Derrick Amissah

10/1/25

CYSE 201S

   Article Review #1: Pattern of Cybercrime Abuse of Individual Internet Users in Nigeria

The study finds that in southeastern Nigeria, most young internet users face cybercrime, especially gadget theft and online fraud.

Introduction

The article "Pattern of Cybercrime Abuse of Individual Internet Users in Nigeria" by Nzeakor, Okafor, and Nwoke (2025) examine what pattern of abuse resulted in Nigerian internet users in Umuahia North LGA, Abia State, Nigeria faced after becoming victims of cybercrime. This article is a contributor to knowledge since they focus in the South-eastern region of Nigeria, which has been far less studied than other geographic regions of Nigeria. The authors demonstrate the connection of being a cybercrime victim to social science theories of criminology, while describing the local social and economic challenges that are present the South-eastern region of Nigeria (Nzeakor et al., 2025, p. 61).

Association to Social Science Principles

The best way to explain cybercrime, and in particular cyberbullying, is to apply different measures from various social science disciplines. Psychology offers the emotional impacts on the victims, the reasons these acts are committed, including stress, sadness and how online reduces self-control, among others. Sociology examines cyberbullying as a group phenomenon, as a peer prefigured an online community. Deviant Place Theory states that people will have more risk

when they are online or in a physical unsafe environment consequently. (Nzeakor et al., 2025, p. 63). Anthropology illustrates how the cultural and local customs of southeastern Nigeria affect the nature of cyberbullying and how a community reacts (Nzeakor et al., 2025, p. 61). Criminology highlights the definition of abuse online, who they victimized, and possible responses law enforcement can take to limit these crimes (Nzeakor et al., 2025, pp. 67–68). Communication studies detail how harmful behaviors are shared, increased, and misinterpreted through various digital settings, some allowing for both good and bad encounters (Nzeakor et al., 2025, pp. 65–66). Although lens do not always overlap, combining evidence demonstrates that no one discipline will fully explain the causes, occurrences and solutions concern items like cyberbullying.

Research Questions, Hypotheses, and Variable

A cross-sectional survey method was implemented, and 1,067 individuals were randomly selected from a population of over 223,000 internet users in Umuahia North LGA using multistage cluster and systematic sampling procedures. The survey was started and was supported by in depth interviews and semi structured discussions with police officers to validate findings (Nzeakor et al., 2025, p.65). The primary instrument used a semi structured questionnaires demographic component, and different scales probing victimization. Data were analyzed using SPSS for descriptive and inferential statistics, with t-tests used to compare dimensions of cybercrime victimization from a participant and police officer perspective. The instrument was pilot tested for usability and then had test retest measures conducted to ensure that it was both reliable and valid (Nzeakor et al., 2025, p.66).

Data and Analysis

The study utilized both quantitative data generated from surveys and qualitative data generated from interviews. The quantitative data indicated that 95% of respondents had been targeted by some form of cybercrime, which is a very high prevalence (Nzeakor et al., 2025, p. 67). A deeper dive into the qualitative data revealed that the most common forms of cybercrime were property-related cybercrime, and particularly theft of an information, communication, and technology (ICT) device and online fraud. Across these studied, respondents are far more likely to experience property-related forms of cybercrime, compared to violent forms of cybercrime, according to the statistical tests conducted (Nzeakor et al., 2025, p. 68). Furthermore, the study also found that respondents reported experiencing more cyber-enabled crimes, which is normal forms of crimes facilitated through computers and cyber-dependent, which is crimes that can only be completed through computers (Nzeakor et al., 2025, p. 69).

Challenges

The article focuses not only on marginalized groups, but it makes reference issues potentially affecting them southeastern Nigeria. It shows that socioeconomic issues, like limited access to cybersecurity tools, or a lack of formal education, could predispose victims to cybercrime (Nzeakor et al., 2025 61). The evidence shows that most victims were young and educated, meaning even privileged people are exposed more significantly to risks—more significant risks than those not as digitally informed, such as marginalized groups. The article provides evidence for implementation of more tailored information sessions, run more rigorously based on local needs, to prevent these issues (Nzeakor et al., 2025 71).

Societal Contributions

This research contributes importantly to knowledge by filling a gap around cybercrime victimization in Nigeria, providing data-informed information useful for policymakers and law

enforcement. It demonstrates an immediate need for cybersecurity education, a more robust legal framework, and targeted interventions to eliminate property-based cyber involved crimes, as these offenses were the most evident (Nzeakor et al., 2025, p. 70). The use of both surveys and interviews gives a full picture, connecting numbers to real-life stories, and helping create practical, community-based solutions to cybercrime (Nzeakor et al., 2025, pp. 70–71).

Conclusion

In conclusion, the article integrates social science concepts and authentic empirical data to demonstrate the characteristics and consequences of cybercrime in southeastern Nigeria. It shows that property crimes and cyber-enabled crimes were the most common to internet users in Umuahia North LGA. By using criminology theories and close data study, the research builds knowledge of both local and global sides of cybercrime and stresses the urgent need to improve cybersecurity awareness and protection for vulnerable groups (Nzeakor et al., 2025).

Citations

Nzeakor, O. F., Okafor, R. N., & Nwoke, C. N. (2025). Pattern of Cybercrime Abuse of Individual Internet Users in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, 8(2), 60–79. https://vc.bridgew.edu/ijcic/vol8/iss2/5