How Awareness Shapes Online Risk – Insights from Nigerian Internet Users

Akela Villegas

September 28, 2025

CYSE 201S: Cybersecurity & Social Science

Abstract

This review looks at the article *Emerging Trends in Cybercrime Awareness in Nigeria* by Nzeakor, Nwokeoma, Hassan, Ajah, and Okpa (2022). The authors explore data from 1,104 internet users in Umuahia, Abia State, Nigeria on how they understand different cybercrime types and how that awareness connects to personal experiences of victimization. The survey shows that people are most likely to have knowledge of common crimes like fraud, but they know far less about threats like identity theft or cyberterrorism. It was found that those with higher awareness reported more victimization. This finding brings forth challenges that more knowledge means less risk and highlights the need for prevention strategies, not just awareness campaigns.

Connection to Social Science Principles

This study directly reflects social science principles by exploring how knowledge, risk, and behavior coincide with a specific cultural setting. It relates to routine activity theory because Internet users' online routines create opportunities for motivated offenders. It also connects to social learning theory, as people's awareness often comes from seeing or hearing about others' experiences. It also highlights the digital divide with the unequal distribution of digital literacy that can leave groups more vulnerable to cybercrime.

Research Question, Hypotheses, IV & DV

- Research Question: How aware are Internet users in Umuahia of different cybercrime types and does that awareness influence their experience of victimization?

- Hypothesis: The authors anticipate that higher awareness would go hand in hand with lower victimization, but they found the opposite.
- Independent Variable (IV): Level of awareness across cybercrime categories like identity theft, fraud, hacking, and much more.
- Dependent Variable (DV): Self- reported experience of being a victim of cybercrime

Research Methods, Data, & Analysis

The researchers used a quantitative survey with structed questions. They gathered demographic information, asked about awareness of several cybercrime types, and collected self reports of victimization. The data was analyzed with descriptive statistics and tests to compare awareness between groups and to examine how awareness related to victimization.

Relation to Course Concepts

The findings relate to several ideas from our course materials:

- Risk perception: knowing about a risk does not necessarily change how people act online
- Victim precipitation: even if a person is aware of general online threats, some online behaviors may cause one to unintentionally increase their personal risk
- Marginalization: groups with less access to digital literacy programs or education which can lead to less awareness and increase harm

Marginalized Groups: Challenges, Concerns, & Contributions

Although the article does not specifically call out marginalized groups, its setting in Umuahia, Nigeria naturally highlights populations who have less access to digital infrastructure, reliable internet, and education. Nzeakor et al. (2022) report that awareness of cybercrime is uneven across the sample, showing participants with more education or higher income tend to come across a wider range of cyber threats, whereas participants with limited schooling or access to technology recognize fewer. Even when they are aware of cybercrime, marginalized groups may have fewer resources to recover from victimization like no access to legal support, banks, or strong consumer protections. By documenting these gaps, the study contributes indirectly to understanding how structural inequalities shape cybercrime risk and helps policy makers see where targeted interventions are needed.

Contribution to Society

This study shows that awareness alone is not enough. By identifying which cybercrimes types people know least about, it helps educations, governments, and organizations design targeted campaigns. This would mean smarter allocation of training resources and more inclusive outreach so that vulnerable groups are not left behind.

Conclusion

Nzeakor et al. (2022) provides a clear, data-driven perspective of cybercrime awareness in Nigeria. Their work demonstrates how social science methods like surveys, analysis of behaviors, and hypothesis testing can show gaps between knowledge and protection. Future research should focus on why awareness sometimes coincides with greater victimization and should never forget the marginalized voices. Overall, the article makes a meaningful contribution to both cybersecurity policy and the broader understanding of how humans navigate digital risk.

References

Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., & Okpa, J. T. (2022, November 2). *Emerging trends in cybercrime awareness in Nigeria*. Virtual Commons – Bridgewater State University. https://vc.bridgew.edu/ijcic/vol5/iss3/4/