why not?
b) Do you use any antivirus software? Why or why not?
c) How do you generally select and manage passwords across different websites? Do you use any password managers?
d) Do you use multifactor authentication for any sites?
e) Do you use any password/PIN/pattern on your devices?

Tech and S&P Practices of Others
Q17 For the people you assist (or have assisted), how do they mostly access the Internet (if they do)?
a) Do they face any challenges with this?
b) Do any of them use public computers? For what purposes?

Q18 For the people that you most frequently support, what technologies, devices or services do they regularly use? Prompts: smartphones, computers, social media, mobile money etc.
a) In what contexts/for what purposes do you think they mostly use these devices or services?
b) Do you know if they share these devices or services? Why?

Q19 Are you aware of any standard security and privacy practices that these users may have for these devices or services?
a) How often do they update their devices' OS? Why or why not?
b) Do they use any antivirus on their devices? Why or why not?
c) How do they generally select and manage passwords across different sites? Do they use any password managers?
d) Do they use multifactor authentication for any sites? Why?

Other Tech and S&P Challenges
Q20 Are any services in [country x], e.g., government services, digitized?
a) Please provide examples of these services.
b) How do you personally access these services?
c) How do most people (e.g., those you support) access these services?
d) What are some challenges people face in accessing these services?

Q21 Are you aware of any scams or phishing schemes in [country x]?
a) Please provide examples.
b) Have you (or anyone you know or assist) fallen for these?
c) How can users in [country x] protect themselves from these scams? Have you provided this advice to any users?

Q22 Do you feel digitally surveilled in [country x]? Please elaborate.
a) Who is responsible for this surveillance?
b) Are people (including those you support) concerned about this?
c) Do you use any techniques to protect yourself?
d) What advice (if any) would you give to other users to (potentially) protect themselves with regards to the stated surveillance?

Q23 Are any sites, apps or platforms banned or blocked in [country x]?
a) Please provide examples of these sites or platforms.
b) Who has blocked these services?
c) What workarounds are people (including those you support) using?
d) Are you personally using any workarounds?

Other Contextual Factors
Q24 Do you vary the advice or support you provide to people based on any of the following factors? Please elaborate on why or why not. [Prompts: Gender, religion, age, type of job, any other]

Demographic Questions
D1 What is your age?
D2 What is your gender?
D3 What is the highest level of education you have already attained?
D4 Do you have a background in IT or computers as part of your work experience or school? Please elaborate.
D5 What is your occupation/profession?
D6 Do you have any feedback or questions about this interview?

Appendix B. Additional Figures

TABLE 1: Factors that we considered in selecting countries. For internet freedom scores, 0% means the least free while 100% means the most free. For the gender inequality index, 0 means the most equal while 1 means the most unequal.

Code	Country	Region	Population Size [103]	Internet Penetration [18], [102]	Smartphone Ownership [84]	Internet Freedom [26]	Gender Inequality [92]
KE	Kenya	East Africa	56.4M	29%	53%	68%	0.506
NG	Nigeria	West Africa	232.7M	55%	38%	57%	0.680
GH	Ghana	West Africa	34.4M	68%	50%	65%	0.512
MX	Mexico	Latin America	130.9M	76%	62%	61%	0.309
BR	Brazil	Latin America	212.0M	81%	67%	65%	0.390
CN	China	East Asia	1.419B	88%	72%	10%	0.168
IN	India	South Asia	1.450B	46%	47%	51%	0.490
PK	Pakistan	South Asia	251.3M	21%	31%	26%	0.534
TR	Türkiye	Middle East	87.5M	81%	75%	32%	0.638

TABLE 2: Demographics of the local experts in our study. An underscore (_) means participants preferred not to say.

ID	Country	Location	Age	Gender	Education	IT Background	Local Expert's Role in their Community
P01	Kenya	Urban	40	Woman	Form Four	No	Sells electronic devices including phones.
P02	Kenya	Rural	37	Man	Diploma	Yes	Owns and operates a cybercafe.
P03	Kenya	Rural & urban	30	Woman	Bachelors	Yes	Operates a tech repair shop.
P04	Kenya	Urban	30	Man	High school	No	Sells phones, SIM cards, and other accessories.
P05	Kenya	Urban	25	Woman	Diploma	Yes	Works at a government ICT center.
P06	Kenya	Semi-urban	29	Woman	Bachelors	Yes	Owns cybercafe and trains HS students on ICT.
P07	Kenya	Urban & rural	33	Man	Masters	Yes	Owns and has previously worked in a cybercafe.
P08	Kenya	Urban	33	Man	Diploma	No	Works at a local cybercafe.
P09	Kenya	Urban	28	Man	Bachelors	Yes	Works at a government ICT center.
P10	Kenya	Rural	31	Woman	Bachelors	No	Works at a government ICT center.
P11	Nigeria	Urban	_	Man	Masters	Yes	Operates a tech repair shop.
P12	Nigeria	Urban	28	Man	Masters	Yes	Sell computers and operates a tech repair shop.
P13	Nigeria	Urban	_	Woman	Masters	Yes	Works at a cybercafe.
P14	Nigeria	Urban	28	Woman	Bachelors	Yes	Graphics design, and owns an ICT training center.
P15	Nigeria	Urban	_	Man	Masters	Yes	Sale and repair of computers.
P16	Nigeria	Rural	28	Man	Bachelors	Yes	Works at a cybercafe.
P17	Nigeria	Urban	_	Man	Bachelors	Yes	Performs website design and owns a cybercafe.
P18	Nigeria	Rural	23	Man	Bachelors	No	Multimedia designer and IT services consultant.
P19	Nigeria	Urban	_	Woman	Masters	Yes	Typing, printing and computer training.
P20	Nigeria	Urban	30	Woman	Bachelors	No	Runs a cybercafe, performs data entry and analysis.
P21	Ghana	Rural	38	Man	Diploma	Yes	Works at a cybercafe.
P22	Ghana	Urban	25	Man	High school	No	Manages and operates a cybercafe.
P23	Ghana	Urban	24	Man	High school	No	A graphic designer and IT technician.
P24	Ghana	Rural	20	Man	High school	Yes	Provides community tech support and assistance.
P25	Ghana	Urban	36	Man	Masters	Yes	PC and printers technician.
P26	Ghana	Urban	43	Man	Bachelors	Yes	A teacher, performs phone repairs and sales.
P27	Ghana	Urban	24	Man	Bachelors	Yes	Computer sales, repair and software installation.
P28	Ghana	Rural	_	Man	Bachelors	No	Works at a cybercafe.
P29	Ghana	Semi-urban	44	Man	Masters	Yes	Teacher and a manager at a cybercafe.
P30	Ghana	Rural	43	Man	Bachelors	Yes	Works at a cybercafe, and assists with printing.
P31	Mexico	Rural	38	Man	Bachelors	Yes	Teacher that people consult with concerns on IT.
P32	Mexico	Rural	42	Woman	Bachelors	Yes	Teacher, owns a cybercafe, and repairs computers.
P33	Mexico	Rural	38	Man	_	Yes	Computer repair technician.
P34	Mexico	Urban	29	Man	Bachelors	Yes	A civil servant who works with rural communities.
P35	Mexico	Urban	33	Woman	Bachelors	Yes	Only woman in her region that owns a cybercafe.
P36	Mexico	Rural	47	Man	Masters	No	Teaches IT at a primary school, and does tech repair.
P37	Mexico	Urban	40	Man	Bachelors	Yes	Works in IT and but also supports rural communities.
P38	Brazil	Urban	43	Man	Technical course	Yes	Teaches IT to people with limited knowledge.
P39	Brazil	Urban	19	Man	Technical course	Yes	Help desk support to public schools.
P40	Brazil	Urban	39	Man	_	Yes	Tech repairs, and are now authorized by Apple.
P41	Brazil	Urban	48	Woman	Masters	Yes	Refurbishes and donates computers to public schools.
P42	Brazil	Urban	21	Man	High school	Yes	Intern at school lab, does installation and repair.
P43	Brazil	Urban	23	Man	High school	Yes	IT mentorship at a local church, and does tech repair.
P44	Brazil	Urban	18	Woman	Technical course	Yes	Organizes events to teach computer skills to people.
P45	Brazil	Urban	22	Man	High school	Yes	Intern at school lab, does installation and repair.
P46	Brazil	Urban	23	Man	High school	Yes	Tech support services at the office of the Public Prosecutor's office.
P47	China	Urban	24	Man	Bachelors	No	Police officer and mainly handles fraud.
P48	China	Urban	51	Woman	Bachelors	No	Police officer and mainly handles fraud.
P49	China	Urban	35	Man	Bachelors	Yes	Network security engineer and provide security solutions on social media.
P50	China	Urban	34	Man	High school	Yes	Owns 12 tech repair service stores
P51	China	Urban	26	Woman	Bachelors	Yes	Work as a network security service business manager.
P52	India	Semi-urban	40	Man	Bachelors	Yes	Runs a cybercafe and cable business.
P53	India	Urban	58	Man	Diploma	Yes	A teacher of yoga.
P54	India	Urban	39	Man	High school	Yes	Operates a tech repair shop, and does software and hardware repairs.
P55	India	Urban	29	Man	Masters	No	Sells mobile phones and performs repairs.
P56	India	Urban	38	Man	High school	No	Store manager, and sells electronics e.g., phones.
P57	Pakistan	Urban	34	Man	Bachelors	Yes	Owns and operates a mobile repair shop for hardware and software issues.
P58	Pakistan	Urban	38	Man	High school	Yes	Owns and operates a mobile repair shop for hardware and software issues.
P59	Pakistan	Urban	30	Man	High school	Yes	Freelancer and provides e-commerce services.
P60	Pakistan	Urban	33	Woman	Masters	Yes	Freelance and provides Amazon services to clients.
P61	Pakistan	Urban	26	Man	Masters	Yes	Freelancer and also works as a data scientist.
P62	Pakistan	Urban	22	Woman	Bachelors	Yes	Online tutor and researcher.
P63	Pakistan	Urban	31	Woman	Bachelors	Yes	Works full-time as a technical writer, and part time as an online tutor.
P64	Pakistan	Urban	31	Woman	Masters	Yes	Social mobilizer at NGO and provides training.
P65	Pakistan	Urban	32	Woman	Bachelors	Yes	A teacher and also sells mobile phone accessories.
P66	Türkiye	Rural	50+	Man	Associates degree	No	A public servant.
P67	Türkiye	Urban	26	Woman	Bachelors	Yes	Teacher and provides tech support and advice.
P68	Türkiye	Urban	21	Man	High school	Yes	Mobile phone repairs.
P69	Türkiye	Urban	45	Man	Masters	Yes	Works at a university library.
P70	Türkiye	Urban	29	Woman	Bachelors	Yes	A pharmacist but also helps people access e-government services.

Appendix C. Meta-Review

The following meta-review was prepared by the program committee for the 2026 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

C.1. Summary

The paper investigates security and privacy advice across nine majority world countries. The authors conducted 70 semi-structured interviews with local experts, including cybercafe operators and tech repair specialists. They find that the advice provided by local experts in the majority world largely matches the advice they provide to their constituents, but also various significant barriers such as economic constraints, language barriers, and social friction.

C.2. Scientific Contributions

- Independent confirmation of important results with limited prior research.
- Establishes a new research direction.
- Provides a valuable step forward in an established field.

C.3. Reasons for Acceptance

1) The paper reports on an impressive effort in human-centered security research by interviewing 70 local experts in nine majority world countries.
2) The paper investigates security advice in non-western countries with their own unique constraints and considerations, and widens the focus on WEIRD populations in human-centered security research.

C.4. Noteworthy Concerns

Reviewers had the following concerns:

1) The heterogeneous participant pool precludes meaningful comparisons.
2) The lack of distinctly new findings regarding problems and solutions adopted in majority-world countries. The main conclusion (that is, that users in less developed digital environments face practical and cultural barriers to adopting security advice) is not novel. Similar themes (e.g., distrust in Western advice, necessity-driven trade-offs, digital illiteracy) have been explored in previous ICT4D and usable security literature.

Another reviewer has the following major concerns:

1) Given that digital surveillance and security are also shaped by local laws, political regimes, and regulations, the absence of a legal or regulatory analysis limits the generalizability of the findings.
2) A limitation of the work is that the paper only documents how advice differs. However, the paper does not develop a framework or typology that explains how security and privacy advice transform under different infrastructural and cultural constraints.

Appendix D. Response to the Meta-Review

We acknowledge our heterogeneous participant pool as a limitation, and deliberately avoid making country-level comparisons for this reason. While some of our findings overlap with prior work in the majority world, we argue that our results are novel from a security and privacy advice perspective. To our knowledge, we are the first to compare majority world advice to Western advice. We show similarities and differences as well as how different contextual factors shape advice in the majority world. The reviewers also note that we neither offer a legal or regulatory analysis of our findings nor develop a framework or typology that explains how different infrastructural and cultural constraints influence advice. These were outside our scope, and we mention them as promising directions for future research.