



Audrezara Journal of Communication and Social Research (AJCSR), Vol. 2(1), 49-58, 2026.



AUDREZARA JOURNAL OF COMMUNICATION AND SOCIAL RESEARCH (AJCSR)

Vol. 2, Issue 1, pp. 49-58, April, 2026.

DOI: <https://doi.org/10.5281/zenodo.19916497>

E-ISSN: 3121-9721

A Quasi-Experiment of the Efficacy of Cyber-Security Education as a Strategic Intervention for Enhancing Financial Cybercrime Awareness, Detection Skills, and Reducing Vulnerability in Nigeria

¹Shadrach Idi* & ²Emeka Williams Etumnu

¹Department of Mass Communication, Taraba State University, Jalingo

²Department of Mass Communication, Imo State University, Owerri



ORCID:

¹ <https://orcid.org/0000-0001-7996-8281>

² <https://orcid.org/0000-0002-7186-117X>

***Corresponding Author:** shadrachidi@gmail.com

History: Received: November 26, 2025; Revised: January 27, 2026; Accepted: February 18, 2026.

Abstract

This research investigated cyber security education as an intervention strategy in enhancing awareness of financial cybercrimes, detection skills, and motivation toward adoption of precautionary measures in order to reduce vulnerability among Internet users in Nigeria. The study was anchored on the inoculation theory, which assumes that exposing the audience to a given risk experience or information will help create some immunity, awareness, and protection against future risks. The study used a quasi-experimental research design with 500 participants divided equally into the treatment group and control group. The treatment group was given cyber-security education training for eight weeks, while the control group was not. Both groups took a test before and after the treatment. The results were later compared, and it was revealed that participants (treatment group) that received cyber security education training demonstrated a higher awareness of financial cybercrimes, a better ability to detect the crimes, and motivation to adopt precautionary measures to reduce vulnerability compared to those participants (control group) that were not exposed to the training. The theoretical and practical implications for the findings were later presented.

Keywords: Cyber security education, Financial Crime, intervention strategy, detection skills

Introduction

The rise of digital technologies has significantly influenced all aspects of human activities, especially as it relates to financial transactions. Today, there has been a high rate of migration to online commerce and



banking (Omarini, 2022; Ezennia & Marimuthu, 2020). This development has brought about numerous benefits, especially in the area of convenience, where individuals from the comfort of their homes can make purchases to be delivered to their homes as well as carry out banking transactions without entering the banking halls. This development was motivated by pervasive penetration of the Internet and digital devices like smartphones and iPhones, among others. However, as they use the Internet, they become vulnerable to cybercriminals. These criminals breach users' data privacy and protection to access sensitive information and use the same to harm the user, especially as it relates to financial scams (Shillair et al., 2022; Sasi et al., 2023; Chika & Tochukwu, 2020; Ekwenchi & Shadrach, 2023; Alkhalil et al., 2021; Goldstein et al., 2018).

In Nigeria, Internet financial fraud, often known as "yahoo," is a growing phenomenon. Despite the existence of a cybercrime law, scholars (accounts (Eboibi & Ogorugba, 2023; Ojolo & Singh, 2023; Makeri, 2017) have consistently argued that there is a growing number of young people engaging in exploiting technological loopholes and poor digital media literacy users to defraud the users' money. A report by Statista (2024) revealed that Internet penetration in Nigeria is 45% of the total population of more than two hundred million, implying that there is high access and utilisation of digital media among Nigerians; however, the rapid growth does not correlate with adequate digital media literacy, especially in cyber security. Prior studies (Garba et al. 2020; Mejabi et al. 2018) have established that many Nigerians lack the knowledge to identify phishing mails and other cyber risks, and many lack the skills to safeguard their digital footprints in order to avoid falling victim to cybercrimes, especially financial crimes. A number of studies and media reports revealed how several individuals and even organisations lose huge sums of money due to their vulnerabilities resulting from their ignorance of cyber protection measures (Ikuerio & Zeng, 2022; George, 2023). In 2019 alone, Nigeria has lost on average N127 billion (\$328,842,878 million) to cybercrimes (Ohwovoriole 2019). The country is often seen as the global headquarters of cybercrimes due to its consistent and high-profile reports of cybercrimes.

To curtail the growing menace of financial cybercrimes in Nigeria, the government has introduced several frameworks and policies, such as the Cybercrime Act, the National Cybersecurity Policy and Strategy, and the National Data Protection Regulation, among others. Despite these initiatives, online financial crimes remain unabated, as many Internet users fall victim to scammers on a daily basis. This is doubtful because the first line of defence against cybercrime is the individual Internet user's knowledge of cyber risks and protection strategies. A lack of this awareness and knowledge contributes to increased cybercrimes (Kikerpill, 2020). Thus, cybereducation remains the foundation for mitigating cyber risks in Nigeria. Cyber education has the capacity to provide the cyber user with the needed knowledge and skills to detect financial cybercrimes in any form and strategies for data and privacy protection measures, as well as equip individuals with the knowledge to conduct safe online transactions, including online purchases and banking, without fear (Tew, 2019). Cyber education can take the form of school curricula, media awareness programs, and accessible multimedia tools, such as video tutorials and interactive simulations, among others. Applying cyber education as part of the general strategy for public campaigns against cybercrimes, including financial crime, is crucial in Nigeria. By fostering a culture of cybersecurity education, individuals and organisations can better understand how to stay safe online, despite the sophisticated and evolving strategies employed by cybercriminals throughout the country.

Despite the importance of cyber education in preventing cybercrimes in Nigeria, several scholars (e.g., Igwe & Ibegwam, 2014; Njoku et al., 2019) have found that many Nigerians have not been exposed to any such trainings, and for the few that have been exposed to the related trainings, there is a paucity of experimental research establishing the effectiveness of cyber education as an intervention strategy to combat online financial crimes in the country. The majority of the existing studies (Garba et al., 2021; Amankwa 2021; Tew, 2019; Aliyu et al., 2023) adopted designs like quantitative surveys, conceptual



approaches, literature review approaches, and stand-alone qualitative designs in the form of interviews. Though these approaches provide useful insights to our understanding of the importance of cyber education in Nigeria, they lack the capacity to establish a cause-and-effect relationship between exposure to cyber education and a reduction in vulnerability to financial cybercrimes among Nigerians. This gap underscored the need for the current study, which adopts a quasi-experimental design to determine the relationship between the provision of cyber education and a reduction in financial cybercrime vulnerability among young Internet users in Nigeria.

Theoretical framework and hypotheses formulation

The inoculation theory serves as the foundation for this study. Inoculation theory was propounded by McGuire (1961). Inoculation theory also suggests that by methodically exposing the audience to some risky information or experiences against contrasting phenomena or threats, the audience will develop a stronger immunity against the threat (Compton, et al., 2016). The theory is based on two elements, namely threats and refutational preemption. A threat refers to the awareness of potential contrasting communication that might challenge one's beliefs or attitudes and expose one to certain dangers, while refutational preemption involves presenting counterarguments or messages against anticipated threats (Matusitz & Breen, 2005). In a nutshell, the theory posits that just as vaccines expose individuals to weakened viruses to build immunity, exposure to certain information about a given risk can help build resistance to falling victim to the risks. In relation to the phenomenon of cyber financial threats and cyber education, the assumption is that by providing Internet users access to knowledge about common cyber financial threats through cyber education in the form of simulation experiences such as exposure to simulated phishing mail and other learning approaches, the user might learn how to detect obvious scams as well as develop resistance tactics employed by scammers online. This means that providing continuous cyber education will bolster and continually update users' ability to curtail impeding financial threats common in the digital landscape. Based on the empirical evidence and the theoretical framework above, we proposed the following hypotheses:

H1 Individuals who received cyber security education will show a higher level of awareness about financial cybercrimes than individuals who do not receive cyber security education.

H2 Individuals who receive cybersecurity education will have better skills to detect financial crimes than those who do not receive cyber security education.

H3 Individuals who received cyber security education are more likely to protect themselves against financial cybercrimes than individuals who do not receive cyber security education.

Method

Research design

The study adopts an experiment design. The population of the study is undergraduate students of a public university in Nigeria. Prior studies (e.g., Lim & Tan, 2020; Shadrach & Ekwenchi, 2023) have established that this group are major consumers of the Internet and new media devices and, thus, are more vulnerable to cybercrimes, especially financial scams.



Sampling procedure

The study used a sample of 500 participants. Participation was willing, and participants were permitted to withdraw from the study at any point if they wished. The sample size was determined using G*Power software at a power ($1-\beta$) of 0.90, an effect size of 0.30, and an alpha level (α) of 0.05. The participants were divided into two groups known as the treatment group ($n = 250$) and the control group ($n = 250$). A stratified random sampling technique was adopted to select the participants from a single department of the university. The stratification was based on level or year (level 100 to level 400) in the university, age bracket (18–35 years), and gender (male or female). Adopting a homogenous sample facilitates comparison and helps establish a cause-and-effect relationship in experimental research, according to scholars (Babbie, 2015).

Treatment procedure

In order to conduct the study, three specialists and lecturers of cyber security were hired to deliver cyber-security education to the participants in the treatment for eight weeks. The experts prepared the teaching materials. In the first week, the participants were taught the basics of cyber security awareness, with a focus on concepts of online safety and the common types of cyber threats. The second week focused on cyber safety practices, with an emphasis on strong passwords, safe browsing, and the importance of deleting cookies and search histories, and two-factor authentication, among others. In week three, the participants were taught ways to identify common cyber threats, such as malware, phishing, and identity theft, and the warning signs to watch for in each case. In week four, participants were taught how to spot fraudulent emails and websites. In week five, participants were taught the concepts of social engineering tactics, they were exposed to knowledge about the various tactics used by cybercriminals to manipulate individuals into sharing personal information. Furthermore, week six was dedicated to financial cybercrime, where the participants were taught safety online banking safety practices and how to recognise scams that target financial transactions. In the seventh week of the study, the participants were trained how to respond to potential threats or scammers, and in week eight, they were taught how to report to authorities where their data was breached. All of the lessons include hands-on, simulation, group, and individual exercises.

Variables measurement and instrument

Before and after the treatment, the researchers administered a similar test (a questionnaire) to the participants in both groups. The test measured awareness of financial cybercrimes, detection skills, and motivation to adopt protection measures. For each variable, 10 items were developed. The items were framed on a 5-point Likert scale ranging from strongly disagree (1) to strongly agree (5). The questionnaire was validated by three experts in cyber-security education. To assess the reliability of the questionnaire. A pilot study involving 50 university students who did not take part in the study was conducted. The reliability test results indicated that the measures for cyber financial crime awareness ($\alpha = .89$), skills for detection ($\alpha = .79$), and motivation to adopt precautionary measures to reduce vulnerability ($\alpha = .81$) all exceeded the acceptable threshold of .75, demonstrating that the measurement instrument was reliable. Furthermore, descriptive and inferential statistics, particularly means, standard deviations, and an independent t-test at a .05 level of significance, were used for data analysis.

Results

Data from the questionnaire copies for the two tests for both treatment and control groups are presented below.



Table 1. Showing the mean and t-test results on awareness of cyber financial scams scored by each group in the first and second tests.

Group	1 st Test (Pretreatment)			Sig	2 nd Test (Post-treatment)			Sig
	M1	SD1	Df		M2	SD1	Df	
Control	1.9	0.43			1.8	0.13		
Treatment	1.8	0.33	19	0.73	4.1	0.33	13	0.01

n = 250 for each group.

The table shows the mean scores (M) and standard deviations (SD) for both control and treatment groups on their awareness of cyber financial scams before (1st test) and after (2nd test) an intervention. In the pretreatment test, the control group (M = 1.9, SD = 0.43) and the treatment group (M = 1.8, SD = 0.33) had similar levels of awareness, with no significant difference between the groups ($p = 0.73$). However, in the post-treatment test, the treatment group exhibited a significant increase in awareness (M = 4.1, SD = 0.33, $p = 0.01$), while the control group's awareness remained almost unchanged (M = 1.8, SD = 0.13). This suggests that the intervention significantly improved the treatment group's awareness of cyber financial scams. This goes further to validate the first hypothesis (H1), which states that “individuals who received cyber security education will show a higher level of awareness about financial cybercrimes than individuals who do not receive cyber security education.”

Table 2. Showing mean and t-test results on detecting cyber financial scams scored by each group in the first and second tests.

Group	1 st Test (Pretreatment)			Sig	2 nd Test (Post-treatment)			Sig
	M1	SD1	Df		M2	SD1	Df	
Control	1.2	1.2			1.5	0.72		
Treatment	1.1	1.2	22	0.87	4.8	0.13	19	0.01

n = 250 for each group.

The table presents the mean scores (M) and standard deviations (SD) of two groups—control and treatment—on their ability to detect cyber financial scams before (1st test) and after (2nd test) an intervention. In the pretreatment test, both the control group (M = 1.2, SD = 1.2) and the treatment group (M = 1.1, SD = 1.2) had similar low mean scores, indicating no significant difference between the groups ($p = 0.87$). However, after the intervention (post-treatment), the treatment group showed a significant improvement in detection ability (M = 4.8, SD = 0.13, $p = 0.01$), whereas the control group's performance remained relatively low (M = 1.5, SD = 0.72), suggesting that the treatment had a significant positive effect. This further validated the second hypothesis (H2), which states that “individuals who received cyber security education will have better skills to detect financial crime actions than individuals who did not receive cyber security education.”

Table 3. Showing mean and t-test results on the likelihood of adopting precautions against cyber financial scams scored by each group in the first and second tests.

Group	1 st Test (Pretreatment)			Sig	2 nd Test (Post-treatment)			Sig
	M1	SD1	Df		M2	SD1	Df	
Control	1.3	1.3			1.3	0.62		
Treatment	1.2	1.3	19	0.65	4.9	0.18	19	0.01



n = 250 for each group.

The table presents the mean scores (M) and standard deviations (SD) for both the control and treatment groups regarding the likelihood of adopting precautions against cyber financial scams, measured before (1st test) and after (2nd test) an intervention. In the pretreatment test, both the control group (M = 1.3, SD = 1.3) and the treatment group (M = 1.2, SD = 1.3) showed similar likelihoods of adopting precautionary measures, with no significant difference ($p = 0.65$). After the intervention, the treatment group demonstrated a significant increase in the likelihood of adopting precautions (M = 4.9, SD = 0.18, $p = 0.01$), while the control group's scores remained unchanged (M = 1.3, SD = 0.62). This indicates that the intervention significantly improved the treatment group's likelihood of adopting precautionary measures; hence, the third hypothesis (H3), which says, "Individuals who received cyber security education are more likely to protect themselves against financial cybercrimes than individuals who do not receive cyber security education, was also accepted.

Discussion

The first goal of this study was to measure if cyber-security education creates awareness about cybercrimes, particularly financial risks such as scams, among users. Based on the outcome, it has been established that cyber-security education significantly impacts awareness of cyber financial crimes. This was based on the fact that participants who received cyber-security training as part of the experiment demonstrated higher consciousness of the risks than those who were not exposed to the training. This finding therefore supported the first hypothesis (H1). Therefore, it can be said that exposing internet users to cyber-security educational training will enhance their alertness against cybercrimes, especially online financial scams. This finding supports prior researchers (Tarrand et al., 2022; Crick et al., 2019; Saglam et al., 2023) who advocate for the integration of cyber-security education at all levels in dealing with the increasing rate of cybercrimes, especially financial. Scholars in Nigeria (Ekwenchi & Shadrach, 2023) argued that the high rate of digital illiteracy among Nigerians is a key factor encouraging cyber fraud in the country. They further explained that many Nigerians are not conscious of the risks associated with the use of digital media such as the Internet and smart devices; hence, they shared their personal information online without caution as well as engaged in several risky behaviors that put them at a higher risk of cyberfinancial fraud.

Secondly, the study aimed to determine the correlation between cyber-security education and the user's ability to detect cyber-financial crime and the tendency to adopt precautions to curtail vulnerability. The results indicate that cybersecurity education enhances individuals's ability to detect cyber financial scams. Specifically, the study established that participants who were exposed to the intervention (treatment group) scored higher in identifying phishing emails, fake websites, URLs, and identity theft attempts than those who did not receive cyber-security education (control group). The finding here further validated the second hypothesis (H2). This finding aligns with prior findings (Jampen, et al., 2020; Graham & Triplett, 2016; Amankwa, 2021; McCrohan, et al., 2010). The prior studies agreed that users who are educated in terms of cyber security can easily identify risks and data breach strategies employed by cyber criminals. This goes to imply that individuals who are exposed to cyber-security training will develop the knowledge and skills to spot phishing mail, social engineering, identity theft, investment scams, and other complex ways cybercriminals are employed. This understanding will help them navigate the digital ecosystem with confidence, unlike those individuals that are not exposed to any training.

Finally, the effectiveness of cyber education in motivating intentions toward the adoption of precautions to curtail online financial scams was established in the current study. The outcome of the study revealed participants who received cyber security (experimental group) demonstrated more willingness to adopt



precautionary measures such as avoiding suspicious emails, websites, and URLs, improving password management, using anti-virus software, and clearing cookies, among others, than participants who did not receive any treatment. The implication is that the provision of cyber security education can serve as a motivation for the adoption of protection measures among new media consumers, particularly undergraduate students in Nigeria. This corroborates the submission of prior studies (Anderson, et al, 2024); these prior studies previously established a positive relationship between digital literacy and behavioural changes toward cyber protection. Research (Omodunbi, et al, 2016; Ibikunle & Eweniyi, 2013) in Nigeria categorically remarked that to combat cybercrimes, people need to be empowered with the required knowledge of the strategies employed by cyber criminals; such understanding can significantly encourage them to be on watch against any criminal tendency directed at them online.

Implications for Theory

Theoretically, this study confirms the postulations of the inoculation theory. By implication, the provision of cyber education empowers people to be “inoculated” against cyber criminals, hence reducing their vulnerability. Additionally, this study has extended studies on cyber education, which failed to conduct experiments to determine the influence of cyber education. It has also bridged the gap regarding the paucity of similar studies in Nigeria, despite the high rate of cybercrime.

Implications for practice

The outcome of the study calls for the Nigerian government and relevant agencies to intensify their efforts in improving safeguarding new media consumers and sanitising the Nigerian digital media ecosystem. In this regard, cyber education should be made a compulsory subject at all levels of education in the country. Similarly, the ministry of information, through the National Orientation, should design a framework for informal cyber-security education delivery using diverse channels of communication, including the mass media. As part of social responsibility, digital service providers, including banks and e-commerce platforms, should provide multi-media cyber educational contents for their customers, which should be easily accessible on their various platforms.

Conclusion, Limitation, and Suggestion for Further Studies

This study demonstrated the fact that provision of cyber security education in Nigeria will significantly contribute to awareness, knowledge, and likelihood to adopt protection measures against cyber criminals, hence reducing the rate of causalities. However, caution is needed in applying the findings of this study to the general population. This is because the study used a limited sample from a demographic group of students in a single institution. Therefore, there is a need to retest the findings using other demography as well as expanded sample samples in different settings in Nigeria. Nevertheless, the study was able to bring to light the strategic role of cyber education in promoting cyber safety, particularly as it relates to financial-related crimes that have bedevilled Nigeria and undermined digital economy activities.

Acknowledgements: The author would like to thank the specialists and lecturers of cybersecurity who assisted in delivering the eight-week educational intervention. Appreciation also goes to the students who participated in this study.

Funding: The authors received no financial support for the research, authorship, and/or publication of this article.



Conflict of Interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

How to Cite: Shadrach, I. & Etumnu, E.W. (2026). A quasi-experiment of the efficacy of cyber-security education as a strategic intervention for enhancing financial cybercrime awareness, detection skills, and reducing vulnerability in Nigeria. *Audrezara Journal of Communication and Social Research*, 2 (1), 49-58. <https://doi.org/10.5281/zenodo.19916497>

References

- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 563060. <https://doi.org/10.3389/fcomp.2021.563060>
- Aliyu, A., Muhammad, Z., Adamu, B. A. A., & Abdulrahman, C. Y. (2023). Cyber security education and awareness. *Ilaro Journal of Science and Technology (IJST)*, 3, 1–5. <https://sciencetechjournal.federalpolyilaro.edu.ng>
- Anderson, M., March, E., Land, L., & Boshuijzen-van Burken, C. (2024). Exploring the roles played by trust and technology in the online investment fraud victimisation process. *Journal of Criminology*, 57(4), 488–514. <https://doi.org/10.1177/26338076241248176>
- Babbie, E. R. (2015). *The practice of social research*. Nelson Education.
- Chika, D. M., & Tochukwu, E. S. (2020). An analysis of data protection and compliance in Nigeria. *International Journal of Research and Innovation in Social Science (IJRISS)*, 6(5), 377–382.
- Compton, J., Jackson, B., & Dimmock, J. A. (2016). Persuading others to avoid persuasion: Inoculation theory and resistant health attitudes. *Frontiers in Psychology*, 7, 122. <https://doi.org/10.3389/fpsyg.2016.00122>
- Eboibi, F. E., & Ogorugba, O. M. (2023). Cybercrime regulation and Nigerian youths' increasing involvement in internet fraud: Attacking the roots rather than the symptoms. *Journal of Legal, Ethical and Regulatory Issues*, 26(S2), 1–17.
- Ekwenchi, O. C., & Shadrach, I. (2023). Navigating the digital abyss: A conceptual exploration of internet privacy, personal data safety, and the path forward. *Jalingo Journal of Social and Management Sciences*, 5(3), 207–217.
- Ezennia, C. S., & Marimuthu, M. (2020). Factors that positively influence e-commerce adoption among professionals in Surulere, Lagos, Nigeria. *African Journal of Science, Technology, Innovation and Development*, 14(2), 405–417. <https://doi.org/10.1080/20421338.2020.1840051>
- Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *International Journal on Emerging Technologies*, 11(5), 41–49.
- George, G. (2023, April 2). Bank customers, companies lose billions to Nigeria's weak cybersecurity. *Punch Newspapers*. <https://punchng.com/bank-customers-companies-lose-billions-to-nigerias-weak-cybersecurity/>
- Goldstein, K., Tov, O. S., & Prazeres, D. (2018, April 9). The right to privacy in the digital age. *Pirate Parties International Headquarters*. <https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf>
- Graham, R., & Triplett, R. (2016). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*, 38(12), 1371–1382. <https://doi.org/10.1080/01639625.2016.1254980>



- Ibikunle, F., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: Challenges and solution. *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE)*, 1(1), 1–13. <https://www.ijcrsee.com>
- Igwe, K. N., & Ibegwam, A. (2014). Imperative of cyber-ethics education to cybercrimes prevention and cyber-security in Nigeria. *International Journal of ICT and Management*, 2(2), 102–113
- Ikuero, F. E., & Zeng, W. (2022). Improving cybersecurity incidents reporting in Nigeria: Micro and small enterprises perspectives. *Nigerian Journal of Technology (NIJOTECH)*, 41(3), 512–520. <https://www.nijotech.co>
- Kikerpill, K. (2020). The individual's role in cybercrime prevention: internal spheres of protection and our ability to safeguard them. *Kybernetes*, 50(4), 1015–1026. <https://doi.org/10.1108/k-06-2020-0335>
- Jampen, D., Gür, G., Sutter, T., et al. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, 10. <https://doi.org/10.1186/s13673-020-00237-7>
- Lim, S. S., & Tan, K. R. (2020). Front liners fighting fake news: Global perspectives on mobilizing young people as media literacy advocates. *Journal of Children and Media*, 14(4), 529–535. <https://doi.org/10.1080/17482798.2020.1827817>
- Makeri, Y. A. (2017). Cybersecurity issues in Nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), 1–6. <https://www.ijarcsse.com>
- McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, 9(1), 23–41. <https://doi.org/10.1080/15332861.2010.487415>
- McGuire, W. J. (1961). The Effectiveness of Supportive and Refutational Defenses in Immunizing and Restoring Beliefs against Persuasion. *Sociometry*, 24, 184–197. <https://doi.org/10.2307/2786067>
- Matusitz, J., & Breen, G.-M. (2005). Prevention of sexual harassment in the medical setting: Applying inoculation theory. *Journal of Health and Social Policy*, 21(2), 53–71.
- Njoku, D. O., Nwokorie, E. C., Okolie, S. A., & Odii, J. N. (2019). Cyberspace activities awareness and security strategies in tertiary institutions in Nigeria. *Iconic Research and Engineering Journals*, 3(2), 439–450. <https://doi.org/10.1701507>
- Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *FUOYE Journal of Engineering and Technology*, 1(1), 37–45. <https://engineering.fuoye.edu.ng/journal>
- Ojolo, T. L., & Singh, S. B. (2023). Combatting Yahoo-Yahoo phenomenon in Nigeria: Deepening analysis and rethinking new strategies. *Interdisciplinary Journal of Economics and Business Law*, 12, 82–96.
- Omarini, A. (2022). The changing landscape of retail banking and the future of digital banking. In M. Heckel & F. Waldenberger (Eds.), *The future of financial systems in the digital age: Perspectives in law, business and innovation* (pp. 189–203). Springer. https://doi.org/10.1007/978-981-16-7830-1_8
- Saglam, R. B., Miller, V., & Franqueira, V. N. L. (2023). A systematic literature review on cybersecurity education for children. *IEEE Transactions on Education*, 66(3), 1–15.
- Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2023). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*, 2(6), 455–513. <https://doi.org/10.1016/j.jiixd.2023.12.001>
- Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-



Audrezara Journal of Communication and Social Research (AJCSR), Vol. 2(1), 49-58, 2026.

- based results, challenges, and promise. *Computers & Security*, 119, 102756. <https://doi.org/10.1016/j.cose.2022.102756>
- Statista. (2024, June 28). Internet usage in Nigeria. https://www.statista.com/topics/7199/internet_usage-in-nigeria/
- Tarrad, K. M., Al-Hareeri, H., Alghazali, T., Ahmed, M., Al-Maeeni, M. K. A., Kalaf, G. A., Alsaddon, R. E., & Mezaal, Y. S. (2022). Cybercrime challenges in Iraqi academia: Creating digital awareness for preventing cybercrimes. *International Journal of Cyber Criminology*, 16(2), 15–31. <https://doi.org/10.5281/zenodo.4766564>
- Tew, P. A. D. (2019). Cybersecurity education in Nigeria: A pre-requisite for the life-long learner in the 21st century. *The Colloquium*, 7(1), 18–21.