

# Digital Security Perceptions and Practices Around the World: A WEIRD versus Non-WEIRD Comparison

Franziska Herbert<sup>†1</sup>, Collins W. Munyendo<sup>†2,3</sup>, Jonas Hielscher<sup>1</sup>, Steffen Becker<sup>1,3</sup>, and Yixin Zou<sup>3</sup>

<sup>1</sup>Ruhr University Bochum

<sup>2</sup>The George Washington University

<sup>3</sup>Max Planck Institute for Security and Privacy

## Abstract

Existing usable security and privacy research remains skewed toward WEIRD (Western, Educated, Industrialized, Rich, and Democratic) societies, whereas studies on non-WEIRD societies are scarce and mostly qualitative. The lack of large-scale cross-country comparisons makes it difficult to understand how people's security needs, perceptions, and practices vary across contexts and cultures. To fill this gap, we surveyed participants ( $N=12,351$ ) from 12 countries across four continents – with seven WEIRD and five non-WEIRD countries – to examine participants' perceptions (e.g., regarding importance of different data types and risks posed by possible attackers) and practices (e.g., adoption of protective measures and prior negative experiences). We found significant differences between WEIRD versus non-WEIRD countries across almost all variables, with varying effect sizes. For instance, participants from non-WEIRD countries relied more on friends and family for advice on digital security than their WEIRD counterparts, but they also viewed friends and family as more likely attackers. We provide our interpretations of the cross-country differences, discuss how our findings inform security interventions and education, and summarize lessons learned from conducting cross-country research.

## 1 Introduction

Despite recent advances in security and privacy research, users still bear the responsibility to protect their own digital security [95,96]. Experts often advise users to adopt best practices, such as choosing secure passwords and using two-factor authentication [92]. The adoption of recommended practices is low due to issues in the provided advice [91] and existing tools [2,93] as well as users' limited time, resources, and competing priorities [44,130]. Other work has investigated users' perceptions of various topics and tools such as Wi-Fi networks [60], HTTPS [63], and antivirus software [110,130], finding misconceptions to be prevalent [43].

<sup>†</sup>Co-first authors; Franziska and Collins contributed equally to this work.

While extensive research on users' digital security perceptions and behaviors exists, the insights are primarily drawn from participants in WEIRD (Western, Educated, Industrialized, Rich, and Democratic) countries [36,56]. While studies exploring non-WEIRD populations have been increasing, they are mostly qualitative and confined to a single country. There is little research directly comparing people's digital security perceptions and practices between WEIRD and non-WEIRD countries. Such comparisons are needed to improve the security community's knowledge about threats and attacks that impact users, and to inform more inclusive technologies.

To fill this gap, we conducted a large-scale cross-country survey ( $N=12,351$ ) drawing a national representative sample from each of the following 12 countries across four continents, including seven WEIRD countries (Germany, Italy, Israel, Poland, Sweden, the United Kingdom, and the United States) and five non-WEIRD countries (China, India, Mexico, Saudi Arabia, and South Africa). Our survey is one of the largest-scale cross-country security user studies compared to prior work [24,35,68,103,108]. The 12 countries, accounting for about 42% of the world's population, are highly diverse in their locations, language, economic metrics, internet penetration rates, and cultural norms. We investigated participants' perceptions (familiarity with terms, perceived importance of various data types, and possible attackers) and practices (adoption of security measures, information sources, and prior experiences with cybercrime) concerning digital security, centering around the following research questions:

**RQ1:** What are users' digital security perceptions and practices within and across 12 countries?

**RQ2:** Are there significant differences between participants from WEIRD versus non-WEIRD countries?

We found several broad trends for perceptions and behaviors. For instance, participants reported universally high familiarity with terms such as "malware" and "ad blocker," and almost all participants reported taking at least one of the protective measures we queried. We also observed significant differences between WEIRD versus non-WEIRD countries for

almost all constructs with varying effect sizes. Non-WEIRD participants attached more importance to the various data types, used more information sources, and had higher perceptions of possible attackers compared to their WEIRD counterparts. WEIRD and non-WEIRD participants also preferred different protective measures, although their adoption rates were similar. Our findings challenge assumptions derived from conventional WEIRD-skewed studies and call for efforts to align threat assessment, provided tools, and resources between WEIRD and non-WEIRD societies. We conclude with reflections on the WEIRD versus non-WEIRD differences and practical recommendations for closing this gap.

## 2 Related Work

**Country-specific studies.** Prior work has provided the baseline for many constructs we measured in our survey. For example, the German Federal Office for Information Security conducted Germany-wide representative surveys in 2020 and 2022, showing that 25% and 29% of respondents had been affected by some sort of cybercrime [82, 128]. Studies conducted in Poland have shown that the public’s acceptance of online banking largely depends on the perceived security of cyberspace [85], but there is no consensus on what constitutes best practices [113]. Prior work in Sweden and the UK has primarily focused on security awareness and education [6, 8, 12], such as how cybersecurity education curricula improve security awareness and practices [19, 62, 99] but face challenges in implementation [18, 84].

Other work in the Middle East, Africa, Asia, and Latin America has shown the unique threat models, needs, and challenges of people living in these regions and how they are not sufficiently addressed by broad solutions designed and evaluated in the West. For instance, despite awareness of security tools, most Saudis do not engage with these tools and have not received any security awareness training [5]. Prior work in Mexico has highlighted the shortage of cybersecurity budgets and capacity building [61]. Research in South Africa has shown users’ misconceptions about app permissions and encryption [114] and general knowledge gaps regarding privacy [94]. Research in Kenya has shed light on how users’ privacy concerns with mobile loan apps are outweighed by their need to procure loans [77] while users of cybercafes significantly rely on cafe managers for security and privacy advice even though the advice might put them at risk [78].

Moreover, research in Asia and the Middle East has highlighted how socio-cultural norms and power relations shape people’s security perceptions and practices. Studies involving the Arab Gulf populations have shown collectivist cultural norms’ impact on users’ online self-representation [1, 66]. Similar patterns emerge from studies in South Asian countries such as Bangladesh, India, and Pakistan, where device sharing is common among families (especially between women and their husbands, parents, and children) [79, 97, 100, 101].

Users’ perceptions are also shaped by local infrastructure and processes of urbanization and digitization [4, 108]. Studies in China reveal users’ challenges with ubiquitous mobile payment systems, such as limited awareness of surveillance [109].

Despite their limited generalizability, these country-specific studies contribute important insights into how socio-cultural factors, context, and technology use cases shape people’s perceptions and practices. Our work builds on these studies by directly comparing security and privacy perceptions and practices in WEIRD versus non-WEIRD countries.

**Cross-country studies.** To a lesser degree, researchers have conducted studies spanning multiple countries, showing variances across countries for different constructs [20, 24, 36, 43, 67, 103, 104, 121]. For instance, Herbert et al. [43] identified one’s country of residence as a strong predictor of misconceptions around digital security topics, with significant differences found between Western and non-Western countries. Using the Security Behavior Intentions Scale (SeBIS) [25], Sawaya et al. found that participants from Asian countries, and especially Japan, exhibited less secure behavior [103]. Harbach et al.’s study across eight countries found that participants from non-US countries (except for Italy) were more likely to use a secure lock screen [35]. Sharma et al. highlighted a clear division between the Global North and Global South countries in user perceptions of COVID contact tracing apps, with Global North users being more reluctant to share personal information and location data [108].

Other studies have identified similar patterns across countries, such as uncertainty about digital security topics [43], a common process in account security incident response [88], and the crucial role of self-confidence in influencing security behavior more than actual knowledge [103]. Researchers have also explored the underlying factors behind cross-country differences [17, 120], including culture, knowledge, unintended technology use, context, usability, and cost considerations.

Our work builds on prior cross-country studies by (1) covering a diverse set of WEIRD and non-WEIRD countries for comparisons; (2) having a larger sample size with a national representative sample for each country; and (3) examining a broader range of constructs. We investigated perceptions and practices to cover both attitudinal and behavioral aspects of one’s security posture. Additionally, most of our constructs have not been measured in previous cross-country studies.

## 3 Method

Through a large-scale online survey ( $N=12,351$ ), we investigate digital security perceptions and practices of participants from 12 countries (seven WEIRD and five non-WEIRD) around the world, with at least 1,000 participants recruited from each country. While we drew from the same dataset by Herbert et al. [43], our study is novel in several ways:

(1) we analyzed a completely different set of variables – this analysis is based on survey questions Q6–Q8 and Q20–Q22, while the prior study focused on Q9–Q16; (2) we report participants’ perceptions and practices, which were not covered in the previous publication; and (3) we focused on WEIRD versus non-WEIRD comparisons, which, to our knowledge, has not been done in prior work on security-related topics.

### 3.1 Survey Design

**Topic selection and item generation.** We consulted seven researchers when drafting our initial survey. Through several workshops, the researchers identified various digital security threats and advice provided to the general public, both in everyday life and through research. We then complemented the expert insights with prior work [27, 92, 107, 128] to generate our survey questions. Our final survey covered topics related to both the users’ demographics and technology use as well as constructs related to digital security perceptions and practices. We provide our full questionnaire on OSF: <https://osf.io/4dkwe>. Below, we describe the parts related to our research questions.

**Introduction and tech use background.** First, we detailed the purpose of our study alongside how data would be handled and used; participants needed to consent before proceeding. We started by asking participants about their internet and device usage (Q1 and Q2). As increased reliance on technology could increase the risk of cybersecurity attacks, we viewed participants’ tech use background as an indicator of the attack surface to which they are exposed.

**Perceptions.** We measured participants’ perceptions via three constructs. Questions about familiarity with terms (Q6) were partly based on Kang et al. [55]. We expanded the scope by including terms related to security and privacy enhancing technologies (e.g., “2FA” and “incognito mode”) and specific threats often used in educational campaigns (e.g., “malware” and “phishing”). Questions about participants’ perceived importance of various data types (Q21) and possible attackers that could pose a threat to their digital security (Q22) were generated and pilot-tested via workshop sessions, and we used Rohrmann’s verbal rating scales to measure the items [98].

**Practices.** We measured participants’ S&P practices via three constructs. For prior experience with cybercrime (Q7), we drew from the BSI survey [128] for seven items and added “data abuse” and “romance/love scams” based on insights from the researcher workshops. Similarly, items for information sources related to digital security (Q8) were based on Redmiles et al. [90] and insights from the researcher workshops. Possible protective measures for staying safe online (Q20) were based on Reeder et al. [92].

**Demographics.** Lastly, we collected participants’ demographic information related to gender (Q23), education (Q24), tech background (Q25), and migration background (Q26), as prior work has shown sociodemographic differences in people’s security postures [71, 89, 124, 130]. Since our participants hailed from diverse educational systems, we used ISCED, an internationally-established method for measuring education [118]. Other demographic information, including age and region, was collected by our panel provider.

### 3.2 Survey Implementation

**Country selection.** We recruited participants from 12 countries. Seven countries are WEIRD: Germany (DEU), Israel (ISR), Italy (ITA), Poland (POL), Sweden (SWE), the United Kingdom (UK), and the United States (USA) while five countries are non-WEIRD: China (CHN), India (IND), Mexico (MEX), Saudi Arabia (SAU), and South Africa (ZAF). For the WEIRD versus non-WEIRD classifications, we followed the approaches in prior work [10, 39] as follows:

- **Western:** Countries in North America and Western Europe, as well as Israel, Australia, and New Zealand were classified as Western societies, following Gosling et al. [30].
- **Educated:** Human development regarding the general population of the country was rated as very high, high, medium, or low according to the Human Development Report by the United Nations [117].
- **Industrialized:** Countries were classified as having an advanced or emerging/developing economy based on data from the World Economic Outlook [51].
- **Rich:** The classification of high, upper middle, lower middle, and low income was used to reflect the household wealth based on the Global Wealth Report [32].
- **Democratic:** Countries were classified as having a full democracy, a flawed democracy, a hybrid regime, or an authoritarian regime according to the Democracy Index [26].

Countries were classified as WEIRD if they met all the above five criteria, with a few exceptions.<sup>1</sup> Table 1 documents the WEIRD parameters by country and classification. In addition to the WEIRD versus non-WEIRD classifications, we paid attention to a country’s population size, geographic location, languages, and culture as other important dimensions when sampling. (1) Altogether, the 12 countries account for 42% of the world’s population and are spread across four continents. (2) Languages influence people’s adherence to security advice [37], and there are gaps when English-language advice is translated to other languages [15]. Our sampling

<sup>1</sup>The Democracy Index is subject to temporal variations due to critical political changes. Following the practice in Beyebach et al. [10], we categorized Israel, Italy, and the United States as WEIRD countries since their average Democracy Index score in the last two decades is closer to full democracy, even though they had flawed democracy according to the Democracy Index in 2023 [26].

Table 1: WEIRD vs non-WEIRD Classification of Countries.

Country	Western	Educated	Industrialized	Rich	Democratic	Classification
CHN	Non-Western	High	Emerging	Upper Middle	Authoritarian	Non-WEIRD
IND	Non-Western	Medium	Emerging	Lower Middle	Flawed	Non-WEIRD
MEX	Non-Western	High	Emerging	Upper Middle	Hybrid	Non-WEIRD
SAU	Non-Western	Very High	Emerging	Upper Middle	Authoritarian	Non-WEIRD
ZAF	Non-Western	High	Emerging	Lower Middle	Flawed	Non-WEIRD
DEU	Western	Very High	Advanced	High	Full	WEIRD
ISR	Western	Very High	Advanced	High	Flawed	WEIRD
ITA	Western	Very High	Advanced	High	Flawed	WEIRD
POL	Western	Very High	Advanced	Upper Middle	Flawed	WEIRD
SWE	Western	Very High	Advanced	High	Full	WEIRD
UK	Western	Very High	Advanced	High	Full	WEIRD
USA	Western	Very High	Advanced	High	Flawed	WEIRD

goes beyond the English-speaking world, and the 12 countries represent at least 20 languages (when counting the official languages). (3) Furthermore, culture plays a salient role in people’s security attitudes and behaviors [29]. The 12 countries represent diverse cultures when measured by Hofstede’s cultural dimensions, such as individualism and uncertainty avoidance [46]. (4) Lastly, the 12 countries have received varying degrees of attention in existing usable security and privacy literature [36]: the existing literature is extremely skewed toward US samples; Germany, UK, and India are also fairly represented, whereas the remaining countries in our sample have received little attention.

**Pilot testing, panels, and translation.** To estimate the length and comprehensibility of the survey, we created a preliminary version in German, then refined and improved the survey based on feedback from our social circles and colleagues. To ensure the survey is accessible, we administered a pilot on Prolific with 100 participants in Germany and used the feedback to improve the clarity of survey questions.

To collect responses from people living in the 12 countries, we commissioned Kantar, a reputable full-service provider of online surveys. Kantar was responsible for the survey’s implementation, translation, participant recruitment and compensation, and data quality assurance. To enable large international studies such as ours to be carried out simultaneously, Kantar uses its own research panel (LifePoints) in addition to a vetted list of panel suppliers around the world. Kantar’s own panel consists of non-professional individuals, who (1) made a conscious decision to participate in online surveys through a double opt-in process, (2) were recruited using multiple sources (e.g., opt-in emails and social media campaigns), and (3) take surveys in exchange for a reward (e.g., membership points for a particular vendor). Kantar does not provide further details on the recruitment process for other panels in their network. While the available panels in each country often differ, Kantar’s general procedures for vetting respondents and ensuring data quality (e.g., cross-validating IP addresses,

browser languages, and geolocations; CAPTCHA checks; removing speeders; removing those who have failed attention checks) are consistent across countries.

For the translation, Kantar implemented the first version of the survey in German according to our requirements. Then, a professional interpreter translated the survey into English and several team members carefully reviewed the translation for accuracy and consistency. The survey was then translated into the respective official languages in each country (Arabic, Chinese, Hebrew, Italian, Polish, Spanish, and Swedish) by professional translators commissioned by our panel provider. When possible, we had bilingual team members check and confirm that translations were accurate.

**Data collection and participant compensation.** Data was collected from December 2021 to February 2022 across all 12 countries. From each country, we aimed to obtain a quota-representative sample in terms of *age*, *gender*, *education*, and *region*. In the US, we additionally aimed for *ethnicity*. Our panel provider determined the quotas based on the most recent available census data. Table 4<sup>2</sup> shows how well the target quotas have been met for each country. The median completion time was about 24 minutes across all countries (min: 19.5 mins in China; max: 32.3 mins in South Africa). While our panel provider did not disclose the exact participant compensation rates, they broadly used the following rates: €2.51 in China, India, Italy, Mexico, Poland, South Africa, UK, and US; €2.61 in Germany; €3.20 in Sweden; €3.45 in Saudi Arabia; and €5.25 in Israel. Kantar further informed us that these rates are in line with industry standards, and we did not have influence on these rates.

### 3.3 Sample Description

Table 2 shows key demographic information of our participants and their device usage and smart home adoption. Eth-

<sup>2</sup>Tables 4 to 7 are available via the online appendix in our OSF repository: <https://osf.io/4dkwe>.

nicity was collected only for US participants by our panel provider (White: 70.3%, African American: 11.5%, Hispanic/Latino: 9.6%, Asian: 6.0%, Other: 2.2%). Our study had almost even proportions of male and female participants in each country. A vast majority of participants in each country use smartphones in their daily lives (highest in China: 99.8%, lowest in UK and USA: 88.8%); laptops, stationary personal computers, and tablets were the next most widely used devices. Participants in China, India, and Saudi Arabia also reported wide adoption of smart home devices.

### 3.4 Data Analysis

For common trends across the 12 countries, we report descriptive statistics depending on the data type. For instance, for familiarity with terms (Q6), we report the aggregated percentages of participants who reported at least basic familiarity; for possible attackers (Q22), we report the mean values of the likelihood of someone posing a risk on a 5-point scale.

For WEIRD versus non-WEIRD comparisons, we conducted tests to identify statistically significant differences. The specific test depended on the data type, i.e., Chi-square tests for categorical dependent variables, Wilcoxon-Mann Whitney tests for ordinal and non-normal distributed interval dependent variables. To this end, we used Wilcoxon-Mann Whitney tests for familiarity with different terms (Section 4.1), perceived importance of various data types (Section 4.2) and possible attackers (Section 4.3); and Chi-square tests for previous experiences with cybercrimes (Section 4.4), information sources for learning about digital security (Section 4.5), and adoption of protective measures (Section 4.6).

To control the probability of observing false positives, we performed Bonferroni correction for all WEIRD versus non-WEIRD comparisons. For presentation brevity, we describe the key findings and trends in Section 4, and include the detailed results in Tables 5 and 6. For effect sizes, we report  $\phi$  for  $X^2$  tests and  $r$  for Wilcoxon-Mann Whitney tests [16].

### 3.5 Robustness Checks

We performed robustness checks on our data. Specifically, we examined how many participants claimed to be affected by cybercrime (Q7) or implemented security measures (Q20) while simultaneously stating that they were not familiar with the corresponding term (Q6). Table 7 shows that the rates for such participants were low for most of the constructs but with variances ranging from 1.5% to 12.5%.

### 3.6 Limitations

As is typical for self-reported online surveys, it is hard to tell if participants followed our instructions and responded

accurately to all questions. Country-specific geopolitical dynamics, such as VPN usage being a legally gray area in China and Saudi Arabia, might further influence participants' responses in ways that a quantitative study cannot fully unveil. Further, while bilingual members of our team reviewed the translations done by our panel provider for consistency and accuracy, some of the terms might have been lost in translation across countries.

A small portion of our participants exhibited potentially inconsistent patterns in their survey responses as shown in Section 3.5. After careful deliberations, we decided against excluding these participants because we could not assert whether this was real inconsistency or an artifact of the questionnaire design: (1) We did not offer a *prefer not want to answer* option for the familiarity question, so answers indicating no familiarity might be skewed in this direction. (2) The exposure to Q6 might have influenced answers in Q20. (3) Some questions between Q6 and Q20 explain certain constructs, which may also foster the tendency toward selecting more measures than actual usage. We believe these responses are still valid as they passed other data quality checks (e.g., passing the attention check, and providing sensible open-ended responses to Q5).

Despite our best efforts, our sample is not fully representative of the target quotas in some countries (see Table 4). Our participants were skewed slightly towards being middle-income and well-educated across all countries except South Africa and Mexico. Still, we achieved representative quotas across age and gender with a maximum discrepancy rate of less than 2% across all countries, except for Saudi Arabia, where discrepancies were around 5%. We could not achieve education quotas for China, India, Italy, Mexico, Saudi Arabia, and South Africa due to the high percentage of low-education populations in these countries [118] who are difficult to reach via online surveys. The skewed, more educated non-WEIRD samples might also explain some of our findings, as we discuss in Section 5.2. Additionally, our panel provider had insufficient data about the regional quotas in Israel and Saudi Arabia, and we complemented it with publicly available data.

Lastly, our survey questions were mostly closed-ended. While we observed differences across countries, we did not have the opportunity to probe and ask participants to explain their answers. Thus, we can only speculate potential reasons for these differences. That being said, we believe that our study lays the foundation for future work to empirically validate explanations for the cross-country variances we found.

### 3.7 Positionality

We are aware that our backgrounds, values, and biases substantially influence how we conduct research [69], and researchers are always at risk of reproducing knowledge that reifies power [112]. Our team comprises highly educated researchers with varying years of experience conducting em-

Table 2: Participant demographics. Data for age as delivered by our panel provider. Information about participants’ gender, education level, device, and smart home use was collected in the questionnaire.

	Country											
	NON-WEIRD					WEIRD						
	CHN (1008)	IND (1011)	MEX (1045)	SAU (1018)	ZAF (1048)	DEU (1019)	ISR (1011)	ITA (1019)	POL (1054)	SWE (1049)	UK (1018)	USA (1051)
<b>Gender</b>	%	%	%	%	%	%	%	%	%	%	%	%
Female	46.6	46.0	49.2	41.5	50.2	49.5	49.7	52.0	50.3	50.4	51.1	51.6
Male	51.9	50.9	47.0	49.8	44.6	49.2	44.5	46.7	44.5	48.6	48.3	46.8
Other	1.5	3.1	3.8	8.7	5.2	1.3	5.8	1.3	5.2	1.0	0.6	1.6
<b>Age</b>	%	%	%	%	%	%	%	%	%	%	%	%
18–24	9.6	19.8	19.3	19.0	21.9	7.4	14.1	8.1	9.8	11.0	8.6	11.0
25–39	35.1	37.8	36.3	54.6	40.7	22.7	31.3	20.3	28.5	23.3	25.5	25.1
40–54	41.8	25.7	26.9	24.0	23.8	27.4	24.3	29.6	24.7	25.3	26.7	27.0
55+	13.5	16.7	17.5	2.4	13.6	42.5	30.3	42.0	37.0	40.4	39.2	36.9
<b>Education</b>	%	%	%	%	%	%	%	%	%	%	%	%
Low (ISCED 0-2)	8.0	3.8	30.6	7.5	25.5	15.4	9.2	15.5	3.4	9.7	18.8	2.6
Medium (ISCED 3-4)	36.3	36.0	28.7	38.8	39.7	51.9	34.9	54.3	58.5	43.4	33.3	40.5
High (ISCED 5-8)	55.4	58.0	40.1	53.1	31.6	32.4	54.3	29.9	37.8	45.6	47.7	55.6
Other	0.3	2.2	0.6	0.6	3.2	0.3	1.6	0.3	0.3	1.3	0.2	1.3
<b>Q1. Device Use</b>	%	%	%	%	%	%	%	%	%	%	%	%
Smartphone	99.8	98.8	94.5	97.8	97.8	92.7	96.9	97.7	96.4	95.2	88.8	88.8
Tablet	51.6	37.5	43.0	45.6	34.6	45.4	30.0	52.0	38.3	49.2	50.6	43.5
Laptop	72.3	76.0	59.3	69.2	74.8	68.7	72.0	73.2	83.6	73.5	71.6	60.4
Stationary PC	63.1	41.9	41.9	42.7	30.7	49.0	61.3	54.7	45.2	44.7	37.1	42.2
Smart Speaker	36.7	36.1	22.7	17.7	8.1	17.8	7.1	25.9	6.2	12.5	26.8	24.5
Wearable	32.2	38.3	15.5	34.9	18.4	14.1	16.5	23.2	25.0	13.7	20.1	16.9
<b>Q2. Smart Home</b>	%	%	%	%	%	%	%	%	%	%	%	%
Energy & Climate	47.9	47.9	36.8	53.9	34.8	14.5	26.6	23.9	19.8	25.6	20.2	25.1
Security	44.9	49.9	35.6	50.8	41.2	10.6	26.5	28.4	20.2	27.4	21.7	32.2
Home & Garden	31.4	33.8	17.4	48.4	23.1	11.8	37.0	17.1	18.8	18.9	9.5	17.0

pirical, human-centered security research. Our team members are from four different countries and have backgrounds in multiple disciplines spanning anthropology, human-computer interaction, psychology, and security engineering. However, we acknowledge that our team does not have a representative from every country covered. Despite our best efforts to minimize loss through translation by using professional translation services, we might have missed out on cultural or semantic context relevant to interpreting some findings.

## 4 Results

We present descriptive statistics and WEIRD vs non-WEIRD comparisons for key variables. Three are about perceptions: familiarity with terms (Q6), perceived importance of various data types (Q21), and possible attackers (Q22). Three are about practices: experiences with cybercrime (Q7), information sources (Q8), and adopted protective measures (Q20).

### 4.1 Familiarity with Terms

We elicited participants’ self-reported familiarity with various terms related to digital security and privacy, as such familiarity lays the groundwork for perceiving risks and taking appropriate measures [21]. The percentages we report are aggregated across participants who selected “I know what this is but I don’t know how it works” (basic familiarity), “I know how this works” (intermediate familiarity), and “I know very well how this works” (advanced familiarity) for each country and the WEIRD vs non-WEIRD groups. Figure 1 gives an overview of our findings.

**Universally high familiarity with ad blockers, data leak, identity theft, and malware.** Across all countries, most participants reported familiarity with “ad blockers,” “data leak,” “identity theft,” and “malware.” The familiarity rate was between 70% and 90% for most countries. For “ad blockers” and “malware,” China represents the high end (91%), and

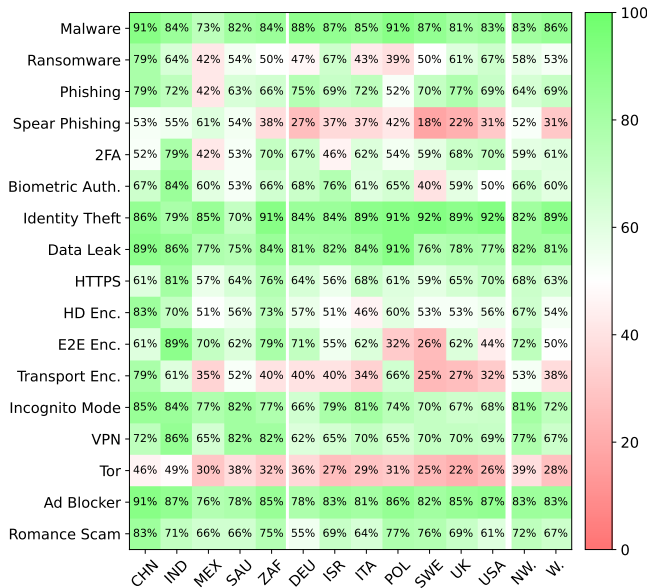


Figure 1: Participants’ familiarity with various IT security and privacy terms as aggregated percentages by country and by non-WEIRD (NW) and WEIRD (W) countries (Q6).

Mexico represents the low end (76% and 73%, respectively). For “data leak” and “identity theft,” Poland represents the high end (91%), and Saudi Arabia represents the low end (75% and 70%, respectively). Sweden, USA, and South Africa had over 90% familiarity for “identity theft.”

For “incognito mode” and “VPN,” we also observed high familiarity rates across the 12 countries (roughly between 60% and 85%), although the average familiarity rates were slightly lower compared to the terms above. For “incognito mode,” participants in China continued to have the highest familiarity rate. Participants from Saudi Arabia and South Africa were the most familiar with VPN (82%). By contrast, participants from Germany were the least familiar with both terms (66% and 62%, respectively).

**Mixed familiarity with terms related to scams and authentication.** For some other terms, we observed mixed self-reported familiarity across countries, ranging from roughly 40% to 80%. These terms center around scams and authentication, including “biometric authentication,” “phishing,” “ransomware,” “romance scam,” and “two-factor authentication.” For the two terms related to authentication (biometric authentication and 2FA), participants in India reported the highest familiarity for both terms (84% and 79%, respectively). In contrast, participants in Sweden and Mexico were the least familiar with these terms (40% and 42%, respectively). For “phishing,” “ransomware,” and “romance scam” – which all revolve around scam schemes – participants in China reported the highest familiarity, whereas participants in Mexico, Germany, and Poland were the least familiar with these terms.

**Universally low familiarity with encryption, spear phishing, and Tor.** We also observed interesting differences for variances related to a given term. For instance, while the familiarity rate for “hard drive encryption” is decent (above 50% for all countries), “end-to-end encryption” and “transport encryption” were lesser known to participants in some countries. Only about a quarter of participants in Sweden were familiar with these two terms. Similarly, while the average familiarity rate for “phishing” was high, the term “spear phishing” (i.e., social engineering attacks targeting specific individuals rather than general phishing attempts toward masses of people) did not ring a bell to participants in most countries. “Tor”, short for “The Onion Router”, was the least familiar term across all countries, with the familiarity rate below 50% for all countries. The familiarity rate was somewhat higher in China (49%) and India (46%), whereas participants in the US and Europe remained largely unfamiliar with this term.

**Higher familiarity with terms among non-WEIRD participants.** We found significant differences in familiarity rates between WEIRD versus non-WEIRD countries for 14 out of the 17 terms. “Malware”, “two-factor authentication,” and “ad blocker” were the only three exceptions where no significant differences between WEIRD versus non-WEIRD countries were found. While the WEIRD parameters (especially education) might suggest that people in WEIRD countries would be more knowledgeable about these terms, counterintuitively, our non-WEIRD participants reported higher familiarity rates for most of the terms where significant differences emerge, such as “spear phishing” (52% NW; 31% W), “end-to-end encryption” (72%NW; 50% W), “transport encryption” (53% NW; 38% W), and “Tor” (37% NW; 28% W).

## 4.2 Perceived Importance of Data Types

Since perceived information sensitivity is central to security and privacy behaviors in different contexts [105], we asked participants to assess the importance of protecting 15 various data types using a 5-point scale (1–not important to 5–very important). Figure 2 gives an overview of our findings.

**High perceived importance for most data types.** All data types were rated as important to protect by participants across all the countries ( $M > 3.5$ ). Moreover, passwords, bank account details, ID cards, and biometric data were unanimously perceived as “very” important to protect ( $M > 4.5$ ). All the other data types were, on average, rated as “quite a bit” important to protect ( $M > 4.0$ ).

That said, there were a few data types that were perceived as less important relatively, with a mean lower than “quite a bit” important to protect in at least one country. For instance, both *delivery notes & invoices* and *full name* were rated between “moderately” and “quite a bit” important to protect in five countries. *Location and movement data* were perceived as

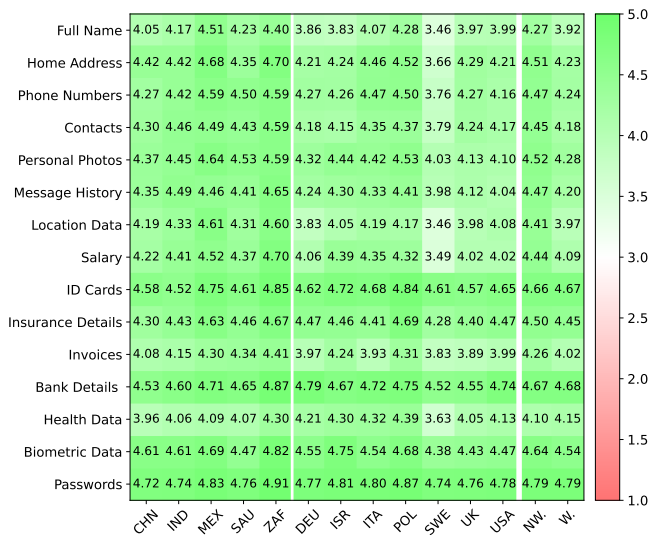


Figure 2: Participants’ perceived importance of protecting different data types on a scale from 1 (not important to protect) to 5 (very important to protect) by country and by non-WEIRD (NW.) and WEIRD (W.) countries (Q21).

less important in three countries, namely Sweden ( $M=3.46$ ), Germany ( $M=3.83$ ), and the UK ( $M=3.98$ ).

**Lower perceived importance of data types among Swedish participants.** Interestingly, Sweden stands out as an outlier in our cross-country comparisons, as Swedish participants rated their data as less worthy of protection consistently across different data types compared to other countries. For instance, Swedish participants gave the lowest rating for *full name*, *location and movement data*, and *salary/earnings* ( $M \approx 3.5$  for all three). We suspect that this finding might be partly due to the fact that the Swedish Tax Agency (Skatteverket) makes such data accessible as public information, so that Swedish citizens might deem their self-protection futile or trust their government’s protection of such data.

**Higher perceived importance among non-WEIRD countries.** We found significant differences between WEIRD and non-WEIRD countries for the perceived importance of 10 out of 15 data types. The five data types that were perceived similarly across the board were *ID cards*, *insurance documents*, *bank details*, *health data*, and *passwords*. Non-WEIRD participants attached higher importance to more data types than WEIRD participants, although the size of the difference for most comparisons was quite small. The starkest differences were found for *full name* ( $M_{NW}=4.27$ ;  $M_W=3.92$ ) and *location and movement data* ( $M_{NW}=4.41$ ;  $M_W=3.97$ ).

### 4.3 Possible Attackers

As individuals’ S&P perceptions are subject to social influences [126], we assessed participants’ perceptions of the likelihood that various groups or entities can pose a risk to their digital security, using a 5-point scale (1–not likely to 5–very likely). Figure 3 gives an overview of our findings.

**Lower risk perceptions toward social circles.** Groups closer to one’s social circles, such as family members, were less likely to be perceived as a threat than groups outside one’s social circles, such as private sector companies. Across all countries (except India), family members were viewed as posing minimal risk to participants’ digital security ( $1.66 < M < 2.79$ ). The lowest mean value came from German and Swedish participants, while the highest mean value came from Indian participants. Participants across all countries also had lower risk perceptions toward friends/acquaintances and work colleagues who are other components of one’s social circle, with a slightly higher upper bound, both from India ( $M=2.99$  and  $M=3.12$ , respectively). We relate the higher risk perceptions from Indian participants to the broader literature on device sharing being a common practice in South Asia, making privacy a not readily available concept, especially for women and lower-income groups [54, 64, 79, 101].

**Higher risk perceptions toward criminals and hackers.** Criminals and hackers were rated as the most explicit attackers by participants across all countries; the mean values show that they are between “moderately” and “quite a bit” likely to become attackers ( $3.11 < M < 3.94$ ), with no differentiation between the two concepts. Officials in the participants’ own country, officials in other countries, and private sector companies were at the intermediate layer between participants’ inner social circles and explicit attackers, as they were rated as moderately likely to pose a risk ( $2.32 < M < 3.32$ ).

**Higher risk perceptions of possible attackers among non-WEIRD countries.** We found significant differences between WEIRD versus non-WEIRD participants for the risk perceptions of all possible attackers. Non-WEIRD participants consistently had higher risk perceptions toward all groups, and the differences were not only significant but also more sizeable. The WEIRD versus non-WEIRD differences were pronounced for groups that belong to participants’ inner social circles, including family members ( $M_{NW}=2.39$ ;  $M_W=1.80$ ), friends/acquaintances ( $M_{NW}=2.73$ ;  $M_W=1.99$ ), and colleagues ( $M_{NW}=2.90$ ;  $M_W=2.1$ ).

### 4.4 Prior Experiences with Cybercrime

As prior experience with cybercrime or negative incidents is a significant driver of adopting S&P measures [89, 130], we

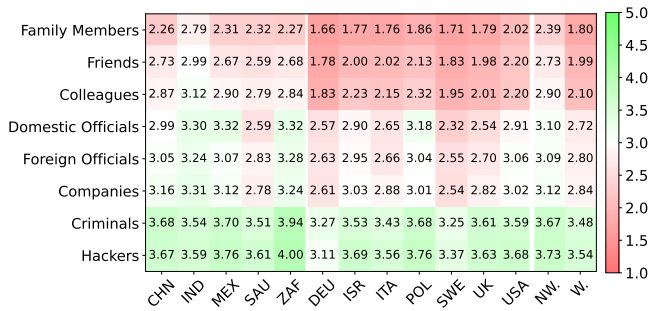


Figure 3: Participants’ perceived likelihood that various groups pose a risk to their digital security, on a scale from 1 (not likely a risk) to 5 (very likely a risk) by country and by non-WEIRD (NW.) and WEIRD (W.) countries (Q22).

asked participants whether they had been affected by nine different types of cybercrime: malware, phishing, ransomware, cyberbullying, fraud with only shopping, external access to an online account, cyberstalking, data abuse, and romance/love scams. Figure 4 gives an overview of our findings.

**Experiencing cybercrime was common.** Except for the UK (44%) and Germany (48%), more than half of the participants in all other countries reported having been affected by one or more of the queried cybercrimes. All rates were higher than those in the 2022 BSI survey [82], which drew responses from a nationally representative sample in Germany and used similar questions despite small differences.<sup>3</sup>

**Higher rates for malware, lower rates for ransomware.** Malware stands out as the most commonly experienced type of cybercrime, with substantial cross-country variances (22%–58%). Other relatively more common cybercrimes include data abuse (12%–49%) and online shopping fraud (14%–44%). By contrast, ransomware was the least commonly reported cybercrime among our participants (5%–18%), likely because ransomware usually targets organizations rather than individual users [80]. The other two types of cybercrime less commonly experienced were cyberstalking (4%–27%) and romance scams (5–26%).

**Higher exposure to cybercrime among non-WEIRD participants.** For all nine types of cybercrime, we found significant differences between WEIRD versus non-WEIRD participants, with non-WEIRD participants consistently having higher exposure rates. For instance, non-WEIRD participants more commonly reported experiencing malware (52% NW; 38% W); malware exposure was reported by more than half of the participants in China (51%), Mexico (58%), and Saudi

<sup>3</sup>The BSI study asked participants if they had been victims of cybercrimes before presenting the specific crimes. In our survey, participants were directly asked about specific crimes.

Arabia (55%). Non-WEIRD participants also reported considerably higher exposure rates (10% of difference or more) for cyberbullying (23% NW; 11% W), online shopping fraud (35% NW; 20% W), unauthorized access to online accounts (25% NW; 14% W), data abuse (36% NW; 18% W), and romance scam (21% NW; 8% W).

Among the non-WEIRD countries, participants from China, India, and Saudi Arabia reported higher exposure to cybercrime. China had the highest exposure rate for data abuse (49%), India had the highest exposure rate for shopping fraud (40%), and Saudi Arabia had the highest exposure rate for cyberbullying (34%) and romance scams (26%). By contrast, the exposure rate to almost all types of cybercrime (except malware) was consistently low among WEIRD countries, with a few exceptions. Shopping fraud was more commonly reported in Israel (24%) and the US (26%). Among the WEIRD countries, Israel and the US also had the highest exposure rate to cyberstalking and data abuse, respectively.

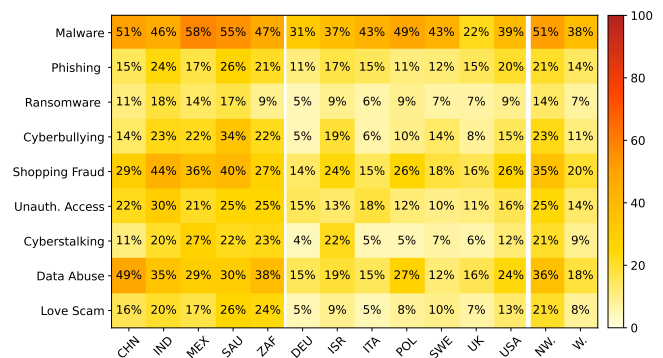


Figure 4: Participants’ exposure rate to nine types of cybercrime by country and by non-WEIRD (NW.) and WEIRD (W.) countries (Q7).

## 4.5 Information Sources

Considering the influence of expert advice on people’s S&P practices [81, 89, 129], we asked participants to indicate where they looked for information related to digital security from a list of nine sources. Figure 5 gives an overview of our findings.

**New media preferred over traditional media.** Online news and social media were frequently reported as sources for learning about digital security information across all countries, with the highest adoption rates among Indian participants (75% and 73%, respectively) and the lowest adoption rates among UK participants (34% and 17%, respectively). By contrast, the adoption rate for traditional media (e.g., print media, radio or podcasts, and TV) was much lower across all countries. For instance, television served as an information source for nearly half of Indian participants (43%) but was

less frequently used in most other countries, ranging from 15% in the UK to 36% in China.

**Mixed popularity for human sources.** Friends and family, security experts, and authorities are examples of human sources for learning about digital security. Among these sources, we observed a mixed rate of popularity. For instance, over half of Indian participants (61%) reported relying on friends and family for learning about digital security, whereas the rate dropped to between 30% to 40% for the remaining countries (except 43% for Saudi Arabia). Between 17% and 47% of participants turned to security experts as an information source. Consumer centers and authorities represent the least utilized source in most countries (9% to 17%), except in China (28%) and India (23%).

**Higher adoption of information sources among non-WEIRD participants.** We found significant differences between WEIRD versus non-WEIRD participants for all information sources we queried. From traditional media to new media, and from authoritative figures to friends and family, non-WEIRD participants consistently reported leaning on these sources more often than WEIRD participants. The differences were especially pronounced for online news (63% NW; 42% W), social media (64% NW; 27% W), friends and family (44% NW; 32% W), and security experts (43% NW; 27% W). Conversely, only 7% of non-WEIRD participants reported not using any of the nine queried sources, whereas the rate increased to 25% for WEIRD participants.

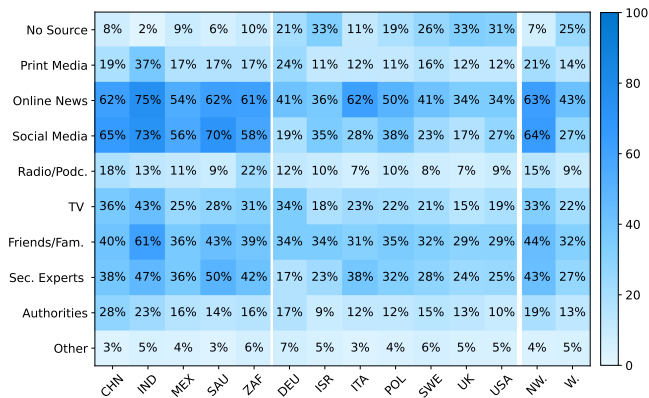


Figure 5: Participants’ sources for seeking information on digital security by country and by non-WEIRD (NW) and WEIRD (W) countries (Q8). “No Source” was an exclusive option, otherwise multiple selection was possible.

## 4.6 Adoption of Protective Measures

We asked participants to self-select which measures they have taken for their digital security from a list of 14 items. Figure 6 gives an overview of our findings.

### High adoption of anti-virus, updates, and backups.

Across all countries, participants reported high adoption rates of anti-virus software (64%–80%) and updating the operating system and other programs (47%–77%). The two backup methods we queried were also relatively popular. The adoption rates of disk-based backup (i.e., backing up on an external hard drive) varied from 30% to 51%, whereas the adoption rates of cloud-based backup (i.e., backing up to the cloud) had a slightly lower average and larger variances, ranging from 19% to 54%. Notably, participants in South Africa, Sweden, Mexico, and Israel preferred cloud-based backup, whereas participants in other countries showed a higher inclination towards disk-based backup.

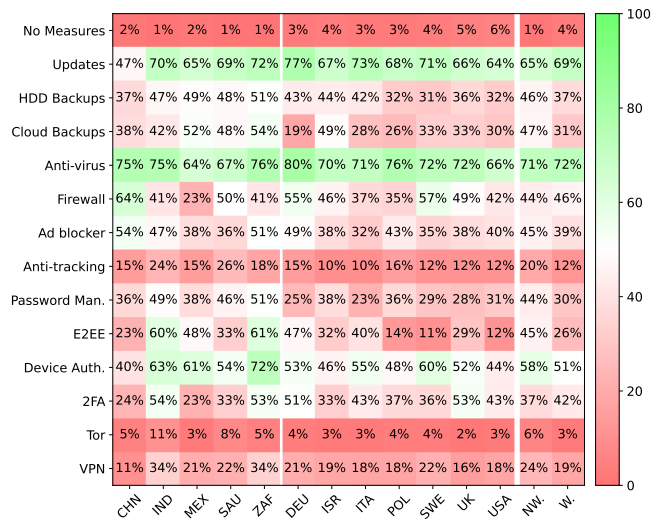


Figure 6: Percentage of participants by country and by non-WEIRD (NW) and WEIRD (W) countries who reported taking specific S&P measures (Q20). “No Measures” was an exclusive option; otherwise, multiple selection was possible.

**Low adoption of PETS.** The various privacy-enhancing technologies (PETs) in our list generally received lower adoption rates across all countries. The adoption rates for VPN varied between 10% and 20% approximately for most countries, with India and South Africa being outliers (both 34%). For anti-tracking tools, adoption rates were as low as 10% (Israel and Italy) and as high as 26% (Saudi Arabia). The Tor network was the least adopted measure, with the adoption rate being between 2% and 5% for most countries. Saudi and Indian participants reported slightly higher adoption rates for Tor (8% and 11% respectively).

### Different preferences for adopted measures between WEIRD versus non-WEIRD participants.

We found significant differences between WEIRD versus non-WEIRD participants for 12 out of 14 measures, with anti-virus and firewall being the only two exceptions that were adopted across

the board. Different from our other findings, the differences here went in both directions across WEIRD and non-WEIRD.

Non-WEIRD participants reported significantly higher adoption rates for PETs, including VPN (24% NW; 19% W), Tor (7% NW; 3% W), and anti-tracking tools (19% NW; 12% W), likely as workarounds against government surveillance in authoritarian regimes. Non-WEIRD participants were also more proactive at doing data backups, including both disk-based (47% NW; 37% W) and cloud-based (47% NW; 31% W) backups. For WEIRD participants, their preferred measures revolved around updates (65% NW; 70% W) and two-factor authentication (38% NW; 42% W).

## 5 Discussion

We investigate how digital security perceptions and practices vary within and across seven WEIRD and five non-WEIRD countries through a large-scale cross-country survey ( $N=12,351$ ). Non-WEIRD participants reported higher familiarity with S&P terms, had higher risk perceptions of sensitive information types and possible attackers, adopted more information sources, but also experienced more cybercrimes. Below, we situate our key findings in prior work, interpret the WEIRD versus non-WEIRD differences, provide our reflections on operationalizing the WEIRD framework, and end with practical recommendations.

### 5.1 Situating Findings in Related Work

**Comparisons with prior cross-country studies.** We provide a detailed comparison between findings from our study and those from prior cross-country studies on similar topics in [Table 3](#). Several studies have covered similar dimensions, especially on trust and safety issues (related to [Section 4.4](#) on prior experience with cybercrime) and security behaviors (related to [Section 4.6](#) on adopted measures). However, to our knowledge, we are the first to quantify the cross-country variances for familiarity with terms, possible attackers, and information sources, building on prior qualitative [[55, 88](#)] and quantitative studies done in a single country [[89](#)].

It is also worth noting that even within the same dimension, the specific constructs often differ. For instance, Schoenebeck et al. examined perceptions of harms and remedies about online harassment broadly [[104](#)], whereas our study focuses on experiences with specific instances such as cyberbullying. Our study captured participants' perceived importance regarding 15 various data types, whereas Sharma et al. contextualized such perceptions in the context of COVID-19 contact tracing apps [[108](#)]. As such, our study provides complementary insights, but the construct-level differences also mean that the comparisons must be made with caution since many of the findings are not entirely comparable.

**Novel insights enabled by the WEIRD versus non-WEIRD comparisons.** While the WEIRD framework has various limitations — as we discuss more in [Section 5.3](#) — it provides a structured way for identifying and interpreting cross-country variances meaningfully. Compared to prior work that clustered countries based on Western versus non-Western [[43](#)], geographic location (e.g., identifying Asian or European countries as outliers) [[41, 103](#)], or used one country as the baseline for all pairwise comparisons [[43, 104](#)], the WEIRD versus non-WEIRD comparisons provide a more nuanced potential explanation for observed cross-country variances: factors such as a country's economy and system of governance also matter, in addition to where it is physically located.

Crucially, the WEIRD versus non-WEIRD comparisons do not take away the utility enabled by per-country analysis or pairwise country-level comparisons, which can still be derived from our descriptive statistics. For example, regarding device locking behavior, our study confirms the finding from Harbach et al. [[35](#)] that US participants less commonly adopted this measure, but the WEIRD versus non-WEIRD comparisons enabled us to identify that this measure was more commonly adopted among non-WEIRD participants.

**Antivirus and updates remain popular protective measures.** Beyond the WEIRD versus non-WEIRD comparisons, our study also identifies several universal patterns across most participants in ways that confirm, contrast, or add more nuances to prior work. As our participants reported being fairly involved in taking measures for protecting their digital security — all (98% NW; 96% W) reported taking at least one of the 14 queried measures — the most popular ones remain largely the same compared to prior work. Regular updates and the use of antivirus software were the top two adopted measures in our sample, used by at least 60% participants across WEIRD and non-WEIRD countries, and they were also among the most popular in several prior studies with US-based crowdworkers [[13, 53, 130](#)]. Measures related to device locking were also relatively popular in our sample (56% NW; 52% W), although the rates showed a small decline compared to Harbach et al.'s 2016 study with a different set of countries [[35](#)], likely because we inquired about a broader set of devices beyond smartphones. Notably, the average backup rates in our study were much higher than those reported in previous studies with US participants only [[123, 127](#)]. We also observe a similar trend as in Zou et al. [[130](#)]: the more popular measures can either be fully automated (such as antivirus software and ad blockers) or at least require limited user interactions (such as updates). Updates were the only exception. By contrast, PETs with more demanding setups (such as Tor and VPN) had low adoption rates across all countries.

**Friends and family as both information sources and possible attackers.** Another main finding across our WEIRD and non-WEIRD participants is the perception of dual roles

Table 3: Finding comparisons with prior cross-country studies on related topics.

Dimension		Topic	Year	Ref.	Countries	Prior Work Key Findings	Our Key Findings		
Sec.	Priv.	Saf.							
✓			Smartphone locking	2016	[35]	Australia, Canada, Germany, Italy, Japan, Netherlands, UK, USA	Users in most non-US countries were more likely to lock their screen; Japanese users considered smartphone content more sensitive, but also perceived locking to be inconvenient.	Device locking behavior (laptop, smartphone, tablet) was more common among non-WEIRD participants. US participants less commonly reported doing this than most other countries.	
✓			Security behavior	2017	[103]	China, Japan, South Korea, UAE, USA	France, Russia, Korea	Participants from Asian countries, especially Japan, exhibited less secure behavior (measured by SeBIS).	Focusing on a broader set of behaviors than SeBIS, we found WEIRD and non-WEIRD participants had different tastes for protective measures. We also measured actual adoption rather than intention.
✓			Account security	2019	[88]	Brazil, USA, Vietnam	Germany, India	Participants in the five countries shared a common process in responding to suspicious login attempts for their Facebook accounts: incident awareness, mental model generation, and behavioral response.	Non-WEIRD participants more commonly experienced unauthorized access to online accounts. We did not examine users' qualitative mental models toward suspicious logins.
	✓		Contact tracing	2021	[108]	27 countries		Users from the Global South were more comfortable sharing personal information and location data for contact tracing; Global North and Global South users converged on the motivation of using the apps and trusted non-profits.	Non-WEIRD participants attached more importance to various data types in general – which somewhat contradicts findings in Sharma et al. – although we did not focus on contact tracing.
✓	✓		S&P misconceptions	2023	[43]	12 countries		Higher misconceptions were found among non-Western countries (China, India, Mexico, Saudi Arabia, South Africa) compared to Western countries.	Our study was drawn from the same dataset, but the analysis used a completely different portion of the dataset. We also added the new WEIRD versus non-WEIRD comparisons rather than pairwise country-level comparisons with a fixed baseline.
		✓	Online harassment	2023	[104]	14 countries		Compared to the US, participants from all other countries exhibited higher perceptions of harms (especially insults, rumors, and harm to family reputation).	Related to online harassment, we examined participants' prior experience with cyberbullying. Non-WEIRD participants reported experiencing more cyberbullying than WEIRD participants.
✓	✓		S&P practices	2023	[116]	The Philippines, Brazil, Egypt, and Nigeria	India	The study examined respondents' knowledge of and attitude toward 14 S&P features (e.g., clearing browser history, password manager, and 2FA). No quantitative cross-country comparisons were made due to the study's qualitative nature.	Our study shared some overlap regarding the constructs for familiarity with terms and adopted protective measures. By comparison, we expanded the scope of included countries and quantified the cross-country differences. E.g., for 2FA, we found that WEIRD participants were more familiar with the term and more commonly adopted the measure.
		✓	Artificial intelligence	2023	[57]	10 countries		US participants expressed stronger privacy concerns surrounding AI, while China, Russia, and Japan are outliers where respondents reported lower privacy concerns.	Our study did not focus on AI or privacy concerns.
		✓	Smart home	2024	[23]	Germany, UK, USA	Mexico	Participants in Germany showed the most concern; participants in the US and Mexico were more likely to take precautions.	Our study did not focus on concerns or precautions related to smart homes.
		✓	Sextortion	2024	[41]	10 countries		Victimization was most common in the US, Australia, Mexico, and South Korea, and least common in Europe. Perpetration was common in South Korea, and least common in Belgium, Netherlands, Poland, and Spain.	Related to sextortion, we inquired participants' familiarity and prior experience with romance scams. Non-WEIRD participants were more familiar with the term and had more exposure. The highest exposure rates were in Saudi Arabia and South Africa.

played by friends and family. While participants turned to friends and family to obtain information about digital security (42% NW; 32% W), friends and family were also perceived as somewhat likely attackers to their own digital security ( $M_{NW}=2.39$ ,  $M_W=1.80$  for family members;  $M_{NW}=2.73$ ,  $M_W=1.99$  for friends or acquaintances). This connects the dots from prior work that individually shows the positive influence coming from friends and family on people's security attitudes and behaviors [22, 22, 76, 86, 86, 89, 126], as well as potential threats from social circles, e.g., in account and device sharing [72, 74] and intimate partner surveillance [115].

## 5.2 WEIRD versus Non-WEIRD Differences

Our study contributes the following key insights on how WEIRD versus non-WEIRD participants differed in their perceptions and behaviors related to digital security:

- Non-WEIRD participants reported being more familiar with most of the S&P technical terms we queried (14 out of 17).
- Non-WEIRD participants attached more importance to various data types; with significant but small differences.
- Non-WEIRD participants had higher risk perceptions for possible attackers, particularly for family members, friends/acquaintances, and colleagues.
- Non-WEIRD participants reported higher exposure across all nine types of cybercrime.

- Non-WEIRD participants reported higher adoption of information sources across different media and human sources.
- WEIRD and non-WEIRD participants exhibited different rates of adoption for protective measures. However, no group had significantly higher adoption rates than the other.

Some of these findings need to be contextualized further in the construct design and sample. For example, a surprising finding is that non-WEIRD participants reported higher familiarity with most S&P terms we queried, despite WEIRD countries' edge on the average educational level. Nevertheless, most of these differences are significant but small in size (e.g., 1% for “malware” and “ad blocker”).

Additionally, our online survey likely sampled more educated and tech-savvy participants from non-WEIRD countries compared to the general population, as they had similar device usage rates and higher smart home usage rates than our WEIRD participants (see [Table 2](#) and [Table 4](#)). Moreover, self-reported familiarity with a term does not guarantee correct mental models or appropriate usage of corresponding tools [43, 63, 122]. Taking this into account, our study does not directly contradict, but rather adds more nuances, to prior work that has found non-Western participants to exhibit more misconceptions [43] and less secure behaviors [103]. At the same time, our robustness check results (see [Table 7](#)) show that for most participants who reported experience with a certain cybercrime or adoption of a certain tool, they had at least a basic level of familiarity with the stated term.

While the familiarity gap can be contextualized, the general trend we observe across the WEIRD versus non-WEIRD differences is that non-WEIRD participants were more aware of potential digital security risks, more proactive in seeking information, but also more exposed. Non-WEIRD participants viewed the various information types as more worthy of protection and were more likely to perceive other people (particularly those from inner social circles) as possible attackers. Meanwhile, and unfortunately, non-WEIRD participants were also more affected by all nine types of cybercrimes.

### 5.3 Reflections on the WEIRD Framework

Our analysis is largely inspired by Hasegawa et al., which highlighted the alarmingly low representation of non-WEIRD countries in usable security and privacy literature [36]. By operationalizing the WEIRD framework in a large-scale online survey, we empirically show that differences exist between WEIRD and non-WEIRD countries across multiple attitudinal and behavioral dimensions related to digital security, and novel insights can be gleaned by expanding the scope of the investigation to non-WEIRD countries.

The WEIRD concept was first introduced by Henrich et al. to group countries in commonalities in measuring various psychological perceptions and decision-making processes [40]. The original article has been cited over 16k times, and the

application has extended to other domains, including evolution [7], archaeology [59], human-computer interaction [70], and AI ethics [106]. Compared to other frameworks that attempt to cluster countries (e.g., Global North versus Global South, developing versus developed, and Western versus non-Western), it also has a more granular classification system.

Nonetheless, just as any framework, this framework has its own limitations. For instance, one of the dimensions within WEIRD is Western versus non-Western, which is already a contested topic. Huntington's work [50] is a commonly used classification, but it has also been criticized by political science scholars who found contradictory empirical evidence [14]. While the dimensions of WEIRD are fixed, the specific sources and indices chosen across different studies to measure Western, Educated, Industrialized, Rich, and Democratic can also differ, leading to potentially different outcomes when classifying individual countries. Lastly, the WEIRD framework is meant to be fluid for its implementation: as geopolitics and societies keep evolving, a country can move between WEIRD versus non-WEIRD categories over the span of just a few years, e.g., due to changes in elections and political environments. While transparency on the specific indices and sources used to measure WEIRD helps reproducibility — as we did in [Section 3.2](#) — it also means that researchers should pay attention to potential metric-level differences when comparing different studies operationalizing WEIRD and refrain from attaching a fixed label to individual countries.

The fact that WEIRD operates at the country, rather than individual, level also suggests opportunities for future work. One direction could be re-analyzing our dataset by connecting the dependent variables to individual-level sociodemographic factors such as gender, age, and internet skills. Another direction could be replicating our results using cultural dimensions — which are not explicitly covered by the WEIRD framework, and also exhibit measurement variances across country versus individual levels [29]. While we consider these analyses out of the scope of this paper, we view them as important and promising directions for future work.

### 5.4 Practical Recommendations

**Align security advice with user behaviors.** Prior work has revealed substantial gaps between expert-recommended practices and end-user behaviors [90–92, 130]. Our findings, quantified in a large-scale cross-country survey, provide a few concrete pointers for how to close the gap at scale. Participants were largely sticking to low-effort, automated protective measures, reiterating the importance of making security- and privacy-enhancing tools easy to use or, even better, integrating the tools into users' existing workflows to reduce manual effort. We have seen the trend in password research where more recent work has shifted to encourage adoption by improving the user experience for password managers [49, 73] and

passkeys [65]. Meanwhile, antivirus education remains a persistent challenge for the security community: the adoption of antivirus software remains high among non-expert users, even though experts have long questioned its usefulness [13, 53].

**Interrogate root causes of threat models around friends and family.** While our work statistically quantifies the dual role of friends and family as both positive influencers and potential threats, future work — ideally qualitative research — is needed to uncover the root causes of such threat models. For instance, prior qualitative work done with South Asian women has provided valuable insights into *why* perceptions of household members being possible threats occur — due to device sharing and the broader gender role expectations around women that shape this practice [54, 64, 79, 101]. Prior work in Bangladesh has identified employees working in repairing sites could be viewed as another threat actor [3]. Interestingly, the pattern is not restricted to non-WEIRD settings, as Herbert et al. also identified the same pattern in their study with four at-risk populations in Germany, a WEIRD country [42]. To better understand how the dual roles are tied to the local social, cultural, and political landscapes, and to avoid improper generalizations that ignore the vast diversity within WEIRD or non-WEIRD clusters, we need in-depth and context-specific inquiries. These insights and use cases can feed into security awareness campaigns [9, 48, 58], as existing efforts still primarily emphasize threats from hackers and cybercriminals (rather than one’s close social circle).

**Innovate channels for security education.** Our finding that non-WEIRD participants were more proactive at seeking information about security reflects the huge potential for future work to tap into the specific news and social media platforms, particularly in non-WEIRD countries, and understand their roles in disseminating security knowledge as well as amplifying harmful content. By contrast, existing security research on media influence is still primarily based on Western contexts and English-only analysis [28, 87, 125]. As examples that head in this direction, recent work has started to explore how Douyin, the twin of TikTok in China, has become a hotbed for cybercrime learning [38] and pig butchering scams [33]. Other work has uncovered how cybercafe managers become an information source for users in Kenya, providing crucial, albeit sometimes inaccurate, advice on topics such as account creation and password management [78]. While these sources can be leveraged as innovative channels for security education and triggers for positive behaviors, infrastructural limitations, power politics, more collectivist norms around privacy can introduce additional dynamics and challenges [34].

**Invest more research and support for non-WEIRD populations.** The co-existence of high awareness yet high exposure underscores the need for more investigation and support for

non-WEIRD users. For instance, future work can bring in observational data to mitigate potential biases related to self-reported data. Incidents like malware could be overreported due to misconceptions [31, 111], e.g., when people take online tracking as malware [75], whereas scams face the underreporting problem [83], particularly in less affluent countries [47]. It is also possible that the gap between awareness and secure behaviors comes from the stages after initial awareness is acquired [11, 102]. Using the Security Learning Curve as a guideline [45], more attention, resources, and efforts could target the promotion of self-efficacy and embedding secure behavior into everyday activities for non-WEIRD users. Moreover, as no one would be perfectly safe even with the best self-defense mechanisms, we also need more interventions that strengthen non-WEIRD users’ resilience and access to information and support for recovery [47].

## Ethics Considerations

Since our institution does not have an ethics or institutional review board, we followed the best human subject research practices in the Menlo Report [119] and data protection guidelines from the General Data Protection Regulation (GDPR). Additionally, we consulted our institution’s data protection office to review our practices. Our panel provider agreed to abide by the ICC/ESOMAR Code of Conduct, which sets out ethical and professional obligations when conducting online surveys [52]. They also signed an agreement with us to comply with GDPR guidelines for all participants surveyed.

## Compliance with Open Science Policy

To enable open science, we share our anonymized dataset as an artifact of the publication via <https://doi.org/10.60517/ZW12Z533J>. In our published dataset, we have omitted all responses to Q5, as they have not yet been analyzed. One of the authors requires this content for their dissertation.

## Acknowledgments

Our work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany’s Excellence Strategy – EXC 2092 CASA – 390781972, by the PhD School “SecHuman – Security for Humans in Cyberspace” by the federal state of NRW, Germany, and by the Research Center Trustworthy Data Science and Security (<https://rc-trust.ai>), one of the Research Alliance Centers within the UA Ruhr (<https://uaruhr.de>). Collins W. Munyendo acknowledges partial support from the United States National Science Foundation under Grant Number 1845300. We thank Annalina Buckmann and Priyasha Chatterjee for their help. We would also like to thank all initial project members who co-designed the instrument in 2021.

## References

- [1] Norah Abokhodair, Adam Hodges, and Sarah Vieweg. Photo Sharing in the Arab Gulf: Expressing the Collective and Autonomous Selves. In *Proc. CSCW*, 2017.
- [2] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the Adoption of Secure Communication Tools. In *Proc. IEEE S&P*, 2017.
- [3] Syed Ishtiaque Ahmed, Shion Guha, Md Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proc. ICTD*, 2016.
- [4] 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.
- [5] Shaima Salah Alhashim and MM Hafizur Rahman. Cybersecurity Threats in Line with Awareness in Saudi Arabia. In *Proc. ICIT*, 2021.
- [6] Isak Andersson, Liza Bjursell, and Isak Palm. *Hack the Human: A qualitative research study exploring the human factor and social engineering awareness in cybersecurity and risk management among Swedish organizations*. PhD thesis, Jönköping University, 2023.
- [7] Coren Apicella, Ara Norenzayan, and Joseph Henrich. Beyond weird: A review of the last decade and a look ahead to the global laboratory of the future. *Evolution and Human Behavior*, 41(5):319–329, 2020.
- [8] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 2019.
- [9] Maria Bada, Angela M Sasse, and Jason RC Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*, 2019.
- [10] Mark Beyebach, Marie-Carmen Neipp, Ángel Solanes-Puchol, and Beatriz Martín-del Río. Bibliometric Differences Between WEIRD and Non-WEIRD Countries in the Outcome Research on Solution-Focused Brief Therapy. *Frontiers in Psychology*, 12:754885, 2021.
- [11] M Beyer, S Ahmed, K Doerlemann, S Arnell, S Parkin, A Sasse, and N Passingham. Hp enterprise-awareness is only the first step: a framework for progressive engagement of staff in cyber security, 2015.
- [12] Max Boholm. Twenty-five years of cyber threats in the news: a study of swedish newspaper coverage (1995–2019). *Journal of Cybersecurity*, 7(1), 2021.
- [13] 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.
- [14] Giacomo Chiozza. Is there a clash of civilizations? evidence from patterns of international conflict involvement, 1946-97. *Journal of peace research*, 39(6):711–734, 2002.
- [15] Claudia Lanza and Béatrice Daille. Terminology systematization for cybersecurity domain in italian language. *Actes de la Conférence sur le Traitement Automatique des Langues Naturelles (TALN) PFIA 2019. Terminologie et Intelligence Artificielle (atelier TALN-RECITAL & IC)*, pages 7–18, 2019.
- [16] Jacob Cohen. A power primer. In *Methodological Issues and Strategies in Clinical Research*. American Psychological Association, 2016.
- [17] 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.
- [18] Tom Crick, James H. Davenport, Paul Hanna, Alastair Irons, and Tom Prickett. Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes. In *Proc. ESD*, 2020.
- [19] Tom Crick, James H. Davenport, Alastair Irons, and Tom Prickett. A uk case study on cybersecurity education and accreditation. In *Bridging education to the future*, pages 1–9. IEEE, 2019.
- [20] Adéle Da Veiga and Jacques Ophoff. Concern for information privacy: a cross-nation study of the United Kingdom and South Africa. In *Proc. HAISA*, 2020.
- [21] Sauvik Das, Cori Faklaris, Jason I Hong, Laura A Dabbish, et al. The Security & Privacy Acceptance Framework (SPAF): A Review of Why Users Accept or Reject Cybersecurity and Privacy Best Practices. *Foundations and Trends® in Privacy and Security*, 5(1-2):1–143, 2022.

- [22] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. The Effect of Social Influence on Security Sensitivity. In *Proc. SOUPS 2014*, 2014.
- [23] Tess Despres, Marcelino Ayala Constantino, Naomi Zacarias Lizola, Gerardo Sánchez Romero, Shijing He, Xiao Zhan, Noura Abdi, Ruba Abu-Salma, Jose Such, and Julia Bernd. “My Best Friend’s Husband Sees and Knows Everything”: A Cross-Contextual and Cross-Country Approach to Understanding Smart Home Privacy. In *Proc. PETS*, 2024.
- [24] Jayati Dev, Pablo Moriano, and L. Jean Camp. Lessons Learnt from Comparing WhatsApp Privacy Concerns Across Saudi and Indian Populations. In *Proc. SOUPS*, 2020.
- [25] Serge Egelman and Eyal Peer. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proc. CHI*, 2015.
- [26] EIU. Democracy Index 2023, 2023. <https://www.eiu.com/n/campaigns/democracy-index-2023/>, as of January 30, 2025.
- [27] European Union Agency for Cybersecurity. ENISA Threat Landscape 15 Top Threats in 2020, October 2020. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats>, as of January 30, 2025.
- [28] 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.
- [29] Reza Ghaiumy Anaraky, Yao Li, and Bart Knijnenburg. Difficulties of Measuring Culture in Privacy Studies. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–26, 2021.
- [30] Samuel D Gosling, Carson J Sandy, Oliver P John, and Jeff Potter. Wired but not WEIRD: The promise of the Internet in reaching more diverse samples. *Behavioral and Brain Sciences*, 33(2-3):94, 2010.
- [31] Stjepan Groš. Myths and misconceptions about attackers and attacks. *arXiv preprint arXiv:2106.05702*, 2021.
- [32] Nada Hamadeh, Catherine Van Rompaey, Eric Metreau, and Shwetha Grace Eapen. New World Bank country classifications by income level: 2022-2023, 2022. <https://blogs.worldbank.org/en/opendata/new-world-bank-country-classifications-income-level-2022-2023>, as of January 30, 2025.
- [33] Bing Han. *Individual Frauds in China: Exploring the Impact and Response to Telecommunication Network Fraud and Pig Butchering Scams*. PhD thesis, Ph. D. thesis. University of Portsmouth, 2023.
- [34] SM Taiabul Haque, MD Romael Haque, Swapnil Nandy, Priyank Chandra, Mahdi Nasrullah Al-Ameen, Shion Guha, and Syed Ishtiaque Ahmed. Privacy Vulnerabilities in Public Digital Service Centers in Dhaka, Bangladesh. In *Proc. ICISDM*, 2020.
- [35] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. Keep on Lockin’ in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proc. CHI*, 2016.
- [36] Ayako A Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. How WEIRD is Usable Privacy and Security Research? In *Proc. USENIX Security*, 2024.
- [37] Ayako A Hasegawa, Naomi Yamashita, Mitsuaki Akiyama, and Tatsuya Mori. Why They Ignore English Emails: The Challenges of Non-Native Speakers in Identifying Phishing Emails. In *Proc. SOUPS*, 2021.
- [38] Chengchen He and Xia Luo. Life sharing or crimes sharing: an investigation on crime learning from china short-form video platforms. *Information & Communications Technology Law*, 32(2):240–258, 2023.
- [39] Tom Hendriks, Meg A Warren, Marijke Schotanus-Dijkstra, Aabidien Hassankhan, Tobi Graafsma, Ernst Bohlmeijer, and Joop de Jong. How weird are positive psychology interventions? a bibliometric analysis of randomized controlled trials on the science of well-being. *The Journal of Positive Psychology*, 14(4):489–501, 2019.
- [40] Joseph Henrich, Steven J Heine, and Ara Norenzayan. The weirdest people in the world? *Behavioral and brain sciences*, 33(2-3):61–83, 2010.
- [41] Nicola Henry and Rebecca Umbach. Sextortion: Prevalence and correlates in 10 countries. *Computers in Human Behavior*, 158:108298, 2024.
- [42] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Duermuth, 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.

- [43] 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.
- [44] Cormac Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proc. NSPW*, 2009.
- [45] Jonas Hielscher, Annette Kluge, Uta Menges, and M Angela Sasse. “taking out the trash”: Why security behavior change requires intentional forgetting. In *Proc. NSPW*, 2021.
- [46] Geert Hofstede. *Culture’s Consequences: International Differences in Work-Related Values*. Sage, 1984.
- [47] Mo Houtti, Abhishek Roy, Venkata Narsi Reddy Gangu, and Ashley Marie Walker. A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries. *Journal of Online Trust & Safety*, 12(4), 2024.
- [48] Siqi Hu, Carol Hsu, and Zhongyun Zhou. Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems*, 62(4):752–764, 2022.
- [49] Nicolas Huaman, Sabrina Amft, Marten Oltrogge, Yasemin Acar, and Sascha Fahl. They Would do Better if They Worked Together: The Case of Interaction Problems Between Password Managers and Websites. In *Proc. IEEE S&P*, 2021.
- [50] Samuel P Huntington and Robert Jervis. The clash of civilizations and the remaking of world order. *Finance and Development-English Edition*, 34(2):51–51, 1997.
- [51] IMF. World Economic Outlook (April 2024), 2024. <https://www.imf.org/external/datamapper/datasets/WEO>, as of January 30, 2025.
- [52] International Chamber of Commerce and European Society for Opinion and Marketing Research. International Code on Market and Social Research, December 2007. <https://iccwbo.org/publication/iccesomar-international-code-on-market-and-social-research/>, as of January 30, 2025.
- [53] Iulia Ion, Rob Reeder, and Sunny Consolvo. “...no one can hack my mind”: Comparing expert and non-expert security practices. In *Proc. SOUPS*, 2015.
- [54] Pranjal Jain, Rama Adithya Varanasi, and Nicola Dell. “Who is protecting us? No one!” Vulnerabilities Experienced by Low-Income Indian Merchants Using Digital Payments. In *Proc. COMPASS*, 2021.
- [55] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara B. Kiesler. “My Data Just Goes Everywhere:” User Mental Models of the Internet and Implications for Privacy and Security. In *Proc. SOUPS*, 2015.
- [56] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. Human factors in security research: Lessons learned from 2008-2018. *arXiv preprint arXiv:2103.13287*, 2021.
- [57] Patrick Gage Kelley, Celestina Cornejo, Lisa Hayes, Ellie Shuo Jin, Aaron Sedley, Kurt Thomas, Yongwei Yang, and Allison Woodruff. “There will be less privacy, of course”: How and why people in 10 countries expect AI will affect privacy in the future. In *Proc. SOUPS*, 2023.
- [58] Khando Khando, Shang Gao, Sirajul M Islam, and Ali Salman. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 106:102267, 2021.
- [59] Anton Killin and Ross Pain. How weird is cognitive archaeology? engaging with the challenge of cultural variation and sample diversity. *Review of Philosophy and Psychology*, 14(2):539–563, 2023.
- [60] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. “When I Am on Wi-Fi, I Am Fearless”: Privacy Concerns & Practices in Everyday Wi-Fi Use. In *Proc. CHI*, 2009.
- [61] Luisa Parraguez Kobek. The state of cybersecurity in mexico: An overview. *Wilson Centre’s Mexico Institute*, Jan, 2017.
- [62] Elmarie Kritzinger, Maria Bada, and Jason R. C. Nurse. A study into the cybersecurity awareness initiatives for school learners in south africa and the uk. In *Information Security Education for a Global Digital Society*, pages 110–120. Springer, Cham, 2017.
- [63] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. “If HTTPS Were Secure, I Wouldn’t Need 2FA” – End User and Administrator Mental Models of HTTPS. In *Proc. IEEE S&P*, 2019.
- [64] Ponnurangam Kumaraguru and Niharika Sachdeva. Privacy4ictd in india: Exploring perceptions, attitudes and awareness about ict use. *arXiv: Computers and Society*, 2014.

- [65] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In *Proc. USENIX Security*, 2024.
- [66] Rodda Leage and Ivana Chalmers. Degrees of caution: Arab girls unveil on Facebook. *Girl wide web*, 2:27–44, 2010.
- [67] Yao Li. Cross-Cultural Privacy Differences. In Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano, editors, *Modern Socio-Technical Perspectives on Privacy*, pages 267–292. Springer International Publishing, Cham, 2022.
- [68] Yao Li, Alfred Kobsa, Bart P Knijnenburg, M-H Carolyn Nguyen, et al. Cross-Cultural Privacy Prediction. In *Proc. PETS*, 2017.
- [69] Calvin A Liang, Sean A Munson, and Julie A Kientz. Embracing four tensions in human-computer interaction research with marginalized people. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 28(2):1–47, 2021.
- [70] Sebastian Linxen, Christian Sturm, Florian Brühlmann, Vincent Cassau, Klaus Opwis, and Katharina Reinecke. How weird is CHI? In *Proc. CHI*, 2021.
- [71] Mary Madden. Privacy, security, and digital inequality. *Data & Society*, 2017.
- [72] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. “She’ll just grab any device that’s closer” A Study of Everyday Device & Account Sharing in Households. In *Proc. CHI*, 2016.
- [73] Peter Mayer, Collins W Munyendo, Michelle L Mazurek, and Adam J Aviv. Why Users (Don’t) Use Password Managers at a Large Educational Institution. In *Proc. USENIX Security*, 2022.
- [74] Michelle L Mazurek, JP Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, et al. Access Control for Home Data Sharing: Attitudes, Needs and Practices. In *Proc. CHI*, 2010.
- [75] William Melicher, Mahmood Sharif, Joshua Tan, Lujjo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. (Do Not) Track Me Sometimes: Users’ Contextual Preferences for Web Tracking. In *Proc. PETS*, 2016.
- [76] Lachlan Moore, Tatsuya Mori, and Ayako A Hasegawa. Negative Effects of Social Triggers on User Security and Privacy Behaviors. In *Proc. SOUPS*, 2024.
- [77] 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.
- [78] 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.
- [79] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–24, 2021.
- [80] New Jersey Cybersecurity & Communications Integration Cell. The Evolution of Ransomware: A 5-Year Perspective, 2023.
- [81] 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.
- [82] Annika Onemichl and Carolin Bolz. Digitalbarometer: Bürgerbefragung zur cyber-sicherheit 2022: Kurzbericht zur studie der polizeilichen kriminalprävention der länder und des bundes (propk) und des bundesamtes für sicherheit in der informationstechnik (bsi), 2022.
- [83] Katalin Parti and Faika Tahir. “If We Don’t Listen to Them, We Make Them Lose More than Money:” Exploring Reasons for Underreporting and the Needs of Older Scam Victims. *Social Sciences*, 12(5):264, 2023.
- [84] Denny Pencheva, Joseph Hallett, and Awais Rashid. Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, 18(2):68–74, 2020.
- [85] Michal Polasik and Tomasz Piotr Wisniewski. Empirical analysis of internet banking adoption in poland. *International Journal of Bank Marketing*, 27(1):32–52, 2009.
- [86] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as Informal Lessons about Security. In *Proc. SOUPS*, 2012.
- [87] Maike M Raphael, Aikaterini Kanta, Rico Seebonn, Markus Dürmuth, and Camille Cobb. Batman hacked my password: A subtitle-based analysis of password depiction in movies. In *Proc. SOUPS*, 2024.

- [88] Elissa M Redmiles. “Should I Worry?” A Cross-Cultural Examination of Account Security Incident Response. In *Proc. IEEE S&P*, 2019.
- [89] 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.
- [90] 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.
- [91] 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.
- [92] 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, October 2017.
- [93] Ken Reese, Trevor Smith, Jonathan Dutton, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A usability study of five two-factor authentication methods. In *Proc. SOUPS*, 2019.
- [94] 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.
- [95] Karen Renaud, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, and Craig Orgeron. Is the responsabilization of the cyber security risk reasonable and judicious? *Computers & Security*, 78:198–211, 2018.
- [96] Karen Renaud, Craig Orgeron, Merrill Warkentin, and P Edward French. Cyber security responsabilization: an evaluation of the intervention approaches adopted by the five eyes countries and china. *Public Administration Review*, 80(4):577–589, 2020.
- [97] Mohammad Rashidujjaman Rifat, Mahiratul Jannat, Mahdi Nasrullah Al-Ameen, SM Taiabul Haque, Muhammad Ashad Kabir, and Syed Ishtiaque Ahmed. Purdah, amanah, and gheebat: Understanding privacy in bangladeshi “pious” muslim communities. In *Proc. COMPASS*, 2021.
- [98] Bernd Rohrmann. Verbal Qualifiers for Rating Scales: Sociolinguistic Considerations and Psychometric Data. Technical Report VQSBR07, University of Melbourne, January 2007.
- [99] Rodrigo Ruiz. A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity. In *Proc. ICGS3*, 2019.
- [100] Nithya Sambasivan, Nova Ahmed, Amna Batool, Elie Bursztein, Elizabeth Churchill, Laura Sanely Gaytan-Lugo, Tara Matthews, David Nemer, Kurt Thomas, and Sunny Consolvo. Toward gender-equitable privacy and security in south asia. *IEEE Security & Privacy*, 17(4):71–77, 2019.
- [101] 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.
- [102] M Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In *Proc. ESORICS*, 2022.
- [103] 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.
- [104] 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.
- [105] Eva-Maria Schomakers, Chantal Lidynia, Dirk Müllmann, and Martina Zieffle. Internet users’ perceptions of information sensitivity—insights from germany. *International Journal of Information Management*, 46:142–150, 2019.
- [106] Ali Akbar Septiandri, Marios Constantinides, Mohammad Tahaei, and Daniele Quercia. WEIRD FAcT: How Western, Educated, Industrialized, Rich, and Democratic is FAcT? In *Proc. FAcT*, 2023.
- [107] Serianu, Limited. Africa Cyber Security Report 2016, October 2016. <https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf>, as of January 30, 2025.
- [108] Tanusree Sharma, Md Mirajul Islam, Anupam Das, SM Taiabul Haque, and Syed Ishtiaque Ahmed. Privacy during Pandemic: A Global View of Privacy Practices around COVID-19 Apps. In *Proc. COMPASS*, 2021.

- [109] Hong Shen, Cori Faklaris, Haojian Jin, Laura Dabbish, and Jason I Hong. 'I Can't Even Buy Apples If I Don't Use Mobile Pay?' When Mobile Payments Become Infrastructural in China. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–26, 2020.
- [110] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, Adoption, and Misconceptions of Web Privacy Tools. In *Proc. PETS*, 2021.
- [111] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. In *Proc. PETS*, 2021.
- [112] Paige L Sweet. Who Knows? Reflexivity in Feminist Standpoint Theory and Bourdieu. *Gender & Society*, 34(6):922–950, 2020.
- [113] Oskar Szumski. Cybersecurity best practices among polish students. *Procedia Computer Science*, 126:1271–1280, 2018.
- [114] Sarina Till and Melissa Densmore. A Characterization of Digital Native Approaches To Mobile Privacy and Security. In *Proc. SAICSIT*, 2019.
- [115] 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.
- [116] 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.
- [117] UNDP. Published: 2023-2024 Human Development Report, 2024. <https://hdr.undp.org/>, as of January 30, 2025.
- [118] UNESCO Institute for Statistics. International Standard Classification of Education: ISCED 2011, December 2012. <http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf>, as of January 30, 2025.
- [119] U.S. Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, August 2012. [https://www.caida.org/publications/papers/2012/menlo\\_report\\_actual\\_formatted/](https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/), as of January 30, 2025.
- [120] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining security and privacy research in developing regions. In *Proc. COMPASS*, pages 1–14, 2018.
- [121] Yang Wang, Gregory Norcie, and Lorrie Faith Cranor. Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. In *Proc. TRUST*, 2011.
- [122] Noel Warford, Collins W Munyendo, Ashna Mediratta, Adam J Aviv, and Michelle L Mazurek. Strategies and perceived risks of sending sensitive documents. In *Proc. USENIX Security*, 2021.
- [123] Rick Wash and Emilee Rader. Too Much Knowledge? Security Beliefs and Protective. In *Proc. SOUPS*, 2015.
- [124] 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.
- [125] 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.
- [126] Yuxi Wu, W Keith Edwards, and Sauvik Das. SoK: Social Cybersecurity. In *Proc. IEEE S&P*, 2022.
- [127] Yev. The 2022 Backup Survey: 54% Report Data Loss With Only 10% Backing Up Daily, June 2022. <https://www.backblaze.com/blog/the-2022-backup-survey-54-report-data-loss-with-only-10-backing-up-daily/>, as of January 30, 2025.
- [128] Armgard Zindler and Carolin Bolz. Digitalbarometer 2020: Bürgerbefragung zur Cyber-Sicherheit, September 2020. [https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI\\_2020.html](https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2020.html), as of January 30, 2025.
- [129] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Proc. SOUPS*, 2018.
- [130] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proc. SOUPS*, 2020.