

IMPACT OF SOCIAL MEDIA BASED-DIGITAL LITERACY ON REDUCTION OF INTERNET FRAUD AMONG ECONOMICS EDUCATION UNDERGRADUATES IN SOUTH EAST, NIGERIA

Chiamaka K. Ugwuanyi, Joseph C. Onuoha, Njideka D. Eneogu, & Grace O. Ugwonna

Department of Social Science Education, University of Nigeria, Nsukka
Email: chiamakakosy@gmail.com

Abstract

University students' increasing usage of social media has led to both potential for online education and increased susceptibility to online fraud and other cybercrimes. This study looked at how digital literacy based on social media affected the decline in online fraud among South East Nigerian Economics Education undergraduate students. The study used a quasi-experimental research methodology with 85 undergraduate students of Economics Education chosen from three public universities in South East Nigeria. It was based on frameworks for digital competence and social learning. Participants were divided into two groups: the intervention group and the control group. Cyber ethics, online risk detection, privacy management, critical evaluation of online content, and fraud prevention strategies were the main topics of an eight-week structured social media-based digital literacy program that was given to the intervention group via interactive platform like WhatsApp. Validated tool measuring vulnerability to online fraud ($\alpha = .78$) were used to gather data both before and after the intervention. According to the results, the intervention group's members showed a statistically significant decrease in their vulnerability to online fraud, dangerous online conduct, and cybercrime-related involvement goals. The study comes to the conclusion that structured digital literacy treatments based on social media can be a useful way to protect undergraduates from online fraud. It suggests that in order to encourage responsible online behavior and improve cyber safety in Nigerian higher education institutions, digital literacy programs should be incorporated into university curricula and student orientation programs.

Keywords: Social media, digital literacy, internet fraud, cyber safety, undergraduates, intervention study, Nigeria.

Introduction

Globally, the spread of social media platforms has drastically changed social interaction, education, and communication. Information technology is evolving in step with the times to help individuals with various parts of their lives, particularly obtaining or locating information that is flowing in cyberspace (Apriya et al., 2023). Due to the unparalleled rate of global digitization, the internet has become a necessary tool for most people's everyday life, providing access to a limitless amount of information and communication channels (Apsimet et al., 2024). Social media is become a major platform for academic cooperation, information sharing, digital business, and civic participation among college students, rather than just a tool for networking and amusement. Social media is used by modern people for communication, networking, and advertising, but they should be aware that it has turned into an ideal setting for cybercriminals (Ismaeel, 2025). Since the mid-2010s, internet connectivity has expanded rapidly throughout Nigeria, drastically altering

daily life, with universities being especially impacted (Apsimet et al., 2024). According to Zaliznyak et al. (2023) members of departments were able to meet during COVID-19 pandemic through social media. Besides, majority of initiatives to transact and communicate very well on their social media have been led by practitioners (Dolan et al., 2015). Undergraduates in Nigeria, especially in the South East geopolitical zone, regularly use social media and educational platforms including Facebook, Instagram, Telegram, WhatsApp, and X (previously Twitter). These platforms expose students to a number of cyber hazards, such as identity theft, phishing scams, internet fraud, and financial exploitation, even while they also offer chances for knowledge gain and digital participation. Global communication, trade, and information dissemination have all seen substantial changes as a result of the internet's stability and sharp growth (Althibyani & Al-Zahrani, 2023). Both positive and bad effects are possible in the Kingdom of Saudi Arabia (KSA), where people are more connected to the digital world (Ismaeel, 2025). Digital literacy, or the ability to use digital tools and platforms that allow users to do tasks critically and independently, is a crucial factor in determining how an individual functions in cyberspace (Alhothali & Enezi, 2023). People are prone to situations like recurring phishing attempts and risky cyber-attack techniques that target their personal and financial data because they do not have enough understanding about the many sorts of cyberattacks, which are a growing global problem (Barreda, 2022; Mo et al., 2024).

Higher education institutions in Nigeria are increasingly concerned about internet fraud. Students' susceptibility to online fraud has increased due to the growing complexity of cybercriminals, the prevalence of digital access, and the lack of organized cybereducation. Cybercriminals find undergraduates to be appealing targets because they frequently participate in online transactions, remote work opportunities, digital marketing, cryptocurrency investments, and peer-to-peer transfers. Alongside economic difficulties, cybercrime has become more alluring in Nigerian university (Odoh & Oghuvbu, 2026). Odoh and Oghuvbu continued by stating that due to financial strain and a lack of employment options, many students have turned to online criminal activity as a method of surviving. According to reports from 2019 and 2022, there has been a concerning rise in cyber-related offenses among students, many of whom justify these behaviors as coping strategies in a difficult economic climate (Odoh & Oghuvbu, 2026). In addition to victimization, peer pressure, financial difficulty, and the normalization of online deviance in some online communities have all been identified as factors contributing to youth involvement in cyber-related misconduct. The most common types and methods of financial crimes enabled by social media platforms were phishing, identity theft, online fraud, cyber extortion, and hacking (Ali et al., 2025). These facts highlight the critical need for educational techniques that are more preventive than punitive.

In the twenty-first century, digital literacy has become a crucial skill. Digital literacy is the ability to utilize, engage with, access, and comprehend the digital environment is all part of the complex phenomenon (ismaeel, 2025). Digital literacy goes beyond basic technology abilities and includes the capacity to assess online material critically, comprehend digital footprints, safeguard personal information, identify fraudulent schemes, and act morally in digital settings. Digital literacy has long been a major issue and it plays a big part in solving issues in the Revolution 4.0 period (Apriya et al., 2023). In the meantime, social media has emerged as the most convenient location for people

to conduct their daily tasks, including finding information and thus, digital literacy may be maximized on social media platforms to stop current fraud, namely Islamic financial fraud involving social engineering (Apriya et al., 2023). By using the same platforms where hazards arise as avenues for structured learning and behavioral reorientation, social media-based digital literacy expands on this idea. Social media platforms can function as easily available and contextually relevant instruments for raising cyber awareness and preventing fraud through interactive material, peer modeling, multimedia engagement, and real-time feedback.

According to Althibyani and Al-zahrani (2023), students' awareness of and ability to prevent cybercrime through the development of responsible online behavior is often greatly impacted by digital citizenship. Also, Olubori and Adisa (2025) findings demonstrated that while students were generally comfortable using digital information, many of them were only mediocre at analyzing or assessing the reliability of online content. It has been demonstrated artificial intelligence-powered systems can efficiently be used to detect and prevent cybercrime in Nigerian tertiary institutions by identifying anomalous patterns of cyberattacks and finding threat data from several sources (Nwajioha & Gideon, 2025). Research showed a strong and unquestionable correlation between students' involvement in illegal cyber-acts and their level of legal awareness about cybercrime (Alhadidi et al., 2024). Similarly, it has been demonstrated that students' careless cybersecurity behavior on PCs and smartphones, and notable variations in students' cybersecurity behaviors were discovered when comparing them to socioeconomic and digital gap factors (Farooq et al., 2023). According to Obikoya (2025.) The study showed a correlation between more positive online behaviors, like critical online information assessment and responsible internet use, and greater levels of digital literacy. The economic impact of online fraud among Ghanaian tertiary students was studied by Abdul-Barik et al. in 2025. They discovered that fraud has a detrimental effect on academic achievement and that students would profit from rerouting their ICT skills into respectable careers. Purnama et al. (2021) discovered that among 300 elementary pupils, digital literacy had a substantial impact on reducing online risk. Furthermore, 30 undergraduate students' harmful internet activities were decreased by a digital literacy intervention, as shown by Gong et al. in 2025.

Previous research have looked at university students' digital literacy as well as the frequency of online fraud. However, no empirical research has particularly examined how structured social media-based digital literacy interventions can lessen South East Nigerian undergraduates' vulnerability to online fraud. Instead of evaluating workable preventive frameworks, a large portion of the discourse stays descriptive, focusing on prevalence and causes. Therefore, evidence-based treatments that combine techniques for behavioral change with the development of digital competence are needed in the very digital ecosystems that students often live in. Thus, this study examined the effect of social media-based digital literacy on lowering internet fraud among undergraduate students in South East Nigeria, with a foundation in digital competence theory and social learning perspectives. The researchers hypothesized that social media-based digital literacy had significant impact on the reduction of internet fraud among undergraduate students in South East Nigeria The study' finding adds to the expanding couple of research on cyber preventive education by investigating whether focused digital literacy

instruction given via social media platforms might affect students' knowledge, attitudes, and online behaviors. In order to promote safer and more responsible digital involvement in Nigerian institutions, the results are anticipated to influence institutional policy, curriculum design, and student development initiatives.

Methodology

Research Design

To find out how social media-based digital literacy affects the decline in internet fraud among South East Nigerian undergraduate students, this study used a quasi-experimental pretest–posttest control group design. The design made it possible to compare a control group that did not receive the intervention with an intervention group that was exposed to a structured digital literacy program. To evaluate changes attributable to the treatment, measurements were made both before and after the intervention.

Area of the Study

The study was carried out at a few public universities in Nigeria's South East geopolitical zone, which includes the states of Abia, Anambra, Ebonyi, Enugu, and Imo. The area was picked because young people use the internet extensively and there are growing worries about cyber-related activities in higher education.

Population of the Study

All Economics Education undergraduate students enrolled in South East Nigerian public universities during the 2025–2026 academic year made up the population. Students in grades 100–400 who regularly utilize social media platforms for both social and academic objectives were the target market.

Sample and Sampling Technique

A multistage sampling technique was used to choose 85 Economics Education undergraduate students as a sample: Step 1: From the South East region, three public universities were specifically chosen. Stage 2: Within each institution, department of social science education were chosen purposively. Stage 3: To guarantee representation of the target population, Economics Education students were chosen by stratified random sampling according to their gender and year of study. At random, participants were paired with: Groups for Intervention (n = 42) and Control (n = 43)

Instrumentation

The Internet Fraud Susceptibility and Engagement Scale (IFSES) was used to gather data. This instrument had 15 items rated on 4-point scale of strongly agree to strongly

disagree. These items evaluated propensity to engage in online fraud, risky digital behaviors, and susceptibility to online frauds.

Validity and Reliability

Experts in measurement and evaluation, educational psychology, and cybersecurity studies validated the instruments. Thirty undergraduates who were not part of the study sample participated in the pilot testing. The instrument's Cronbach's Alpha coefficient of 0.78 indicates strong internal consistency.

Experimental procedure

Pretest was administered to both groups before the intervention which was done through online social media platform. Specifically, the intervention was facilitated through WhatsApp platform. To facilitate students' active participation, they were provided with data subscript for the period of the intervention. After the intervention period which lasted for 8 weeks, posttest was administered immediately after the 8-week programme.

Intervention Procedure

The eight-week intervention was conducted via social media sites like Telegram and WhatsApp. The organized program addressed:

1. Cyber ethics and conscientious online conduct
2. Recognizing fraudulent schemes, frauds, and phishing
3. Awareness of digital footprints
4. Password security and privacy protection
5. Using critical thinking to assess web information
6. Cybercrime reporting and prevention

Short instructional films, infographics, weekly live chats, scenario-based simulations, peer group reflections, and interactive tests were some of the delivery methods used.

The control group carried on with their regular academic pursuits without any formal training.

Method of Data Analysis

Analysis of Covariance (ANCOVA) was used to adjust for pretest variations in the data. Using SPSS (Version 26 or later), hypotheses were tested at the 0.05 level of significance.

Ethical Considerations

Ethical clearance was obtained from the institutional research ethics committee. Participants provided informed consent. Participation was voluntary, and withdrawal was permitted at any stage. No identifying information was collected. The intervention content emphasized preventive education and ethical online conduct.

Results

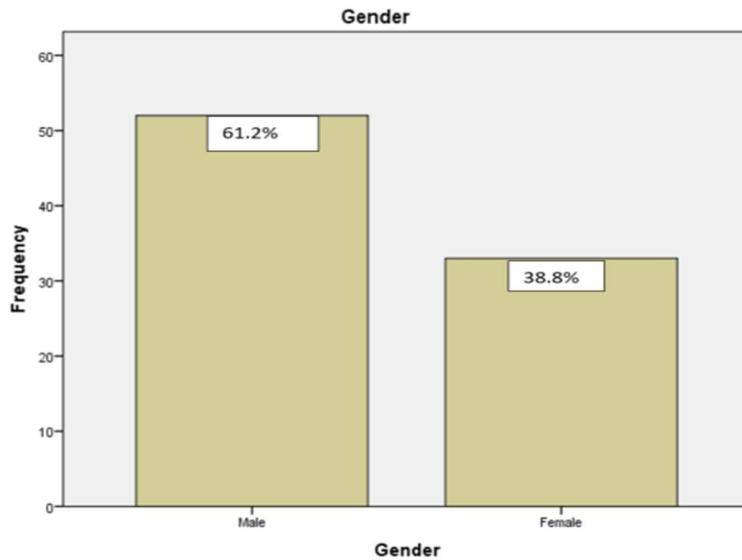


Figure 1: Bar chart presentation of the participants' gender

Figure 1 indicates that 61.2% of the participants are male students while 38.8% are female students.

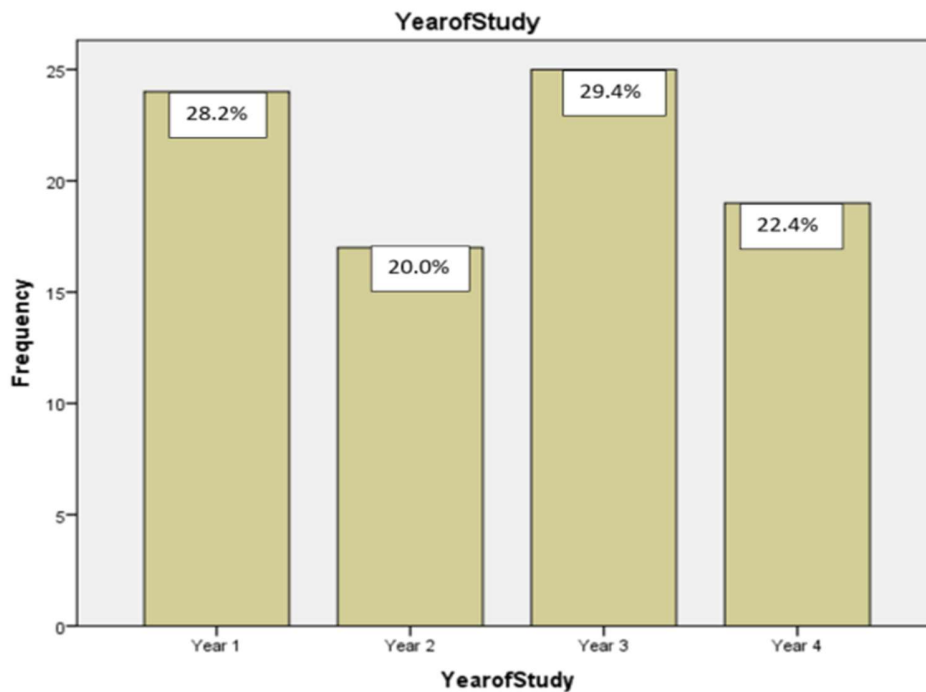


Figure 2: Bar chart presentation of the participants' years of study

Figure 2 indicates that 28.2% of the participants are year 1 students, 20.0% are year two students, 29.4% are year three students while 22.4% are year four students.

Table 1
Mean analysis of the internet fraud scores of participants of the experimental and control groups

Treatment	n	Pretest		Posttest		Adjusted Mean
		Mean	Std. Deviation	Mean	Std. Deviation	
Experimental Group	42	46.88	4.84	27.02	6.66	
Control Group	43	46.95	4.81	44.07	8.60	

Table 1 shows that students of the experimental group had similar pretest mean internet fraud scores ($M = 46.88$, $SD = 4.84$) with those of the control group ($M = 46.95$, $SD = 4.91$). However, at the posttest, the mean internet fraud score of the experimental group ($M = 27.02$, $SD = 6.66$) decreased more than those of the control ($M = 44.07$, $SD = 8.60$).

Table 2
Analysis of covariance of the difference in the mean fraud scores of the experimental and control groups

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	6268.215 ^a	2	3134.108	53.239	.000	.565
Intercept	549.537	1	549.537	9.335	.003	.102
Pretest	94.570	1	94.570	1.606	.209	.019
Treatment	6161.664	1	6161.664	104.669	.000	.561
Error	4827.197	82	58.868			
Total	119106.000	85				
Corrected Total	11095.412	84				

Table 2 reveals that there is a significant difference in the mean fraud scores of the experimental and control groups, $F(1, 82) = 104.669$, $p = .000$. Thus, the null hypothesis is rejected since the associated probability value of .000 is less than the .05 level of significance. Besides, the partial eta square of .561 shows that 56.1% reduction in the mean internet fraud score of the students is attributed to the effect of social media-based digital literacy. This implies that social media-based digital literacy had a statistically significant effect on lowering South East Nigerian undergraduate students' vulnerability to online fraud.

Discussion of Findings

The results of this study showed that social media-based digital literacy had a statistically significant effect on lowering South East Nigerian undergraduate students' vulnerability to online fraud. Compared to their peers in the control group, students who took part in the structured eight-week intervention showed enhanced digital literacy competencies, a significant decrease in risky online behaviors, and a decreased susceptibility to fraudulent schemes. The notable improvement seen in the intervention group indicates that

students' ability to identify and steer clear of fraudulent online behaviors is successfully improved by structured exposure to digital literacy content offered through well-known social media platforms. This result is consistent with the fundamental tenets of digital competence theory, which holds that people who possess critical assessment abilities, privacy management expertise, and cyber-ethical awareness are less likely to become victims of online fraud. The intervention made use of students' pre-existing digital environments by delivering teaching via platform like WhatsApp. Engagement, relevance, and knowledge retention were probably all improved by this contextualized learning strategy. Students may have been better able to recognize phishing attempts, fraudulent investment schemes, impersonation scams, and other fraudulent strategies as a result of the interactive components, which included peer discussions, quizzes, and simulations. The statistically substantial decrease in the vulnerability to online fraud shows that digital literacy is more than just theoretical understanding; it also results in quantifiable behavioral change. Those who were exposed to the intervention shown less propensity to respond to dubious digital solicitations, share private information online, or conduct unconfirmed financial transactions.

These findings are in line with the previous related findings. For instance, Obikoya (2025) demonstrated a link between higher levels of digital literacy and more constructive online behaviors, such as evaluating online content critically and using the internet responsibly. Abdul-Barik et al. investigated the financial effects of internet fraud on Ghanaian university students in 2025. They found that students would benefit from redirecting their ICT talents into respectable employment and that academic progress is negatively impacted by fraud. Digital literacy significantly reduced online risk among 300 elementary school students, according to Purnama et al. (2021). Additionally, Gong et al. (2025) demonstrated that a digital literacy intervention reduced the detrimental online habits of 30 undergraduate students.

Social learning viewpoints, which stress that behavior may be changed through supervised exposure, modeling, and reinforcement in social settings, are supported by this research. Students most likely adopted safer digital standards and strengthened self-regulatory practices through peer conversations and real-time feedback within the social media groups.

Additionally, the decrease in susceptibility implies that proactive capacity-building rather than punitive measures might be the emphasis of preventative education as a way to tackle cybercrime risks within tertiary institutions.

Contextual Implications for South East Nigeria

Due to South East Nigeria's socioeconomic conditions, which include high rates of youth unemployment and widespread digital connectivity, internet fraud can flourish as both victimization and deviant activity. The study's noteworthy findings indicate that organized digital literacy programs can serve as protective factors by encouraging critical online involvement, ethical reasoning, and responsible digital citizenship. Additionally, using social media to provide the intervention shows cost-effectiveness and scalability. By using readily available digital technologies to promote cyber safety awareness, universities in the area might incorporate similar programs without making significant infrastructural investments.

Theoretical and Practical Contributions

By providing empirical evidence that social media-based digital literacy treatments can result in quantifiable decreases in undergraduates' susceptibility to online fraud, the findings add to the body of current literature. This study offers evidence for a workable preventative plan based on educational psychology and behavioral change concepts, in contrast to studies that only record prevalence rates of cybercrime.

From a practical standpoint, the findings support:

- The establishment of required courses in digital literacy

- Including cyber ethics in courses on general studies
- Ongoing internet awareness initiatives via social media sites run by the university
- Cooperation between cybersecurity organizations and educational institutes

Conclusion of the Discussion

In conclusion, the noteworthy effect seen demonstrates that digital literacy based on social media is a successful defense against online fraud among South East Nigerian undergraduate students. Structured digital treatments can lessen susceptibility to online deception and encourage safer digital involvement in higher education settings by improving critical assessment abilities, cyber awareness, and ethical online behavior.

References

- Abdul-Barik, A., Katara, S., & Malik, B. S. (2025). The Economic Impact of Internet Fraud among Students of Tertiary Institutions in the Upper East Region of Ghana. *Asian Journal of Research in Computer Science*, 18(9), 1-9.
- Agina-Obu, R., & Okwu, E. (2023). Impact of digital literacy on university students' use of digital resources in Nigeria. *Asian Journal of Information Science and Technology*, 13(2), 60-65.
- Alhadidi, I., Nweiran, A., & Hilal, G. (2024). Heliyon The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, 10(12), e32371. <https://doi.org/10.1016/j.heliyon.2024.e32371>
- Alhothali, H. M., & Enezi, M. O. (2023). The role of digital education in reducing the risk of cyberbullying among female secondary school students from their point of view in Riyadh-Saudi Arabia.
- Ali, J. O., Nsude, I., Stephen, E., & Nwiphuru, C. (2025). Social media and financial cybercrimes among undergraduates of Alex-Ekwueme Federal University, Ndufu Alike Ikwo, Ebonyi State, Nigeria. *International Journal of Sub-Saharan African Research*, 3(1), 350-359.
- Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on preventing cybercrime. *Sustainability*, 15(15), 11512.
- Apriya, S., Akbar, W., & Jaki, A. (2023). *The urgency of digital literacy in social media to prevent fraud in Islamic banking*. 135–154.

- Apsimet, N. M., Smanova, A. B., & Utegenova, G. A. (2024). *The role of the Internet in the evolution of fraud : a historical aspect*.
- Arslantas, T. K., Yaylacı, M. E., & Özkaya, M. (2024). Association between digital literacy, internet addiction, and cyberloafing among higher education students: A structural equation modeling. *E-learning and Digital Media*, 21(4), 310-328.
- Barreda, M. B. (2022). Crime Rates in the Philippines: A Comparative Analysis of Bulan and Irosin Municipalities from Sorsogon Province. *Journal of Advances in Humanities Research*, 1(3), 37–57. <https://doi.org/10.56868/jadhur.v1i3.136>.
- Buchan, M. C., Bhawra, J., & Katapally, T. R. (2024). Navigating the digital world: development of an evidence-based digital literacy program and assessment tool for youth. *Smart Learning Environments*, 11(1), 8.
- Dolan, R., Conduit, J., Fahy, J., & Goodman, S. (2015). *Social media engagement behaviour : a uses and gratifications perspective*. 4488(December). <https://doi.org/10.1080/0965254X.2015.1095222>
- Gong, J., & Popescu, A. (2025). The Impact of a Digital Literacy Intervention on Internet Addiction and Social Skills in Undergraduate Students.
- Farooq, N., Naveed, K., & Sumera, I. (2023). *Effects of socioeconomic and digital inequalities on cybersecurity in a developing country* (Issue 0123456789).
- Ikwo, N. A., State, E., Ogayiali, J., Nsude, I., Stephen, E., & Nwiphuru, C. (2025). *Social Media and Financial Cybercrimes among Undergraduates of Alex-*. 3(1), 350–359. <https://doi.org/10.5281/zenodo.15100957>
- Ismaeel, S. (2025). The Impact of Digital Literacy on Cybercrime Awareness, Victimization, and Prevention Measures: A Study of Cyberbullying in Saudi Arabia. *Pakistan Journal of Criminology*, 17(1).
- Mo, H., Chitbanchong, S., Puchatree, N., & Thepphitak, S. (2024). Assessing and Enhancing Core Competencies in Vocational Education: A Case Study of Senior Students at Guangxi Police College, China. *International Journal of Management Thinking*, 2(2), 1–19. <https://doi.org/10.56868/ijmt.v2i2.59>
- Nwajioha, P. N., & Gideon, U. (2025). *Application of Digital Technologies in Combating Cybercrime in Nigerian Tertiary Institutions : A Study of Ebonyi State University , Abakaliki*. 2(2), 11–23.
- Odoh, F. A., & Oghuvbu, E. A. (2026). Cybercrime among Delta State University Students, Abraka, Nigeria, from 2015 to 2024. *Islamic University Journal of Social Sciences*, 5(1), 132-145.
- Olubori, O. O., & Adisa, R. M. (2025). Media literacy competencies and online fraud awareness: A study of social media users at Kwara State University. *International Journal of Intellectual Discourse*, 8(4).

Oluwatoyin, G. O. (2025). Impact of digital literacy on secondary school students' online behaviour and well-being in Rivers East Senatorial District, Rivers State. *Journal of Professional Counselling*, 8(1), 193-204.

Purnama, S., Ulfah, M., Machali, I., Wibowo, A., & Narmaditya, B. S. (2021). Does digital literacy influence students' online risk? Evidence from Covid-19. *Heliyon*, 7(6).

Zaliznyak, M., Tsai, K., Gaither, T. W., Wong, R., Duel, B., & Hamilton, Z. (2023). *Analyzing the growth in social media proliferation in academic urology*. 17(2), 69–71