Article Review #2: The Social Science Behind Voice and Text Phishing Using Data from Nigerian Slums

Ava McLaughlin

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

April 16, 2026

Ava McLaughlin

Introduction

This paper will summarize and discuss the article "Vishing and Smishing Perpetrators and Their Victims in Nigerian Slums" by Lateef Junior Adeyemo, Tirimisiyu Yemi Olabulo, and Idenyi Goshen Peter from a social science perspective. The study interviews 30 perpetrators and victims of Voice Phishing (Vishing) and Text/SMS Phishing (Smishing) in three Lagos slums to gather information about techniques used, motives, and effects on victims (Adeyemo et al., 2026). Main discoveries of the study include impersonating valid entities with low-budget materials as a common attacker tactic, attackers often avoid targeting those they know, experienced scammers often teach new ones, attacks are normalized by poverty and peer-influence (sometimes glorified as well), victims rarely report attacks, and many people have a limited understanding of technology, making attacks more likely (Adeyemo et al., 2026).

Relation to Social Science Principles and Concepts

This article is related to three main social science principles in particular: determinism, relativism, and objectivity. Determinism claims that behavior is caused, determined, or influenced by preceding events (CYSE201S (Module 2)); the article reflects determinism by showing that vishing/smishing attackers' behavior is influenced by the people around them, whether they were taught to scam at an impressionable age or enticed by seeing others being praised for their skills. Determinism is also shown through victims of vishing/smishing, as their excessive trust is a result of low technological awareness, rather than their own free will. Relativism, the belief that all things are related and actions should be judged within their full context (CYSE201S (Module 2)), is also shown in the article as the economic and social systems in Nigerian slums are driven by poverty and technological expertise, causing cybercrime behavior to appear normal. Finally, the article relates to the principle of objectivity, which states

that scientists must study topics in a value-free manner (CYSE201S (Module 2)), by interviewing both perpetrators and victims of vishing/smishing instead of favoring one side.

Four course-related concepts that can be seen throughout the article are social engineering, individual motives, cognitive theories, and behavioral theories. Social engineering, "the art of 'Human Hacking' by manipulating people to give up confidential information or bypass security protocols," (CYSE201S (Module 4)), is used to trick victims into giving up financial information via impersonation as a credible company on the phone. Individual motives, like money, curiosity, and recognition, explain vishing/smishing perpetrator behavior in low-income areas in Nigeria (CYSE201S (Module 5)). Cognitive theories "explore how offenders justify their actions and perceive victims" (CYSE201S (Module 5)), explaining behavior in the article, such as justifying vishing/smishing because it is normalized and perceiving victims differently depending on how close they are to them. Lastly, behavioral theories "suggest the behavior is learned" (CYSE201S (Module 5)), which is evident in the article, as researchers found vishing/smishing scams are continuously taught to others and admired in the community.

Research Questions, Methods, and Data Analysis

Although a research question is not explicitly stated, it is inferred that the researchers wanted to understand the techniques and strategies used by attackers, the impacts of vishing/smishing scams on victims, and how social and environmental factors influence both groups. The article does not contain a hypothesis or traditional independent/dependent variables because it is a "qualitative cross-sectional design" focused on understanding behaviors and experiences (Adeyemo et al., 2026). Research methods include snowball sampling (asking participants to recruit people they know) to account for secretive cybercriminals, performing interviews in three Lagos slums, Ajegunle, Amukoko, and Ijora-Badia, because of their "high

prevalence of cyber fraud and socioeconomic vulnerability" (Adeyemo et al., 2026), and sampling twenty victims and ten perpetrators of vishing/smishing to ensure a balanced representation (Adeyemo et al., 2026).

The types of data used in this research article are in-depth interviews and direct quotes from participants (Adeyemo et al., 2026). After analyzing the data, researchers found that attackers often relied on social engineering to gather information about victims and impersonate official entities like network providers, which were highly effective at manipulating emotions and gaining trust. Attackers note that tools are usually easily obtainable and affordable, like pre-registered SIM cards (Adeyemo et al., 2026). Researchers also found that attackers feel guilty when scamming people they know and try to avoid it, suggesting that their behavior is driven by social bonds, not malicious intentions (Adeyemo et al., 2026). Additionally, researchers discovered that many attackers resort to vishing/smishing for economic survival, as it is simple to start, and they feel it is their best option. Because they see it working for others, so many people have turned to vishing/smishing that it feels normal (Adeyemo et al., 2026). Highly skilled vishing/smishing scammers are often seen as role models and take on apprentices, creating generations of cybercriminals. Researchers also found that crimes often go unreported because victims, like the elderly, feel embarrassed or believe the government is corrupt and will do little to help. The researchers conclude their data analysis with interview evidence that a majority of vishing/phishing attacks are a result of a lack of widespread cybersecurity programs (Adeyemo et al., 2026).

Relation to the Concerns of Marginalized Groups and Overall Societal Contributions

This article is strongly related to the concerns of marginalized groups, as it displays how poverty, low technological awareness, and distrust in government lead to a vulnerable society

where cybercrime is normalized to survive. The article claims that “This is not unique to Nigeria; globally, marginalized communities are becoming both the primary targets and unwitting recruits of cyber-fraud networks” (Adeyemo et al., 2026). To combat this rising concern, researchers suggest that cybercrime should be addressed through three root causes: economic desperation, digital illiteracy, and institutional neglect (Adeyemo et al., 2026). In conclusion, the overall societal contributions of the article “Vishing and Smishing Perpetrators and Their Victims in Nigerian Slums” by Lateef Junior Adeyemo, Tirimisiyu Yemi Olabulo, and Idenyi Goshen Peter include explanations of cybercrime and victim behaviors in marginalized areas, common tools, techniques, and social engineering tactics cybercriminals use, and possible future solutions to reduce cybercrime like vishing and smishing.

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. https://doi.org/10.52306/2578-3289.1208

Old Dominion University. (n.d.). CYSE201S (Module 2) *Principles of Social Sciences and Cybersecurity.* https://canvas.odu.edu/courses/201835/files/58917413/download?download_frd=1

Old Dominion University. (n.d.). CYSE201S (Module 4) *Cybersecurity and Human Factors.* https://canvas.odu.edu/courses/201835/files/59116295/download?download_frd=1

Old Dominion University. (n.d.). CYSE201S (Module 5) *Applying Psychological Principles of Cyber Offending, Victimization, and Professionals.* https://canvas.odu.edu/courses/201835/files/59994035/download?download_frd=1