Article Review #2: Vishing and Smishing in Slum Communities

Keyshawn Braxton

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

April 14, 2026

BLUF (Bottom Line Up Front)

This study demonstrates that cybercrime vulnerabilities stem from resource inequality rather than purely technical weaknesses. By analyzing vishing and smishing attacks targeting Nigerian slum residents, the research exposes how poverty and limited digital resources create more prone to being exploited situations in marginalized populations.

Social Science Principles

The article integrates three core social science frameworks. First, sociology examines how economic disadvantage normalizes cybercrime within impoverished communities, creating environments where digital fraud becomes normal and more accepted. Second, psychology reveals how perpetrators exploit emotional triggers such as fear, urgency, and trustto manipulate victims into giving out sensitive information. Third, criminology applies environmental crime theory, showing how opportunity structures and lack of formal oversight enable systematic victimization (Adeyemo et al., 2026).

Research Questions, Hypotheses, and Variables

The central research question addresses how vishing and smishing perpetrators use social engineering tactics and the vulnerabilities that exist among slum residents. While the data doesn't have a traditional hypothesis, the study tests whether demographic and resource disadvantage and digital illiteracy correlate with increased risk to voice and SMS based cyberattacks.

Independent Variables (IV): Criminal techniques (pre-registered SIM exploitation, bulk messaging platforms), social status, digital literacy levels

Dependent Variable (DV): risk behaviors, victimization frequency, reporting of crimes

Research Methods and Data

The researchers employed a design using snowball and purposive sampling. interviews were conducted with 30 participants of those 30 participants, 20 were victims and 10 were

perpetrators across three Lagos locations Ajegunle, Amukoko, and Ijora-Badia. The data recorded experiences, social dynamics, and operations that traditional surveys would miss.

Connection to Class Concepts

This research directly applies four concepts from this course:

1. Routine Activities Theory: Crime occurs when motivated offenders encounter suitable targets without capable administration. Slum residents lack digital literacy while possessing bank accounts and phones making them attractive targets.

2. Social Engineering: Criminals weaponize interpersonal communication to bypass technical security through psychological manipulation rather than code exploitation.

3**. Victimology:** The study centers victim characteristics poverty, education gaps, institutional distrust that increase exploitation risk.

4. Relativism: Economic desperation reframes cybercrime as survival rather than deviance, showing how context shapes ethical boundaries.

Impact on Marginalized Groups

The research identifies two critical challenges facing marginalized populations. First, digital illiteracy in under-resourced communities leaves residents unable to identify sophisticated social engineering tactics, creating informational ignorance that attackers exploit. Second, institutional distrust prevents crime reporting. Victims fear retaliation or believe authorities won't respond to complaints, allowing cybercriminals to operate with freedom (Adeyemo et al., 2026).

Overall Societal Contributions

This study advances cybersecurity practice through two key contributions. First, it demonstrates that effective fraud prevention requires informed awareness campaigns rather than generic technical solutions. Second, it provides policy recommendations like more strict SIM registration enforcement, real-time banking fraud detection, and community cybercrime task forces that address vulnerabilities affecting populations that are more prone to risks.

Conclusion

Effective cybersecurity extends beyond technical infrastructure to address the conditions that enable exploitation. Digital defenses prove ineffective when attackers leverage poverty and information gaps to take advantage of vulnerable populations through human interaction rather than code.

References

Adeyemo, L. J., Olabulo, T. Y., & Peter, I. G. (2026). Vishing and smishing perpetrators and their victims in Nigerian slums. *International Journal of Cybersecurity Intelligence & Cybercrime, 9*(1), 23–43.