

**Article Review #02: Vishing and Smishing Perpetrators and Their Victims in Nigerian  
Slums**

Student Name: Daija Brown

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwkar Yalpi

Date: 4/14/2026

## **Introduction/BLUF**

Vishing scams are prevalent in Nigerian slums due to experienced scammers training the new generation, and the encouragement of these crimes in impoverished areas. The victims' distrust of the government is a challenge that perpetuates victim precipitation.

### **Relation/Connection to Social Science Principles**

This research paper displays the principle of objectivity. It is independently funded and is not designed to disparage anyone. The second principle demonstrated is ethical neutrality. It outlines how distrust in the Nigerian government has contributed to the victimization of citizens. Instead of targeting a specific group or seeking to control the Nigerian citizens, it seeks to provide education to the victims to prevent future victimization. The third social sciences principle this article displays is determinism. The continuation and growth of vishing in Nigeria was determined to be the result of peer hacking encouraged in impoverished areas, government corruption, and experienced scammers training newer scammers. Thus, continuing the cycle.

### **Research Question /Hypothesis/ Independent Variable/Dependent Variable**

Research Question: What issues contribute to the growing vishing crime problem in Nigeria, and how can it be resolved?

Hypothesis: Education can improve the victimization and decrease cybercrime in Nigeria.

Independent Variable: Vishing Scams and Victim Coping Strategies.

Dependent Variable: Victim precipitation,

### **Types of Research Methods used**

“The research method used was a qualitative cross-sectional design across Lagos slums. This was paired with a snowball sampling technique that involved 20 victims and 10 perpetrators for an in-depth interview” (Adeyemo et al., 2026, 2). The qualitative approach was chosen over

the quantitative approach because the quantitative method focuses on numbers rather than behavior. The snowball sampling technique was utilized due to the limitation of identifying perpetrators with other techniques. “This non-probability technique was necessary because traditional random sampling would fail to identify perpetrators, who operate covertly” (Adeyemo et al., 2026, 8).

### **Types of Data Analysis used**

The multinomial logistic regression model was used to establish a correlation between scam recognition and educational background. It was also used to highlight how impactful scams can be on a global scale. Another model that was used was an API machine learning model. This was primarily used to address a gap in identifying language-based smishing attacks. “The study addresses a critical gap in smishing detection for low-resource languages by developing a machine learning model specifically for Swahili text messages” (Adeyemo et al., 2026, 6).

### **Connections to other Course Concepts**

Victim precipitation is a prominent theme throughout the article. The behaviors and experiences of the victims dictate future behaviors from an internal perspective. External factors, such as trust in leadership in education, identify challenges for preventing revictimization. Another course concept is the idea that unethical hacking is a peer-based activity that is prominent in impoverished locations. This combines the psychodynamic and behavioral psychological theories for cyber offending. Finally, the ineffective law enforcement and corrupt government create a Marxian economic environment for the people of Nigeria. Essentially, the poor are exploited and vulnerable to attacks due to the lack of punishment for the perpetrators.

### **Connections to the Concerns or Contributions of Marginalized Groups**

The focus of this research relates to Nigerian scammers and their victims. It highlights government corruption as a factor that contributes to the victimization of Nigerian and the global population. While the study was limited, it did highlight the importance of education because it reduces the probability of falling victim to a vishing or smishing scam. This not only reinforces how education is important for preventing cyber victimization. It also illustrates how trust in leadership is an important factor for preventing cyber crimes.

#### **Overall societal contributions of the study/Conclusion**

This research sheds light on a growing problem with vishing scams and the multiple factors that contribute to victim precipitation. While the sample size was small, other research has shown the correlation between education, trust in leadership, and cybersecurity compliance.

### Reference

Adeyemo, L., Olabulo, T., & Peter, I. (2026). Vishing and Smishing Perpetrators and Their Victims in Nigerian Slums. *International Journal of Cybersecurity Intelligence and Cybercrime*, 9(1), 1. Center for Cybercrime & Investigation.

<https://vc.bridgew.edu/ijcic/vol9/iss1/3/>

**Article Link:** <https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1208&context=ijcic>