



KWASU INTERNATIONAL JOURNAL OF ARTS AND SCIENCE EDUCATION

ISSN:0795-820X (ONLINE)

Journal homepage

ENHANCING CYBERSECURITY AWARENESS AND EDUCATION TO MITIGATE CYBER FRAUD AMONG NIGERIAN UNDERGRADUATES

¹Muhinat B. BELLO, ²ODUN-AYO, Daniel Tolulope, ³Rihanat A. AHMED,

⁴A.D. GBIGBADUA, ⁵Olufunke O. KAYODE

^{1&2}Department of Social Sciences Education, Faculty of Education, University of Ilorin, Nigeria

³Department of Sciences Education, Faculty of Education, University of Ilorin, Nigeria

Department of Arts and Science Education, Faculty of Education, Kwara State University, Malate

¹bello.mb@unilorin.edu.ng

⁴abdulraheem.gbgbadua@kwasu.edu.ng

⁵olufunke.kayode@kwasu.edu.ng,

ARTICLE INFO

Article History

Accepted on July, 2025

Keywords: Cyberfraud; Undergraduates; Intervention; Cybercrime and Rehabilitation

ABSTRACT

This study investigates the rising incidence of cyber fraud among students in tertiary institutions in Kwara State, Nigeria, particularly in the context of increased digital engagement during the COVID-19 pandemic. Utilising a qualitative survey design, data were collected from 72 lecturers across various public institutions. The findings reveal three primary intervention strategies: the integration of cybersecurity education into the curriculum, the implementation of comprehensive cybersecurity awareness campaigns, and the establishment of legal enforcement and rehabilitation programs. Participants emphasised the necessity of embedding digital ethics and literacy within educational frameworks to equip students with the knowledge to navigate online risks responsibly. Additionally, the study highlights the importance of strong institutional policies and cryptographic techniques to enhance digital security. By adopting a multifaceted approach that combines education, awareness, and policy enforcement, this research aims to foster a secure digital environment, ultimately reducing students' involvement in cyber fraud.

Introduction

The growing menace of cyber fraud has become a major global concern, as incidents of financial losses, intellectual property theft, and personal identity fraud have become widespread among individuals, corporate organisations, and governments. This surge in cybercrime is closely

tied to the rapid digital transformation of businesses and the increasing dependence on online platforms. In recent years, particularly during the COVID-19 pandemic, there has been an unprecedented shift toward technology-driven solutions, such as telecommuting and remote learning, to keep people and businesses connected. The pandemic also accelerated the digitisation of products and services, the rise of e-commerce, and the adoption of online business continuity strategies. Consequently, more people are now online than ever before, with the World Economic Forum reporting a 50% increase in internet traffic since April 2020, when the pandemic first took hold.

This widespread digital migration has underscored the need for individuals to acquire more IT knowledge and skills for survival. For students, in particular, technology is now a fundamental part of education. To thrive as 21st-century learners, they must possess technological literacy. However, this increased exposure to the digital world has not only empowered learners to solve academic problems but has also led some to misuse their skills. Many youths, especially students, have begun leveraging their technological abilities to engage in cyber fraud.

Cyber fraud refers to crimes committed online through platforms such as email and social media, including identity theft, phishing, and hacking schemes designed to steal money (Adebayo & Ogunlade, 2019). Among Nigerian youth, cyber fraud has become a prevalent and illegal means of making money. It involves deceiving people on the internet for personal gain, whether financial, social, or otherwise. Despite the opportunities provided by technology, many undergraduates in Nigeria have turned to cyber fraud, reflecting a complex combination of socio-economic pressures, technological advancements, and a lack of awareness about the legal and ethical ramifications of such activities.

Several factors contribute to the involvement of Nigerian undergraduates in cyber fraud. Many students face financial difficulties due to the high cost of education and living expenses, driving them to seek illicit sources of income (Adewale, 2018). Additionally, widespread access to the internet and the growing reliance on digital platforms for communication and financial transactions provide fertile ground for cybercrime. Tech-savvy students, in particular, may exploit these opportunities for personal gain (Oluwaseyi et al., 2020). Unfortunately, a significant number of undergraduates lack proper education on cybersecurity, leaving them vulnerable to manipulation by experienced cybercriminals. The absence of awareness programmes within educational institutions exacerbates this problem (Adebayo & Ogunlade, 2019).

Peer pressure and association with criminal networks, both within and outside academic environments, further lure undergraduates into cyber fraud (Olumide et al., 2021). However, engaging in such illegal activities comes with serious consequences. Students involved in cyber fraud risk severe legal penalties, including imprisonment and hefty fines, as outlined in the Nigerian Cybercrime (Prohibition, Prevention, etc.) Act of 2015 (National Assembly, 2015). Additionally, participation in cyber fraud can tarnish students' academic reputations and jeopardize their future career prospects. Employers increasingly scrutinize candidates' online activities, and a criminal record can have long-lasting effects on an individual's professional life. Moreover, instances of cyber fraud among students can damage the reputation of educational institutions, leading to a loss of trust from stakeholders and potential consequences for institutional accreditation.

Ola Olukoyede, Chairman of the Economic and Financial Crimes Commission (EFCC), has described cybercrime as a "menace and cankerworm" in Nigerian society. He noted that cybercrime is so widespread that "seven out of 10 Nigerian students" are involved in it (2024). If the current trend continues, more than 70% of Nigerian youths could soon become ex-convicts, further exacerbating the issue. In light of this alarming situation, this study investigates strategies to reduce the prevalence of cyber fraud among undergraduates in Kwara State.

Theoretical Explanation

The Differential Opportunity Theory, developed by Cloward and Ohlin (1960), builds on the ideas of anomie, popularized by Emile Durkheim, and strain, as articulated by Robert Merton. Cloward and Ohlin introduced the concept of "opportunity structures" to examine criminal behaviour. They argued that while individuals across all social strata share the same goal of success, the opportunities to achieve these goals are not equally available, especially for those in lower socio-economic classes. When individuals face socio-economic strain, they may resort to criminal behaviour if opportunities for such behaviour exist. According to this theory, the availability of opportunities not only influences one's likelihood of committing a crime but also determines the type and level of crime they might engage in. For example, in communities with limited access to education or technological resources, individuals who feel blocked from achieving their goals may be less likely to commit crimes due to the absence of opportunities.

In essence, the theory suggests that not all opportunities lead to crime, and not all crimes require opportunities. However, opportunities play a significant role in enabling criminal

behaviour. Applying this theory to the current realities of youth involvement in cybercrime in Nigerian society, it can be argued that the rise in cybercrimes among students and undergraduates is linked to increased access to education and technological resources. The internet provides an anonymous platform that many young people exploit to commit cybercrimes. Differential opportunities in internet crime are evident in the varying levels of involvement among youths in different types of cyber fraud. For instance, some youths engage in more sophisticated forms of cybercrime due to their higher level of education and ICT expertise.

Despite its influence, the Differential Opportunity Theory has faced criticism. Critics argue that it overlooks how changes in lifestyle and work routines affect the opportunity structure for crime, suggesting that opportunity itself may be influenced by other factors rather than being the sole determinant of criminal behaviour.

Purpose of the Study

This study examined lecturers' suggested intervention approach to reducing student involvement in cyber-fraud among tertiary institution students in Kwara State, Nigeria.

Research Questions

One research question was supposed to guide the study.

- a. What are the lecturers' suggested intervention approaches to curbing cyber-fraud among tertiary institution students in Kwara state?

Methodology

The study employed a qualitative survey design, utilising open-ended questions to gather data. In qualitative research, purposive or purposeful sampling is often chosen when the goal is to gain a deep understanding of a particular phenomenon. This approach emphasises depth over breadth, focusing on obtaining nuanced insights rather than broad generalisations. The design is well-suited to exploring complex issues in a detailed manner, making it appropriate for this study.

The population for the research included lecturers from seven universities, seven polytechnics, and six colleges of education in Kwara State. The decision to focus on public institutions aligns with Samob's (2010) assertion that researchers can select a sample if it aligns with the specific characteristics of interest. In this case, the target population comprised all 24 tertiary institutions in Kwara State. These institutions were purposively selected for the study, reflecting a total population of 13,821 lecturers (as reported by the Human Resources Department in 2023 from all the sampled institutions). From this total, three lecturers from each institution

were selected, resulting in a sample size of 72 lecturers. The study involved a total of 72 participants, consistent with Creswell and Creswell's (2014) emphasis on the importance of purposeful sampling in qualitative research. Purposeful sampling is particularly valuable when the goal is to gain a deep understanding of a specific phenomenon, as was the case in this study.

A qualitative method was employed, utilising an open-ended interview approach developed by the researchers. Thematic data analysis was used to process the data collected from the 60 participants. Following the guidelines outlined by Creswell (2014), the researcher adhered to the stages of data analysis. To enhance the efficiency of this process, NVIVO 10, a qualitative data analysis software, was utilised. As Creswell (2014) notes, NVIVO assists in the storage, sorting, coding, and analysis of data, as well as in generating representations of the findings. To ensure confidentiality, pseudonyms were used to report the participants' suggestions, following the advice of McCann and Clark (2003). Creswell (2009) further stresses the importance of protecting the anonymity of individuals, roles, and incidents in research. This was achieved by using pseudonyms for both the participants and the locations where data were collected.

Results

The interview data were analysed using a thematic approach, which allowed the findings to be organised into themes, sub-themes, and even sub-sub-themes, as well as represented through graphical models. This method provided a structured way to capture and present the perspectives and actual words of the 72 informants, facilitated by the use of NVivo 12 qualitative analysis software.

Lecturers' Suggested Interventions to Reduce Undergraduates' Involvement in Cyber-Fraud

The study explored the intervention strategies proposed by lecturers to curb students' involvement in cyber-fraud. Three main themes emerged from their suggestions:

1. **Educational Programmes**
2. **Cybersecurity Awareness**
3. **Rehabilitation, Enforcement, and Punishment Approaches**

These themes and their corresponding sub-themes are systematically presented and discussed in the following sections.

Fig. 1: Summary of mapping three intervening approaches to reducing undergraduates' involvement in cyber-fraud.

The study explored intervention strategies proposed by lecturers to curb students' involvement in cyber-fraud, revealing three key approaches: Educational programmes would integrate digital ethics and literacy into the curriculum, equipping students with knowledge to avoid fraudulent activities. Cybersecurity awareness campaigns and workshops would inform students about the risks and consequences of cyber-fraud, fostering responsible online behaviour. Lastly, a blend of legal enforcement and rehabilitation programs was suggested to deter offenders while offering corrective measures for reintegration. These approaches aim to holistically address and reduce cyber-fraud among students.

Educational programmes

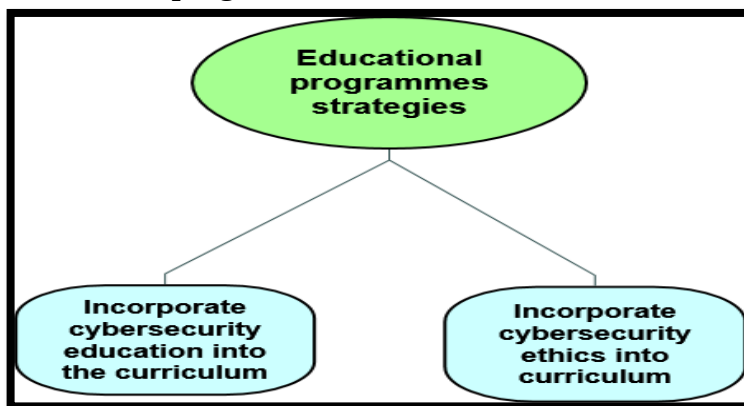


Fig.2:Thematic Mapping of educational programs strategies

All participants emphasised that education is key to development and solving societal problems, including cyber-fraud. Addressing such issues superficially offers only temporary relief, whereas tackling the root causes through education provides a lasting solution. Therefore, the participants unanimously proposed that quality education can significantly reduce cyber-fraud among Nigerian students.

The uniqueness of this study lies in its proposal to integrate cybersecurity education specifically within the General Studies (GNS/GSE) curriculum of tertiary institutions. This

approach not only emphasises the broad and interdisciplinary nature of General Studies but also introduces cybersecurity education as a foundational element for all students, regardless of their major. Unlike previous research, which may have focused on isolated training or awareness programmes, this study advocates for a comprehensive, curriculum-based strategy that empowers students by embedding cybersecurity knowledge and ethical considerations directly

into their academic journey.

By incorporating cybersecurity education into the GNS/GSE framework, students will gain exposure to the causes, consequences, and risks associated with cyber-fraud, helping them to develop critical thinking, analytical, and ethical decision-making skills. This method stands out as a proactive, long-term solution for curbing cyber-fraud, addressing the issue at its root by educating students before they potentially engage in such activities. Furthermore, the integration of mandatory cybersecurity courses and regular workshops not only enhances student awareness but also extends the reach of cybercrime prevention to the larger community, fostering a culture of digital responsibility and safety. This innovative approach aligns with the findings of Levi, Doig, Gundur, Wall, and Williams (2017), who emphasise the importance of security education as a tool for reducing cybercrime. However, the study distinguishes itself by presenting a structured, institutionalised framework for delivering cybersecurity education across disciplines, which could lead to a more sustained and widespread impact on reducing cyber-fraud among students. Participants in this study unanimously supported the infusion of cybersecurity education into the curriculum, recognising it as a vital strategy to raise awareness, prevent cyber-fraud, and promote ethical behaviour among students, thereby contributing to a more secure digital environment.

Cybersecurity Awareness Approach

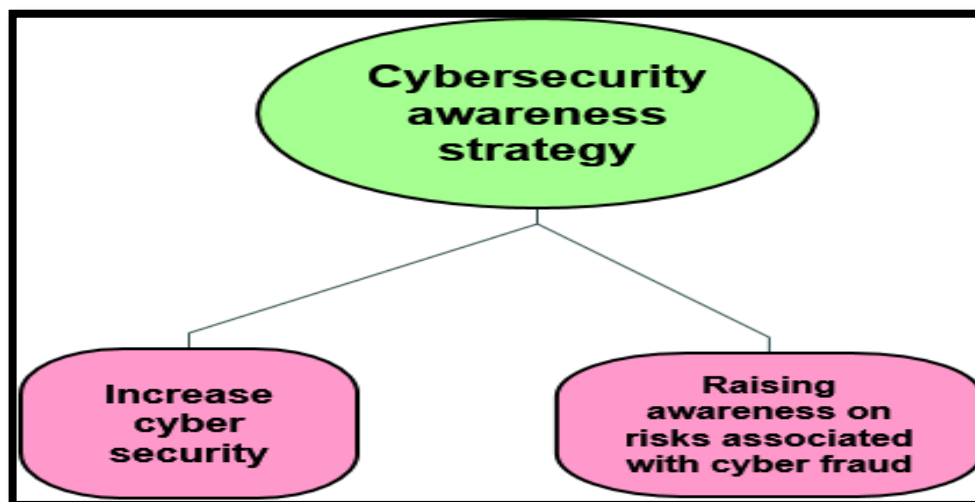


Fig.3. Thematic Mapping of Cybersecurity Awareness Strategy

Cybersecurity awareness encompasses the collective knowledge, attitudes, and behaviours adopted by individuals and organizations to safeguard against cyber threats. It goes

beyond technical know-how to include a broader understanding of risks, best practices, and the ability to make informed decisions regarding digital security (Dunn, 2018). In this context, digital literacy programs, particularly those focused on cybersecurity, play a pivotal role in equipping students with the skills necessary to navigate the online world responsibly. By fostering critical thinking, students can evaluate online information, recognize risks, and make well-informed decisions, which aligns with Jones and Brown's (2021) emphasis on the importance of digital literacy in preventing cybercrime.

In this study a detailed exploration of cybersecurity awareness as a comprehensive strategy for preventing cyber-fraud among Nigerian undergraduates. While existing literature highlights the importance of cybersecurity, this study uniquely combines personal cyber hygiene practices, institutional policies, and cryptographic techniques to present a holistic approach to curbing cyber-fraud. Participants identified the need for educational institutions and businesses to enforce strong password policies and increase the security of digital platforms. This approach acknowledges that limiting access to passwords and improving security measures can discourage hackers from compromising systems.

Moreover, cryptography, suggested by 53 participants, emerged as a key component in raising awareness about the risks associated with cyber-fraud. Cryptographic techniques, particularly encryption, offer robust protection by transforming sensitive data into unreadable code, making it difficult for hackers to exploit vulnerabilities. This proactive defense mechanism, if implemented in educational, financial, and business institutions, can significantly reduce unauthorised access and cyber-fraud activities such as identity theft. This study also highlights the importance of cybersecurity awareness campaigns, which should focus on both the negative consequences of cyber-fraud and the positive opportunities available online. Participants emphasised that proper education and awareness campaigns are crucial to informing individuals about the risks and consequences of cybercrime. By combining these varied intervention strategies, strong password policies, cryptographic methods, and comprehensive awareness campaigns, this study presents an innovative approach to fostering a more secure digital environment for students and institutions alike.

Rehabilitation, Enforcement and Punishment

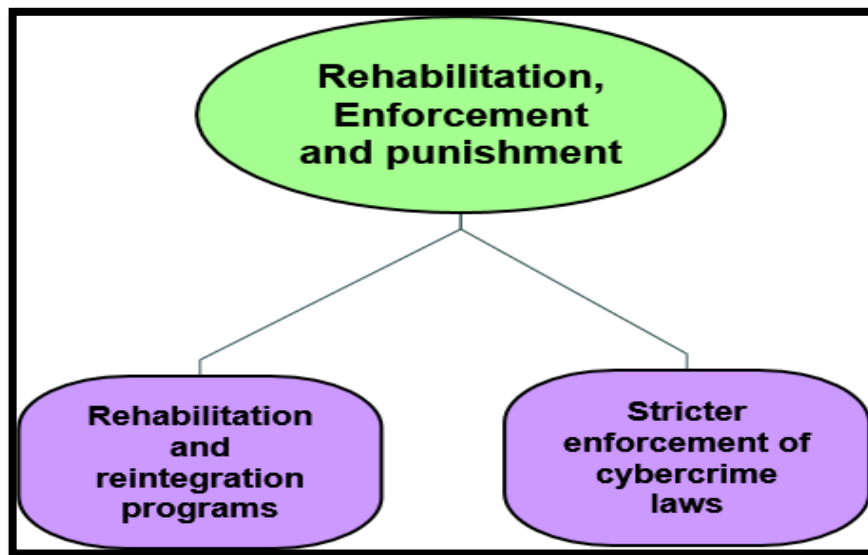


Fig.4: Thematic Mapping of the need for Rehabilitation, Enforcement and Punishment

All respondents agreed that rehabilitation, enforcement, and punishment are essential strategies for combating undergraduate involvement in cyber-fraud. Each element plays a critical role in addressing the root causes, deterring potential offenders, and fostering a culture of cybersecurity awareness.

Rehabilitation, according to the participants, involves understanding the motivations behind students' engagement in cybercrime, such as financial pressures, lack of ethical education, or thrill-seeking behaviour. By addressing these underlying factors, authorities and educators can design tailored interventions. Educational programs focusing on cybersecurity awareness, ethical hacking courses, and mentorship initiatives were suggested as effective ways to reshape students' perspectives, redirecting their technical skills into positive, lawful avenues. Additionally, mental health support was emphasised, as some students may turn to cybercrime due to personal struggles. Access to counselling services would provide emotional and psychological support, steering students toward more constructive choices.

Regarding enforcement, participants highlighted the importance of strengthening both societal and institutional legal frameworks. They emphasised that cybercrime laws must be comprehensive, clearly defined, and rigorously enforced to prevent cybercrime. Establishing specialised cybersecurity task forces that can investigate and prosecute cyber offences was recommended by 98% of the participants. These units could collaborate with educational institutions to identify and address threats originating from within student communities.

Punishment, as proposed by participants, serves as a deterrent to potential offenders. Communicated consequences, such as fines, probation, or imprisonment for severe offences, would discourage students from participating in cyber-fraud. Publicising legal actions taken against cybercriminals could further deter future offences. Additionally, academic sanctions, including penalties or suspension, would reinforce the importance of ethical behaviour within the academic environment. The findings are uniquely demonstrated in the comprehensive integration of rehabilitation, enforcement, and punishment as a unified strategy to address cyber-fraud. Unlike prior studies that focused on individual aspects, this research presents a holistic approach, emphasising that combining these elements—educational programmes, mental health support, robust enforcement, and proportionate punishment—can create a sustained impact. By fostering ethical behaviour, legal compliance, and cybersecurity awareness, educational institutions can not only address the immediate issue of cyber-fraud but also work toward preventing future instances. This strategy supports the development of a secure, responsible, and informed student community.

Conclusion

The study underscores the urgent need for a proactive stance against cyber fraud in educational institutions. By integrating cybersecurity education into the curriculum and promoting awareness, institutions can empower students to make informed decisions online. Furthermore, the combination of legal enforcement and rehabilitation strategies is essential to deter potential offenders and foster a culture of accountability. Based on this, it was recommended that:

- a. Educational institutions should incorporate cybersecurity education into their General Studies curriculum to ensure all students receive foundational knowledge on digital safety and ethics.
- b. There is a need for the school management to organise regular workshops and campaigns to raise awareness about the risks of cyber fraud and the importance of personal cyber hygiene practices.
- c. School management must develop and enforce robust cybersecurity policies, including strong password protocols and access controls, to protect sensitive information.
- d. Tertiary institutions should collaborate with law enforcement agencies to establish clear legal frameworks and rehabilitation programmes for offenders, promoting a culture of cybersecurity awareness and responsibility.
- e. Ongoing research should be conducted to assess the effectiveness of implemented strategies and adapt to the evolving landscape of cyber threats.

References

- Adewale, A. S. (2018). Financial Crime: A Study of Cybercrime in Nigeria. *Journal of Criminology and Criminal Justice*, 5(1), 18-31.
- Adebayo, J., & Ogunlade, A. (2019). Cybercrime and its Impacts on Tertiary Institutions: The Nigerian Experience. *International Journal of Advanced Research in Computer Science*, 10(3), 180-187.
- Cloward, R. A., & Ohlin, L. E. (1960). *Delinquency and Opportunity: A Theory of Delinquent Gangs*. Free Press.
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage Publications.
- Dunn, J. (2018). Cybersecurity Awareness: Bridging the Gap between Knowledge and Behaviour. *International Journal of Human-Computer Interaction*, 34(10), 960-972.
- Jones, A., & Brown, C. (2021). Digital Literacy and Cybersecurity: A Cross-Disciplinary Approach. *International Journal of Cybersecurity Education, Research and Practice*, 2(1), 13-24.
- Levi, M., Doig, A., Gundur, R., Wall, D. & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law and Social Change: an interdisciplinary journal*, 67 (1). 77-96.
- McCann, L. I., & Clark, M. C. (2003). Data Reduction Strategies in Phenomenological Research. In *Phenomenology, Uncertainty, and Care in the Therapeutic Encounter* (pp. 63-79) Springer.
- National Assembly. (2015). Cybercrime (Prohibition, Prevention, etc.) Act. Nigeria.
- Oluwaseyi, O. O., et al. (2020). Cybercrime and the Nigerian Youth: A Study of Causes, Effects, and Solutions. *Journal of Contemporary Issues in Business and Government*, 26(2), 345- 358.
- Olumide, O. O., et al. (2021). Social Media and Cybercrime in Nigeria: A Case Study of Undergraduates in Kwara State. *Journal of Cybersecurity Education, Research and Practice*, 2(2), 109-123.
- Ola Olukoyede. (n.d.). Cybercrime: EFCC Boss, Ola Olukoyede, Raises Alarm. Retrieved from [URL]
- Samob, A. O. (2010). *Purposive Sampling as a Tool for Informant Selection*. *Ethnobotany Research and Applications*, 8, 65-75.
- World Economic Forum. (2020). Internet Usage Statistics 2020. Retrieved from: <https://www.weforum.org/agenda/2020/08/internet-users-usage-countries-change-demographics/>