

Unequal Risks: Ethnicity, Region, and Cybersecurity Outcomes in the United States

Venkata Sai Kaushik Reddy Mitta
Computing & Software Systems
University of Washington
Bothell, WA, USA
kaushik270602@gmail.com
0009-0004-5930-6028

Marc J. Dupuis
Computing & Software Systems
University of Washington
Bothell, WA, USA
marcjd@uw.edu
0000-0002-5303-2511

Abstract—Cybersecurity risks are often treated as uniform, yet disparities across demographic groups suggest otherwise. This study investigates how ethnicity and geographic region shape cybersecurity outcomes in the United States, focusing on victimization, tool adoption, and awareness. Survey data from 470 adult participants were analyzed using ANOVA, Kruskal–Wallis tests, chi-square analyses, and logistic regression models. There are a few key findings. First, Asian/Pacific Islander respondents reported higher awareness and greater use of protective tools; they also faced significantly elevated odds of identity theft, phishing losses, and account takeovers. Second, suburban residents exhibited higher preparedness than urban or rural populations, while also consistently experiencing greater exposure to cyber incidents, particularly financial fraud. Finally, Hispanic/Latinx and rural groups reported lower adoption of security tools, reflecting barriers of access and language. These findings highlight that awareness and adoption alone are insufficient when structural vulnerabilities and targeted exploitation are at play. The study underscores the need for culturally competent education, expanded infrastructure access, and adaptive monitoring systems to reduce disparities and promote a more equitable cybersecurity landscape.

Keywords—*cybersecurity disparities, demographic factors, cyber victimization, digital divide, ethnicity, regional differences*

I. INTRODUCTION

Cybersecurity threats have become a defining challenge of the digital age. Global reliance on digital infrastructure spans finance, healthcare, commerce, and communication, with cybercrime costs projected to rise from \$9.22 trillion in 2024 to more than \$13.82 trillion by 2028 [1]. Attackers now employ increasingly sophisticated tactics, from ransomware—which saw a 57% increase in claims from the fourth quarter of 2023 to the fourth quarter of 2024 [2]—to credential abuse, deepfakes, and AI-powered phishing. The rapid growth of synthetic media, expected to exceed 8 million instances by 2025 [3], illustrates how technology continues to expand the attack surface and erode trust. While technical defenses

evolve in response, the human and social dimensions of cybersecurity remain less understood.

A critical but underexplored aspect of cybersecurity involves demographic disparities. Traditional approaches often treat end users as a uniform population, overlooking how ethnicity, socioeconomic status, and regional context shape exposure to risk. Research suggests communities of color face higher rates of identity theft and reduced access to protective tools and education [4], [5]. Similarly, geographic setting matters: urban, suburban, and rural residents encounter different infrastructures, access levels, and targeting patterns. These disparities mirror broader social inequities, yet remain poorly integrated into cybersecurity research and practice.

The United States provides an important case study. Here, demographic inequities intersect with digital divides in ways that influence victimization, adoption of protective tools, and levels of awareness. Urban centers may attract large-scale attacks due to dense digital ecosystems, while rural communities struggle with limited access to secure infrastructure. Suburban populations, often more affluent and digitally dependent, can be particularly attractive to attackers. Understanding these dynamics requires moving beyond generic awareness campaigns to interventions tailored to specific contexts.

A. Research Objectives

This study addresses this gap by analyzing how ethnicity and geographic region influence cybersecurity outcomes by examining three underlying research questions:

1. **Victimization disparities:** Do different groups experience higher rates of cybercrime such as identity theft, fraud, or phishing?
2. **Tool adoption disparities:** Are protective technologies (e.g., multi-factor authentication, password managers, etc.) adopted unevenly across groups?
3. **Awareness disparities:** How do knowledge and confidence in managing cyber threats vary by ethnicity and region?

By investigating these questions with survey data from 470 U.S. participants, this study provides empirical evidence of demographic influences on cybersecurity outcomes.

B. Contributions

- Provides one of the first large-scale quantitative analyses of U.S. cybersecurity outcomes disaggregated by both ethnicity and region.
- Demonstrates that higher awareness and tool adoption do not necessarily equate to lower risk, highlighting potential paradoxes such as Asian/Pacific Islander respondents reporting both stronger protective practices and greater victimization.
- Identifies suburban residents as a concentrated risk cluster, underscoring that affluence and connectivity may increase rather than reduce exposure.

Together, these contributions underscore that cybersecurity is not solely a technical challenge, but also a social one. Protecting diverse populations requires culturally competent and contextually responsive strategies that address both structural inequities and evolving patterns of attack.

II. BACKGROUND

Cybersecurity is often treated as a primarily technical challenge, yet human and social factors significantly influence risk. Prior research highlights the importance of human error, disparities in adoption of protective tools, and structural inequities that shape digital vulnerability. This section reviews key areas of prior work and identifies the gaps this study addresses.

A. Human Factors in Cybersecurity

Technical defenses such as firewalls and intrusion detection systems are critical but insufficient if users fail to follow secure practices. Studies consistently show that most incidents involve human elements—phishing, misconfigurations, or mishandling of data [6]. Huang *et al.* argue that cyber risk assessments emphasize networks and software flaws while neglecting culture and behavior [7]. Awareness, prior experience, and organizational support all shape user compliance. Scholars increasingly call for holistic risk models that integrate human factors alongside technical vulnerabilities.

B. Technology Adoption in Security Contexts

Adoption of protective tools varies across individuals and organizations. Frameworks such as the Technology–Organization–Environment (TOE) model, the Diffusion of Innovation (DOI) theory, and the Technology Acceptance Model (TAM) help explain uptake. TOE emphasizes organizational and environmental contexts [8], DOI highlights compatibility and observability, and TAM focuses on perceived usefulness and ease of use [9]. Empirical studies identify predictors, such as management support and vendor credibility [10]. While useful, these models rarely consider

demographic variation, leaving open the question of whether adoption differs systematically across ethnic or regional groups.

C. Demographic Disparities in Behavior

Demographic characteristics shape cybersecurity practices in complex ways. A study of 421 healthcare system users found that education was the strongest predictor of secure behavior, followed by gender and age [11]. Women engaged in more protective practices, and older users tended to avoid risky behaviors. Beyond individuals, workforce disparities persist: women remain underrepresented, comprising about one-quarter of professionals, with even lower representation for Black women [12]. These findings point to both behavioral and structural inequities that limit participation and shape vulnerability.

D. Socioeconomic and Digital Divides

Socioeconomic status (SES) strongly influences cybersecurity preparedness. Lower SES groups face barriers such as limited access to broadband, reduced digital literacy, and fewer financial resources for tools. A survey of 758 students in Pakistan demonstrated that SES predicted both adoption of secure practices and victimization likelihood [13]. The stratification model of technology diffusion explains how new technologies often reinforce rather than reduce inequalities. Without targeted interventions, digital divides translate directly into cybersecurity gaps.

E. Geographic Variations in Cyber Risk

Cybercrime is unevenly distributed across regions, reflecting infrastructure, socioeconomic development, and attacker strategies. Globally, Eastern Europe has been a hub for attacking infrastructure [14]. Within countries, cybercrime often clusters in developed, densely populated areas such as London or U.S. metropolitan regions [15], [16]. In the U.S., suburban populations may be especially exposed due to reliance on online financial services and heavy Internet use, while rural populations face risk from lower preparedness. Thus, geography intersects with SES and infrastructure to shape exposure.

F. Measuring Awareness and Behavior

Robust measurement tools are essential for assessing disparities. Chaudhary *et al.* propose evaluation metrics based on impact, sustainability, accessibility, and monitoring [17]. Established instruments include the Human Aspects of Information Security Questionnaire (HAIS-Q) [18], the Security Behavior Intentions Scale (SeBIS), and the Cyber-victimisation Scale (CYBVICS) [19]. These tools capture behavior, intentions, and victimization. However, few studies apply them in ways that capture ethnic or regional differences.

G. Behavioral and Psychological Factors

Awareness does not always translate into secure action. Dual Process Theory explains how intuitive “System 1” decisions make users vulnerable to phishing, while deliberate “System 2” reasoning requires time and effort [20]. Prospect

Theory shows that loss aversion motivates compliance more strongly than potential gains [21]. Awareness programs that emphasize the consequences of inaction may therefore be more effective than those focused on positive benefits. These models highlight the role of cognitive biases in shaping security behaviors. Additionally, the inherent risk tolerance of individuals may vary, whether due to their past experiences or simply as a part of their personality traits [22].

H. Cultural and Social Dynamics

Cultural and social contexts also shape cybersecurity capacity. Research across 78 countries shows that cultural factors influence national practices, though economic development remains a stronger predictor [23]. Within professional communities, racial hierarchies persist, with individuals of equivalent qualifications sometimes receiving unequal recognition based on race or nationality [24]. These dynamics illustrate that disparities in cybersecurity extend beyond technical skills to broader systems of social stratification.

I. Research Gaps

Despite growing recognition of demographic influences, gaps remain. Many studies identify correlations without reliable frameworks for measuring disparities across contexts. Few integrate ethnicity and region simultaneously, limiting understanding of intersectional vulnerabilities. This study addresses these gaps by analyzing how demographic characteristics relate to victimization, tool adoption, and awareness in a U.S. sample of 470 participants.

III. METHODS

This study examined how ethnicity and geographic region influence cybersecurity outcomes in the United States. The analysis used survey data from 470 adult participants and applied descriptive, comparative, and regression-based methods to assess disparities in victimization, tool adoption, and awareness.

A. Data Collection

Data were collected through an online survey of U.S. residents aged 18 or older. IRB approval was sought and obtained prior to recruitment and data collection. Participation was voluntary and informed consent was obtained prior to their engagement with the survey. Prolific, a crowdsourcing platform, was used to recruit participants. Crowdsourcing platforms can be an efficient method to recruit participants, but quality control procedures must be implemented to ensure high quality data [25]–[27]. Additionally, while the sample may not be fully representative of the U.S. population at large, it is nonetheless much more diverse than the traditional methods used in the past (e.g., recruiting students from a college sophomore class) [28].

In the current study, eight quality control questions were embedded within the survey. This included repeated demographic questions at the beginning and end (they must match), simple questions with obvious answers (e.g., 'select

agree to get paid'), among other attention check type questions. In total, 6.15% that began the survey were rejected due to failing one or more quality control questions. The survey itself was completed online using the Qualtrics survey platform. Participants were compensated \$3.00 with most participants (79.9%) indicating that said compensation was comparable or easier for the compensation amount received when compared to similar projects. Based on a median completion time of about 15 minutes, the associated hourly rate was approximately \$12. The entire data collection process was completed within five days.

The instrument included items on demographic background, experiences related to cyber victimization, adoption of protective tools, and levels of awareness and confidence. Questions combined multiple-choice formats with Likert scales. Items were drawn from established measures, such as the HAIS-Q, SeBIS, and CYBVICS, adapted for brevity and survey feasibility.

B. Independent Variables

Two demographic characteristics were the focus:

- Ethnic identification: White (64.3%), Black/African American (12.5%), Hispanic/Latinx (8.5%), Asian/Pacific Islander (9.9%), Native American/Alaskan Native (0.8%), and Other (4.0%).
- Region: Urban (37.4%), Suburban (47.6%), and Rural (15.0%).

Additional variables such as age, gender identification, and education were collected, but not analyzed in detail here. Please see Table I.

TABLE I. Participant Demographics

Gender Identification	Percent
Female	40.2%
Male	57.1%
Non-Binary	2.5%
Prefer not to say	0.2%

Age	Percent
18-29	23.0%
30-39	35.7%
40-49	18.6%
50-59	11.0%
60+	11.7%

Education	Percent
Did not graduate high school	1.1%
Graduated high school (or equivalent)	14.4%
Some college, no degree	19.5%
Associate's degree	10.4%
Bachelor's degree	39.5%
Master's degree or higher	15.2%

C. Dependent Variables

Three outcome domains were analyzed:

1) *Victimization*: Participants reported whether they had experienced cyber incidents, including SSN compromise, fraudulent charges, account takeovers, tax fraud, phishing losses, ransomware, and password leaks. Outcomes were coded as binary (yes/no) for each incident type, with total incidents summed for count models.

2) *Tool Adoption*: Respondents indicated whether they used protective technologies, such as antivirus software, password managers, backups, VPNs, and multi-factor authentication. Usage was coded as binary and aggregated into a composite adoption score.

3) *Awareness and Confidence*: Awareness was measured by concern over phishing, fraud, and data protection, while confidence captured perceived ability to recognize and respond to threats. These were measured on Likert scales and analyzed as continuous and dichotomized outcomes.

D. Analytical Strategy

Analyses were conducted in R with scripts developed for reproducibility. The strategy proceeded in three stages:

1. **Descriptive statistics**: Baseline frequencies and averages for demographic and outcome variables.
2. **Group comparisons**: ANOVA and Kruskal–Wallis tests assessed differences across ethnic and regional groups. Pearson and Spearman correlations evaluated associations between demographics and outcomes. Chi-square tests examined categorical relationships.
3. **Regression modeling**: Logistic regression estimated odds of binary outcomes (e.g., SSN compromise). Poisson and negative binomial regressions modeled count outcomes (e.g., number of incidents, number of tools used). Where significant, ethnicity and region were tested as predictors while accounting for potential confounding.

Outputs were validated with cross-checks and exported directly to formatted tables for presentation. Emphasis was placed on transparency and methodological rigor, consistent with best practices in quantitative social science.

E. Summary

In summary, the survey provided a multidimensional view of cybersecurity disparities. Ethnicity and region were examined as predictors of victimization, adoption, and awareness, using a combination of descriptive statistics, group-level tests, and regression models to identify patterns of disparity.

IV. RESULTS

Findings are presented across three domains: cyber victimization, tool adoption, and awareness/confidence. Each domain is examined by ethnicity and region. Results move from group comparisons to regression modeling, with tables providing statistical detail.

A. Victimization Patterns

1) *By Ethnicity*: Descriptive statistics showed modest variation, with Asian/Pacific Islander respondents reporting higher average incident counts. Omnibus tests (ANOVA: $F = 1.102$, $p = 0.294$; Kruskal–Wallis: $\chi^2 = 10.005$, $p = 0.0751$) found no significant overall differences (see Table II). Correlations were weak. However, chi-square tests indicated a significant association for email account takeover ($p = 0.0400$), and logistic regression revealed Asian/Pacific Islanders had elevated odds of SSN compromise, fraudulent charges, account takeovers, and phishing losses ($p < 0.001$). Hispanic/Latinx respondents showed lower odds ($p = 0.0032$).

TABLE II. Victimization by Ethnicity

Test	Statistic	p	Result
ANOVA	$F = 1.102$	0.294	n.s.
Kruskal–Wallis	$\chi^2 = 10.005$	0.0751	n.s. (borderline)
Chi-Square	–	0.0400	sig. (Email A/T)
Logistic Reg.	–	< 0.001 – 0.0032	several sig.

2) *By Region*: Suburban residents reported slightly higher incident counts and rural the fewest. Overall differences were non-significant (ANOVA: $F = 0.006$, $p = 0.937$; Kruskal–Wallis: $\chi^2 = 2.5604$, $p = 0.278$) (see Table III). Chi-square revealed a marginal link with tax fraud ($p = 0.0229$). Logistic regression showed suburban respondents had consistently higher odds of SSN compromise, fraudulent charges, account takeovers, and tax fraud ($p < 0.001$).

TABLE III. Victimization by Region

Test	Statistic	<i>p</i>	Result
ANOVA	$F = 0.006$	0.937	n.s.
Kruskal-Wallis	$\chi^2 = 2.5604$	0.278	n.s.
Chi-Square	–	0.0229	marginal (Tax Fraud)
Logistic Reg.	–	< 0.001	suburban > others

B. Cybersecurity Tool Adoption

1) *By Ethnicity*: Tool use varied modestly, with Asian/Pacific Islanders reporting higher adoption of VPNs, backups, and password managers. ANOVA showed no significant difference ($p = 0.189$), while Kruskal-Wallis detected variation ($p = 0.001867$). Logistic regression confirmed Asian/Pacific Islanders were more likely to adopt advanced tools ($p < 0.001$). Native American/Alaskan Native respondents showed the lowest usage, though not statistically robust.

TABLE IV. Tool Adoption by Ethnicity

Test	Statistic	<i>p</i>	Result
ANOVA	–	0.189	n.s.
Kruskal-Wallis	–	0.001867	sig.
Chi-Square	–	0.051/0.0708	marginal (PM/VPN)
Logistic Reg.	–	< 0.001	API > others

2) *By Region*: Suburban residents reported the highest adoption and rural the lowest. ANOVA suggested marginal differences ($p = 0.0684$), and Kruskal-Wallis confirmed significance ($p = 0.04047$) (see Table V). Logistic regression showed suburban respondents were more likely to use VPNs, backups, and password managers ($p < 0.001$).

TABLE V. Tool Adoption by Region

Test	Statistic	<i>p</i>	Result
ANOVA	–	0.0684	n.s.
Kruskal-Wallis	–	0.04047	n.s.
Chi-Square	–	0.0783	marginal (PM mobile)
Logistic Reg.	–	< 0.001	suburban > others

C. Cyber Incident Experiences

1) *By Ethnicity*: Asian/Pacific Islander respondents reported consistently higher exposure across phishing, fraud, and account takeover. Omnibus tests showed no significant overall differences (ANOVA: $p = 0.873$; Kruskal-Wallis: $p = 0.088$) (see Table VI). Chi-square identified a link with fraud ($p = 0.0274$). Logistic regression confirmed elevated odds for Asian/Pacific Islanders across most incidents ($p < 0.001$).

TABLE VI. Incidents by Ethnicity

Test	Statistic	<i>p</i>	Result
ANOVA	$F = 0.026$	0.873	n.s.
Kruskal-Wallis	$\chi^2 = 9.582$	0.088	n.s.
Chi-Square	–	0.0274	sig. (Fraud)
Logistic Reg.	–	< 0.001	API > others

2) *By Region*: Suburban residents again showed greater exposure. ANOVA ($p = 0.474$) and Kruskal-Wallis ($p = 0.153$) were not significant, but logistic regression indicated higher odds for nearly all incidents among suburban respondents ($p < 0.001$) (see Table VII).

TABLE VII. Incidents by Region

Test	Statistic	<i>p</i>	Result
ANOVA	$F = 0.515$	0.474	n.s.
Kruskal-Wallis	$\chi^2 = 3.762$	0.153	n.s.
Logistic Reg.	–	< 0.001	suburban > others

D. Awareness and Confidence

1) *By Ethnicity*: No significant associations were found in correlations or chi-square tests, though logistic regression showed Asian/Pacific Islanders reported higher concern and confidence ($p < 0.001$) (see Table VIII). They were also more likely to view phones as more secure than computers.

TABLE VIII. Awareness by Ethnicity

Test	Statistic	<i>p</i>	Result
Correlations	–	> 0.05	weak
Chi-Square	–	> 0.05	n.s.
Logistic Reg.	–	< 0.001	API > others

2) *By Region*: Again, suburban residents reported the highest awareness and confidence. Correlation and chi-square tests were non-significant, but logistic regression showed consistently elevated concern and confidence ($p < 0.001$), along with stronger beliefs in phone security (see Table IX).

TABLE IX. Awareness by Region

Test	Statistic	p	Result
Correlations	–	> 0.05	weak
Chi-Square	–	> 0.05	n.s
Logistic Reg.	–	< 0.001	Suburban $>$ others

E. Summary

Across all analyses, two consistent patterns emerged: (1) Asian/Pacific Islander respondents combined higher awareness and tool adoption with higher victimization rates, and (2) suburban residents reported stronger preparedness but also elevated incident exposure. These findings may suggest that awareness and adoption alone are insufficient when demographic context and attacker strategies create disproportionate risk.

V. DISCUSSION AND CONCLUSION

This study examined how ethnicity and geographic region influence cybersecurity outcomes across victimization, tool adoption, and awareness. Results reveal that disparities are not explained solely by preparedness levels, but by structural vulnerabilities and attacker strategies. Two interesting findings stand out: 1) the high levels of Asian/Pacific Islander awareness, tool usage, and levels of compromise, and 2) the suburban vulnerability cluster.

A. The Asian/Pacific Islander Findings

Asian/Pacific Islander respondents reported higher awareness and adoption of protective tools, yet also experienced significantly greater odds of SSN compromise, fraudulent charges, account takeovers, and phishing losses. One possibility is that this may suggest that protective behaviors, while necessary, do not eliminate risk when groups are disproportionately targeted. High engagement with digital finance and technology may expand attack surfaces, while elevated confidence may lead to underestimation of sophisticated threats. The finding underscores that knowledge alone is insufficient against targeted exploitation. However, another possibility is that due to the frequency in which they have been targeted and fallen victim to such attacks, they are more likely to engage in protective behaviors. Causal inferences cannot be made, especially in the absence of strong theoretical underpinnings to help draw such conclusions. Other research in the cybersecurity domain has noted a similar, perhaps noted to be at times contradictory, finding [29].

B. Suburban Vulnerability Clusters

Suburban residents reported higher adoption of protective tools and greater awareness than urban or rural counterparts, yet consistently faced higher victimization rates across nearly all incident types. Similar to the other finding, multiple factors could explain the result. Perhaps affluence and connectivity can increase exposure. Heavy reliance on online banking, e-commerce, remote work, and IoT devices may create attractive targets for attackers. Logistic regression confirmed suburban residency as a strong predictor of risk, even when awareness levels were high. Alternatively, their experiences as victims may lead them to higher adoption rates of protective measures, such as the use of cybersecurity tools.

C. Implications for Policy and Practice

These findings highlight the need for interventions that are both universal and context-specific.

Culturally competent training: Hispanic / Latinx respondents showed lower adoption of tools, pointing to barriers in accessibility. Tailored programs delivered in Spanish and through trusted community organizations can help bridge gaps. Similar approaches are applicable to other immigrant and non-English-speaking groups.

Addressing structural barriers: Rural residents reported lower tool adoption, reflecting infrastructure and affordability challenges. Expanding broadband access, subsidizing protective tools, and deploying mobile education initiatives would improve resilience.

Regional risk mitigation: Suburban communities require targeted responses such as neighborhood-level awareness campaigns, enhanced IoT monitoring, and partnerships with financial institutions to detect fraud. These measures reflect best practices, but should prioritize regions with the greatest exposure.

Corporate and technical strategies: Financial institutions and technology providers should design fraud detection systems that adapt to evolving attack patterns without reinforcing demographic bias. Adaptive monitoring can protect disproportionately targeted groups, such as Asian/Pacific Islander users, while improving security for all.

D. Limitations

The study has several limitations. First, given that all of the data we obtained was self-reported, social desirability bias is a concern [30]. While some of the procedures employed mitigate the risk of social desirability bias playing a significant role (e.g., participants were anonymous to the research team), it nonetheless cannot be ruled out completely. Second, a single research method was employed—a survey; therefore, common method bias is a concern [31], [32]. The use of quality control questions and different instrument types within the survey itself may mitigate it some, it nonetheless remains a concern. Third, while the sample size ($N=470$) was adequate for initial exploration, subgroup sizes were uneven, limiting power for certain comparisons. Finally, socioeconomic and

occupational data were not incorporated, though these factors likely mediate outcomes. Fourth, the cross-sectional design captures only a snapshot in time, preventing causal conclusions.

E. Future Research

Future studies should include larger, more representative samples, especially for underrepresented groups. Longitudinal designs could capture how risks and behaviors evolve, while integration of objective behavioral data (e.g., confirmed breach records, tool usage logs) would reduce reliance on self-reporting. Longitudinal studies would also help clarify the time-order sequence of events, which would allow us to better infer possible causal relationships in the absence of experimentation.

Additionally, comparative studies across countries would clarify whether the findings identified here are unique to the U.S. or reflect global trends. Examining attacker strategies is also crucial, as targeted exploitation may be driving disparities. Finally, there are other factors not directly examined here that may interact with those that were studied, such as fear and other emotions, especially when confronted with specific threats [33]. It is possible that some of the questions raised here could be answered, at least in part, by those other factors.

F. Conclusion

This research demonstrates that cybersecurity disparities reflect more than differences in awareness or adoption. Demographic characteristics, structural conditions, and targeting strategies intersect to create unequal outcomes. Asian/Pacific Islander respondents, despite stronger preparedness, reported higher victimization, while suburban residents showed similar findings. Hispanic/Latinx and rural populations faced gaps in access and adoption.

The findings highlight that cybersecurity is both technical and social. Addressing disparities requires culturally competent education, structural investment in digital infrastructure, and adaptive monitoring systems responsive to diverse contexts. By integrating demographic insights into policy and practice, stakeholders can move toward a more equitable and resilient digital future.

REFERENCES

- [1] A. Fleck, *Cybercrime Expected To Skyrocket in Coming Years*. Statista: <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>, Feb. 2024.
- [2] C. Mohr, S. Cozzolino, D. An, and W. Burns, *Global Cyber Threat Intelligence (CTI) Annual Cyberthreat Trends Report - 2024*. Deloitte, Mar. 2025.
- [3] N. Jacobson, *Deepfakes and Their Impact on Society*. CPI OpenFox: <https://www.openfox.com/deepfakes-and-their-impact-on-society/>, 2024.
- [4] J. P. Mello Jr., *Researchers Find Cyberattack Discrepancies Based on Race, Gender*. Tech News World: <https://www.technewsworld.com/story/researchers-find-cyberattack-discrepancies-based-on-race-gender-87288.html>, 2021.
- [5] A. Layne, L. Liu, C. Akanaga, and G. Comert, "Why race and place matter: Examining the intersection of cybersecurity and digital equity," *Journal of Black Studies*, pp. 28–50, 2025. doi: 10.1177/00219347251358957
- [6] N. Al-Hashem and A. Saidi, "The psychological aspect of cybersecurity: Understanding cyber threat perception and decision-making," *International Journal of Applied Machine Learning and Computational Intelligence*, vol. 13, no. 8, pp. 11–22, 2023.
- [7] J. U. Wenjing Huang, Sasha Romanosky, "Beyond Technicalities: Assessing Cyber Risk by Incorporating Human Factors," in *Proceedings of the Workshop on the Economics of Information Security (WEIS) 2024*, University of Texas at Dallas, 2024.
- [8] S. Wallace, K. Y. Green, C. Johnson, J. Cooper, and C. Gilstrap, "An extended toe framework for cybersecurity-adoption decisions," *Communications of the Association for Information Systems*, vol. 47, no. 1, p. 51, 2020. doi: 10.17705/1CAIS.04716
- [9] W. Fallatah, J. Kaˆvrestad, and S. Furnell, "Establishing a model for the user acceptance of cybersecurity training," *Future Internet*, vol. 16, no. 8, p. 294, 2024. doi: 10.3390/fi16080294
- [10] A. H. Mumtaz and A. Nalin, "A conceptual model for the organisational adoption of information system security innovations," *Journal of Computer Engineering & Information Technology*, 2017. doi: 10.48550/arXiv.1704.03867
- [11] P. K. Sari, P. W. Handayani, and A. N. Hidayanto, "Demographic comparison of information security behavior toward health information system protection: Survey study," *JMIR Formative Research*, vol. 7, no. 1, p. e49439, 2023. doi: 10.2196/49439
- [12] M. L. Crosby, "The underrepresentation of black females in cybersecurity," *ODU Digital Commons*, 2023. doi: 10.25777/xkz2-7f78
- [13] N. F. Khan, N. Ikram, and S. Saleem, "Effects of socioeconomic and digital inequalities on cybersecurity in a developing country," *Security Journal*, p. 1, 2023. doi: 10.1057/s41284-023-00375-4
- [14] S. Chen, M. Hao, F. Ding, D. Jiang, J. Dong, S. Zhang, Q. Guo, and C. Gao, "Exploring the global geography of cybercrime and its driving forces," *Humanities and Social Sciences Communications*, vol. 10, no. 1, pp. 1–10, 2023. doi: 10.1057/s41599-023-01560-x
- [15] J. Zhuo, M. Hao, F. Ding, J. Dong, D. Jiang, and S. Chen, "The spatiotemporal patterns and driving factors of cybercrime in the uk during the covid-19 pandemic," *Humanities and Social Sciences Communications*, vol. 11, no. 1, pp. 1–10, 2024. doi: 10.1057/s41599-024-04051-9
- [16] M. E. Kwangmin Jung and J. Cho, "Spatial loss clusters and socio-economic drivers of cyber risks," *preprint available at SSRN*, 2023.
- [17] S. Chaudhary, V. Gkioulos, and S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," *Journal of Cybersecurity*, vol. 8, no. 1, pp. 1–19, 2022. doi: 10.1093/cybsec/tyac006
- [18] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (hais-q): two further validation studies," *Computers & Security*, vol. 66, pp. 40–51, 2017. doi: 10.1016/j.cose.2017.01.004
- [19] S. Buelga, B. Martínez-Ferrer, M.-J. Cava, and J. Ortega-Baroˆn, "Psychometric properties of the cybvics cyber-victimization scale and its relationship with psychosocial variables," *Social Sciences*, vol. 8, no. 1, p. 13, 2019. doi: 10.3390/socsci8010013
- [20] D. Kahneman, "Thinking, fast and slow," *Farrar, Straus and Giroux*, 2011.
- [21] A. R. Pratama and F. M. Firmansyah, "Until you have something to lose! loss aversion and two-factor authentication adoption," *Applied Computing and Informatics*, vol. 21, no. 1/2, pp. 53–64, 2025. doi: 10.1108/ACI-12-2020-0156
- [22] M. Dupuis, R. Crossler, and B. Endicott-Popovsky, "The information security behavior of home users: Exploring a user's risk tolerance and past experiences in the context of backing up information," in *The Dewald Roode Information Security Workshop*, (Provo, Utah), 2012.

- [23] S. Creese, W. H. Dutton, and P. Esteve-González, "The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions," *Personal and ubiquitous computing*, vol. 25, no. 5, pp. 941–955, 2021. doi: 10.1007/s00779-021-01569-6
- [24] D. Mumford and J. Shires, "Race and coloniality in cybersecurity," *E-International Relations*, 2023.
- [25] M. Dupuis, K. Renaud, and R. Searle, "Crowdsourcing quality concerns: An examination of amazon's mechanical turk," in *The 23rd Annual Conference on Information Technology Education*, (Chicago IL USA), p. 127–129, ACM, sept 2022. doi: 10.1145/3537674.3555783
- [26] M. Dupuis, B. Endicott-Popovsky, and R. Crossler, "An analysis of the use of amazon's mechanical turk for survey research in the cloud," in *International Conference on Cloud Security Management*, (Seattle, Washington), Oct. 2013.
- [27] G. Paolacci, J. Chandler, and P. Ipeirotis, "Running experiments on amazon mechanical turk," *Judgment and Decision Making*, vol. 5, no. 5, p. 411–419, 2010. doi: 10.1017/S1930297500002205
- [28] D. O. Sears, "College sophomores in the laboratory: Influences of a narrow data base on social psychology's view of human nature.," *Journal of Personality and Social Psychology*, vol. 51, no. 3, p. 515, 1986. doi: 10.1037/0022-3514.51.3.515
- [29] M. Dupuis and R. Crossler, "The compromise of one's personal information: Trait affect as an antecedent in explaining the behavior of individuals," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, (Maui, Hawaii), p. 4841–4850, IEEE, 2019. doi: 10.24251/HICSS.2019.584
- [30] A. J. Nederhof, "Methods of coping with social desirability bias: A review," *European Journal of Social Psychology*, vol. 15, no. 3, p. 263–280, 1985. 10.1002/ejsp.2420150303
- [31] S. B. MacKenzie and P. M. Podsakoff, "Common method bias in marketing: Causes, mechanisms, and procedural remedies," *Journal of retailing*, vol. 88, no. 4, p. 542–555, 2012. doi: 10.1016/j.jretai.2012.08.001
- [32] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies.," *Journal of applied psychology*, vol. 88, no. 5, p. 879, 2003. doi: 10.1037/0021-9010.88.5.879
- [33] M. Dupuis, K. Renaud, and A. Jennings, "Fear might motivate secure password choices in the short term, but at what cost?," in *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS) 2022*, (Maui, Hawaii), p. 4796–4805, Jan. 2022. doi: 10.24251/HICSS.2022.585