Media literacy competencies and online fraud awareness: A study of social media users at Kwara State University

*Olumide Oluwafemi Olubori[1], and Rasaq M. Adisa[2]

[1]Department of Mass Communication, Faculty of Information and Communication Technology, Kwara State University, Malete - Nigeria.
[2]Department of Mass Communication University of Ilorin, Nigeria.*

*Corresponding Author: femibori@gmail.com

Abstract

The rise of social media and digital communication has created new opportunities for students, but it has also made them more vulnerable to different forms of online fraud. This study explored how students' media literacy skills relate to their awareness of online fraud at Kwara State University. The research used a descriptive survey design, and 392 students were selected through stratified random sampling. A structured questionnaire measured four media literacy components access, analysis, evaluation and content creation alongside students' knowledge of common online fraud practices. Descriptive statistics were used to summarise responses, while the Pearson Product–Moment Correlation was applied to determine the relationship between the key variables. The results showed that although students were generally confident in accessing digital information, many had only moderate capabilities in analysing or evaluating the credibility of online content. Awareness of fraud tactics such as phishing, fake social media profiles and scam messages was relatively high, yet only a small proportion of students had reported fraud incidents or admitted to personally losing money. The correlation test revealed a moderate but significant positive relationship between media literacy and fraud awareness (r = .460, p < 0.01), suggesting that students with stronger media literacy skills are better equipped to detect and manage online fraud risks. The study highlights the importance of strengthening media literacy within the university environment. It recommends incorporating structured media literacy training into academic programmes and expanding digital safety and cybersecurity awareness campaigns for students.

Keywords: Media literacy, online fraud awareness, students, digital safety, cybersecurity, higher education.

1. Introduction

The internet has become an integral part of modern life, transforming how people communicate, learn, and conduct business. For young people—particularly university students social media platforms such as Facebook, Instagram, X (formerly Twitter), TikTok, and WhatsApp serve as major spaces for interaction, learning, and self-expression. Beyond entertainment, these platforms provide opportunities for students to build networks, share knowledge, and connect with global conversations. However, the same digital environment that enables creativity and collaboration also exposes users to significant risks. Among the most concerning of these is internet fraud, which has become increasingly prevalent in the social media age. In 2024, the Economic and Financial Crimes

Commission (EFCC) reported securing 4,111 convictions for financial crimes, with cybercrime featuring prominently among the offences investigated. This annual result marked the highest number of convictions in the agency's history and highlighted fraud as one of Nigeria's most prevalent digital threats. Similarly, the Nigerian Communications Commission (NCC) has recognised that e-fraud including identity theft, phishing, and unauthorised access to personal information poses a significant risk to consumers and digital users across the country. For instance, the NCC Director of Consumer Affairs reported that Nigerians lost an estimated ₦12.5 billion to telecommunications-related financial crimes over four years, noting phishing, hacking, and identity fraud as major components of e-fraud. This is Heraldviews. These local trends mirror broader global concerns about cybercrime, reinforcing the reality that while digital platforms enable connectivity, they also attract sophisticated fraudulent behaviours that target unwary users.

According to the Federal Trade Commission (FTC, 2025), scam-related losses linked to social media platforms reached an estimated $1.9 billion in 2024 alone. Fraudsters now exploit social media's open nature through fake profiles, impersonation, and deceptive advertisements to lure unsuspecting users. Young people, who tend to trust online content and interactions, are often prime targets. For university students who spend many hours online daily the risk is amplified by curiosity, peer influence, and limited critical evaluation of information encountered on these platforms. In this context, media literacy has emerged as an essential life skill. Jeong, Cho, and Hwang (2025) define it as the ability to access, analyse, evaluate, and create media in various forms. Media literacy goes beyond technical proficiency; it encompasses the critical capacity to question, interpret, and verify media messages. A media-literate student is more likely to identify suspicious links, authenticate online sources, and avoid carelessly sharing personal data. Research consistently shows that media literacy education enhances young people's capacity to detect misinformation, resist manipulation, and make informed digital choices (Jeong et al., 2025). In Nigeria, the internet continues to play a central role in communication, education, and commerce. Mobile internet penetration has expanded rapidly, with young people representing the largest share of active users. Yet, alongside these benefits lies a troubling rise in internet-related fraud—popularly known as Yahoo Yahoo. Several studies (Esere, Idowu, Iruloh, Durosanya, & Okunlola, 2017) have shown that Nigerian youths, including university students, are not only victims but sometimes perpetrators of cyber fraud. Economic hardship, peer pressure, and exposure to fraudulent role models have been identified as key drivers of this behaviour.

University students are among the most active internet users in Nigeria. Their reliance on social media for academic activities, social interaction, and entertainment makes them particularly susceptible to cyber threats. Yet, while access to information is widespread, students do not always possess the critical skills needed to analyse, evaluate, and respond to questionable online content. This situation raises concerns about their media literacy competencies the cognitive and analytical abilities needed to interpret and use media effectively and how these competencies influence their awareness of online fraud. At Kwara State University (KWASU), thousands of students actively use social media for academic, professional, and leisure purposes. However, despite this high level of

engagement, little is known about how aware these students are of online fraud tactics or how effectively they apply media literacy skills to protect themselves. Existing studies in Kwara State and beyond have largely focused on the motivations behind cybercrime participation, while limited attention has been paid to the awareness and preventive competencies of ordinary users.

The rise of internet fraud poses not only economic but also psychological and academic risks for students. Reports from the Federal Bureau of Investigation (FBI, 2025) and FTC (2025) indicate that billions of dollars are lost annually to digital scams globally, with Nigerian youths featuring prominently in online fraud-related investigations and public discourse. University students are especially vulnerable, as their frequent online interactions, coupled with limited media literacy skills, increase their susceptibility to phishing, romance scams, and fake investment schemes. This gap in understanding forms the basis of the present study, which seeks to examine the relationship between media literacy competencies and online fraud awareness among students of Kwara State University. The study aims to determine the level of students' media literacy, assess their awareness of prevalent internet fraud tactics, and explore whether media literacy significantly influences their ability to recognise and respond to online fraud. By addressing these questions, the research contributes to a deeper understanding of how digital education and critical awareness can serve as preventive tools against online fraud among young social media users.

Problem Statement

Despite the growing use of social media among university students in Nigeria, and the increasing reports of online fraud from agencies such as the EFCC (2024) and NCC (2023), there remains limited understanding of how students' media literacy skills influence their awareness and response to internet fraud. University students, including those at Kwara State University, are among the most active digital users, relying on social media for academic work, social interactions, and entertainment. While they are adept at accessing information online, many lack the critical skills required to analyse, evaluate, and verify content. This creates a vulnerability to phishing, fake accounts, scam messages, and other forms of cybercrime. Previous studies in Nigeria have largely focused on the perpetrators of cyber fraud or general digital skill levels, with little attention paid to the preventive competencies of ordinary users. Consequently, universities lack evidence-based strategies to strengthen students' resilience against online fraud. Without sufficient media literacy, students may continue to fall victim to digital scams, resulting in not only financial losses but also psychological stress and academic disruption. This study seeks to fill this gap by examining the relationship between media literacy competencies and online fraud awareness among students of Kwara State University, providing insights that can inform interventions to enhance digital safety and responsible online behaviour.

Research Questions

To address the issues identified in the problem statement, this study focuses on examining the media literacy competencies of students and their awareness of online fraud. Specifically, it seeks to answer the following research questions:

i. What is the level of media literacy among social media users in Kwara State University?

ii. Research Question One: What is the level of media literacy among social media users in Kwara State University?

iii. Research Question Three: Is there a significant relationship between media literacy and internet fraud awareness?

2. Literature Review
Media Literacy

Media literacy has become an essential competency in the digital age, as individuals increasingly rely on media and technology for communication, learning, and daily interactions. At its core, media literacy refers to the ability to access, analyse, evaluate, and create media content across different platforms (Livingstone, 2014). However, scholars differ on how they conceptualize this skill. Buckingham (2019) emphasizes that media literacy involves both knowledge and skills to engage with media critically, suggesting a strong cognitive component. In contrast, Hobbs (2017) frames media literacy as both an interpretive and participatory practice, arguing that young people must not only consume media but also produce content responsibly. While Buckingham highlights analytical understanding, Hobbs stresses the ethical and creative dimensions of media engagement, indicating that media literacy is not purely cognitive but also social and moral. Potter (2013) expands the discussion by proposing that media literacy consists of knowledge structures, personal locus, and skills, highlighting that awareness alone is insufficient; motivation and cognitive ability are equally important. Livingstone (2004) focuses on four practical skills accessing, analyzing, evaluating, and creating media content which are particularly relevant for university students navigating social media environments. The divergence between Potter's emphasis on cognitive-motivational factors and Livingstone's practical skills framework suggests that a comprehensive understanding of media

literacy must integrate both mental preparedness and actionable competence.

Media Literacy and Online Risk/Fraud Detection

A growing body of research connects media literacy to online risk management, including fraud detection. Jeong, Cho, and Hwang (2025) argue that students with strong media literacy are better able to identify suspicious links, verify sources, and critically assess the credibility of online information. Tandoc and Maitra (2022), however, caution that technical access and analytical skills alone may not prevent victimization; students also require an ethical orientation and practical strategies to navigate deceptive online environments. In other words, one can recognize misleading content yet still make poor decisions if they lack precautionary habits or awareness of digital security. Comparing these perspectives reveals both overlap and tension. Jeong et al. (2025) focus primarily on the protective function of media literacy, emphasizing cognitive skills and critical evaluation. Tandoc and Maitra (2022) extend this by integrating behavioural and ethical dimensions, showing that media literacy must empower action, not just understanding. Together, these views highlight that media literacy serves a dual purpose for students: it protects them from online fraud while also enabling responsible participation in digital spaces. For university students, the implications are clear. Access skills allow them to retrieve academic and social information, but without analytical, evaluative, and ethical competencies, they remain vulnerable to phishing, scams, and fake social media accounts. The creation aspect further ensures students contribute responsibly, producing credible content that does not unintentionally propagate misinformation. Thus, media literacy is not merely an academic skill but

a preventive tool against digital risk, including internet fraud, which is increasingly prevalent in Nigerian social media spaces

Social Media Use Among University Students

Social media has become deeply embedded in the everyday lives of university students, shaping not only how they communicate but also how they interact with information and with one another. Unlike previous generations that relied primarily on face-to-face interactions or traditional media, today's students engage with platforms like Facebook, Instagram, WhatsApp, X, and TikTok for both academic and social purposes. However, this pervasive use comes with significant vulnerabilities, particularly in the way students are exposed to online fraud risks. Research in Nigeria and beyond consistently shows that the very features that make social media appealing its openness, immediacy, and broad reach also make it fertile ground for cybercriminal activity. Agara et al. (2021), for example, found that frequent use of platforms such as Facebook, Instagram, and Twitter significantly exposes students to various forms of cybercrime. Their study revealed that students often share personal details and interact with strangers online, actions that cybercriminals exploit to launch fraudulent activities, including phishing and identity theft. Similarly, studies on phishing behaviour in Nigeria demonstrate that exposure across multiple platforms increases vulnerability. Adeyemo, David, and Olabulo (2025) report that threats like malware, data theft, and phishing attacks vary across social media networks, with Instagram, Twitter, and Facebook being particularly exploited by fraudsters. These platforms' design encourages constant connectivity and quick responses, making it easier for scammers to catch users off guard with deceptive links or messages. A related Nigerian study found that heavy reliance on social networking sites fosters risky behaviours among undergraduates, not only because students spend extended hours online but also because they often establish connections with people they do not personally know. Such connections create opportunities for fraudsters to infiltrate personal networks, gather sensitive information, and launch scams. This pattern is echoed in research from other contexts as well. International studies demonstrate that high-risk online behaviours such as excessive social media use and unverified information sharing are linked to greater exposure to cybercrime, including phishing, malware, and social engineering attacks. These behaviours often stem from students' perception that social media interactions are safe because they occur among peers, even when malicious actors are present in those spaces. In the Nigerian university context, the interplay between heavy social media use and fraud risk is particularly striking. Not only are students exposed to deceptive content, but the social environment of these platforms where trust is often assumed and personal details are readily shared makes them especially susceptible. This reflects a broader trend in which social media use amplifies students' exposure to risks such as financial scams, fake investment schemes, and identity theft, underscoring the importance of digital literacy and proactive risk management in academic communities.

Popular Platforms Used by Students

Different social media platforms appeal to students for different reasons. WhatsApp is widely considered the most essential application because of its convenience in facilitating instant communication. Many students use it for academic discussions, group assignments, and official notices from lecturers and departmental groups

(Okunola & Adesina, 2021). Facebook, while once dominant, is now less popular among younger students but remains relevant for event updates, networking, and following institutional pages.

Instagram and TikTok have grown significantly, especially among undergraduates, due to their visual nature and ease of content sharing. These platforms allow students to showcase creativity through videos, memes, and photos. YouTube is another favorite, often used for tutorials, educational lectures, and motivational content. In contrast, Twitter (now X) is commonly used by Nigerian students for following news trends, political discussions, and online debates (Adegbola & Gearhart, 2022). The variety of platforms highlights that students' social media use is multi-purpose academic, social, creative, and informational.

Patterns of Usage

Studies have consistently shown that university students spend a significant portion of their day on social media. A global survey by Datareportal (2024) reported that individuals aged 18–24 spend between three to five hours daily on social networking sites, often switching between multiple platforms. This is consistent with research in Nigeria, where undergraduates are among the most active demographic groups online (Olatunji, 2022).

Students' usage patterns reveal that social media is not only a leisure activity but also deeply tied to their education. Many use platforms to share notes, search for online resources, and collaborate on projects. During the COVID-19 pandemic, reliance on social media for academic purposes increased, as classes and group discussions were frequently moved online (Islam et al., 2020). At the same time, however, students also reported higher exposure to misinformation and fraudulent schemes during this period, demonstrating how increased reliance on social media can come with heightened risks.

Another important pattern is the habitual nature of usage. Many students open social media apps unconsciously, sometimes multiple times within an hour. This creates a cycle of over-dependence, which researchers describe as "social media fatigue"—a state where individuals feel mentally drained but still compelled to use the platforms (Islam et al., 2020). Such habitual usage reduces critical reflection, making students less likely to evaluate the authenticity of messages they encounter.

Benefits of Social Media for Students

The benefits of social media use among university students are well-documented. First, it enhances communication and collaboration. Students can easily connect with peers, lecturers, and even global communities, making learning more interactive. Second, social media provides educational opportunities. YouTube tutorials, online study groups, and LinkedIn networking are examples of how students gain valuable knowledge and career exposure. Third, social media fosters self-expression and creativity, especially on platforms like TikTok and Instagram where students showcase talents, businesses, and ideas (Adegbola & Gearhart, 2022).

Social media also contributes to social belonging. For many students, university life can feel isolating, and platforms like WhatsApp and Instagram help maintain friendships and provide emotional support. In Nigeria, where students often live far from family, these platforms serve as vital tools for staying connected with loved ones (Okunola & Adesina, 2021).

Understanding Online Fraud/Internet Fraud

The rapid growth of the internet and social media has brought many opportunities for communication, learning, and business,

but it has also created new spaces for fraudulent activities. Internet fraud, also called online fraud or cyber fraud, refers to the use of digital platforms and deceptive techniques to trick individuals into giving away money, personal information, or access to secure systems (Aba & Ojo, 2021). It is one of the fastest-growing forms of crime globally, and young people, especially university students, are among the most vulnerable targets.

Online fraud manifests in several forms. Phishing involves sending fraudulent emails, messages, or links to trick users into revealing passwords or banking details. Scam messages and fake investment schemes lure individuals with promises of financial gain. Identity theft occurs when a person's personal information is used without consent for fraudulent purposes. Fake social media accounts are created to impersonate others or mislead users into engaging with malicious content (Aba & Ojo, 2021; Adeyemo et al., 2023). In this study, these types of fraud were operationalized in the questionnaire as specific items under the "Online Fraud Awareness" section. Respondents were asked to indicate their level of awareness or experience with each fraud type using a four-point Likert scale: Strongly Agree (SA), Agree (A), Disagree (D), and Strongly Disagree (SD). For example: "I am aware of phishing messages (fraudulent emails or texts asking for personal information),"I know about fake investment schemes used by fraudsters." "I am familiar with identity theft cases." "I know that fraudsters use fake social media accounts to deceive students." This operationalization allowed the study to quantitatively measure students' awareness of common online fraud schemes and link it to their media literacy competencies, thereby providing a basis for analyzing whether higher media

literacy is associated with greater fraud awareness.

Common Online/Internet Fraud Schemes

Several fraud schemes are commonly encountered by students in online spaces. One of the most widespread is phishing, where fraudsters send deceptive messages usually through email, SMS, or social media pretending to be trusted organizations such as banks or service providers. The goal is to lure victims into clicking malicious links or providing sensitive information like passwords, ATM card details, or identification numbers (Adeleke, 2020). Students, who often rely on online banking and mobile payment systems, are frequently targeted through such schemes.

Another common form is scam offers, including fake scholarships, investment opportunities, or job advertisements. Many students fall victim to fraudsters who promise quick financial gains or academic benefits but instead steal money or personal data (Okeshola & Adeta, 2022). These scams are especially effective because they exploit students' financial limitations and their eagerness to secure educational or career advancement. Identity theft is another major form of online fraud. Fraudsters steal personal information from victims' social media profiles, emails, or hacked accounts to impersonate them for fraudulent transactions. For instance, a student's hacked Facebook or WhatsApp account can be used to request money from their friends and family. Identity theft can also extend to the misuse of official documents such as student IDs or admission letters (Olatunji, 2022).

A related problem is the creation of fake accounts on social media. Fraudsters often pose as legitimate individuals or institutions to build trust and deceive unsuspecting users. Such accounts may be used to run romance scams, spread false

advertisements, or trick victims into sharing personal details (Aba & Ojo, 2021). In Nigerian universities, cases of fake recruitment accounts or impersonation of lecturers on Facebook and WhatsApp have been reported, further showing how students are specifically targeted.

Impacts of Internet/ Online Fraud on Students

The effects of online fraud on students are far-reaching. Financial loss is the most immediate consequence. Students who fall for phishing links, fake investment schemes, or fraudulent loan offers often lose money that is difficult to recover. For many undergraduates who depend on limited allowances from parents or guardians, such losses can cause serious hardship (Okeshola & Adeta, 2022).

Beyond financial harm, online fraud also has psychological and emotional impacts. Victims often experience stress, anxiety, and embarrassment after being deceived. Some lose trust in digital platforms altogether, which may affect their academic use of online resources and communication tools (Tandoc & Maitra, 2022). For students engaged in online learning or networking, reduced trust in the internet can limit opportunities for growth.

Another significant impact is academic disruption. Fraudulent distractions, such as fake academic links, counterfeit learning platforms, or malicious downloads, can interrupt students' studies. In some cases, students unknowingly install malware that compromises their devices, leading to data loss or exposure of sensitive academic records (Adeleke, 2020).

Online fraud also affects students' social reputation. For example, when fraudsters hack a student's social media account and use it to beg for money or spread harmful content, it damages the victim's credibility among peers. In the context of higher education, where social relationships and networks matter, such incidents can have long-term effects on students' confidence and social standing. frequent exposure to fraudulent schemes contributes to a culture of fear and insecurity among students. Some victims become overly cautious or withdraw from online spaces altogether, which reduces their ability to benefit from the opportunities that digital platforms provide. Others, in contrast, may attempt to imitate fraudsters as a survival strategy, thereby contributing to the cycle of internet fraud.

Uses And Gratification Theory

The Uses and Gratification Theory (UGT), originally developed by Elihu Katz, Jay Blumler, and Michael Gurevitch in 1974, shifts the focus from what media does to individuals to what individuals actively do with media (Katz, Blumler, & Gurevitch, 1974). Unlike earlier theories that depicted media users as passive recipients, UGT posits that people actively select media to satisfy specific psychological and social needs, including information seeking, entertainment, social interaction, personal identity, and escapism (Ruggiero, 2000).

In the context of university students, UGT helps explain why students engage heavily with social media platforms. Some students may use platforms like WhatsApp or X to collaborate on academic tasks, while others may prefer Instagram or TikTok for entertainment or self-expression. However, this active engagement with media also increases exposure to online risks, including phishing, scams, and fake social media accounts. Students who are highly motivated to use social media for multiple purposes may inadvertently overlook potential fraud signals, especially if they lack critical media literacy skills. UGT to media literacy, students' purposeful use of media interacts with their capacity to

evaluate content critically. A student with strong media literacy competencies can navigate social media with both engagement and caution, identifying suspicious messages or fraudulent schemes before acting on them. Conversely, students with limited analytical or evaluative skills may satisfy their media needs while simultaneously increasing their vulnerability to online fraud. Therefore, UGT provides a lens for understanding both the motivations for social media use and the conditions under which fraud risk is heightened or mitigated.

Protection Motivation Theory (PMT)

To complement UGT, this study also draws on Protection Motivation Theory (PMT), propounded by R.W. Rogers in 1975. PMT explains how individuals are motivated to adopt protective behaviours when confronted with perceived threats. The theory suggests that protective actions are influenced by threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy and self-efficacy) (Rogers, 1975). Applying PMT to online fraud, students are more likely to engage in fraud-preventive behaviours such as verifying links, reporting suspicious messages, or avoiding sharing sensitive information when they perceive the risk of cybercrime as serious and believe that their actions can effectively reduce that risk. Media literacy competencies play a critical role in this process: analytical, evaluative, and creative skills enhance students' ability to recognize fraudulent content and respond appropriately, thereby increasing coping appraisal and reducing susceptibility to fraud.

Together, UGT and PMT provide a comprehensive framework for this study. UGT explains why students use social media and how usage patterns may expose them to risk, while PMT explains how media literacy shapes the perception of fraud risk and motivates protective behaviours. Integrating these theories allows the study to examine both the motivational and cognitive dimensions of students' online behaviours, providing insight into the relationship between media literacy and online fraud awareness.

3. Methodology

This study employed a descriptive survey design within a quantitative research framework. The design was considered appropriate because it enabled the researcher to collect data from a large group of students and describe their levels of media literacy and awareness of online fraud in measurable terms. The approach also allowed the use of a structured questionnaire to generate quantifiable data for statistical analysis.

The population of the study consisted of all undergraduate students of Kwara State University (KWASU), Malete, Kwara State, Nigeria, estimated at about 30,000 students according to records from the university's Registry.

The calculation of Taro Yamane is presented as follows:

$$\frac{N}{1 + N(0.05)2}$$
$$= \frac{30,000}{1 + 30,000(0.05)2}$$
$$= \frac{30000}{1 + 30000(0.0025)}$$
$$= \frac{30000}{1 + 75}$$
$$= \frac{30000}{76}$$

=394.7~395

To ensure adequate representation, a sample of 392 were collect and retrieved back from the students using a recognised sample size determination Taro Yamane formula. This figure was deemed sufficient to represent the entire student population while maintaining a manageable number of participants.

Stratified random sampling was employed to ensure fair representation across different colleges and levels of study.

The main instrument for data collection was a structured questionnaire designed to elicit information on students' media literacy skills and awareness of online fraud. The questionnaire was divided into three sections:

- Section A: Captured demographic information such as age, gender, level, and college.
- Section B: Contained items measuring students' media literacy competencies, including their ability to access, analyse, evaluate, and create media content.
- Section C: Focused on assessing students' awareness of online fraud, covering their knowledge of common scam tactics, ability to identify fraudulent content, and personal experiences with online scams.

Responses in Sections B and C were measured using a five-point Likert scale, ranging from *Strongly Agree* to *Strongly Disagree*, to facilitate quantification and comparison of opinions. The questionnaire underwent expert validation by scholars in Mass Communication and Measurement and Evaluation to ensure content accuracy and clarity. A pilot test was also conducted among a small group of students outside the main sample to confirm reliability. The instrument demonstrated high internal consistency, indicating that the items effectively measured the intended variables. The questionnaires were personally administered by the researcher to enhance response accuracy and ensure a high return rate. Upon retrieval, responses were coded and analysed using the Statistical Package for the Social Sciences (SPSS). The analysis involved both descriptive and inferential statistics. Descriptive statistics such as means, percentages, frequency distributions, and standard deviations were used to summarise demographic characteristics, media literacy levels, and awareness of online fraud. Inferential statistical tests, including correlation analysis, chi-square, and t-tests, were applied to determine relationships between variables and to test the research questions. The findings were presented in tables, charts, and graphs for clarity and ease of interpretation.

4. Results and Findings

This study used a quantitative approach using a questionnaire. Out of the 395 expected sample, 392 respondents were successfully filled and retrieved representing 99.2% of the responses. The analyses were done sequence of the research questions earlier stated in the study with the aid of Statistical Package for Social Science (SPSS).

Levels of Media Literacy Competencies

Table 1   Levels of Media Literacy Competencies among Students (N=392)

Media Literacy Skills	Statement	Mean Score	Interpretation
Access to Skills	"I can easily search for academic and non-academic information online"/ "I know how to use different social media platforms effectively."	3.92	High
Analyse Skills	"I can identify the main idea or purpose of media content."/I usually compare information from multiple sources before believing it."	3.70	Moderate
Evaluate Skills	"I can judge whether online information is credible or fake."/"I check authenticity of accounts before following them."	3.55	Moderate
Create Skills	"I know how to create and share responsible online content."/"I avoid posting unverified information online."	3.40	Moderate

Source: Researchers' Field Survey, 2025
Scale used: 1.00–2.49 = Low, 2.50–3.49 = Moderate, 3.50–5.00 = High.

The findings indicate that students demonstrated the highest competency in Access skills (Mean = 3.92), indicating confidence in retrieving information online. Competencies in Analyse (Mean = 3.70), Evaluate (Mean = 3.55), and Create (Mean = 3.40) were moderate, suggesting that while students can access information, they may struggle to critically evaluate content or contribute responsibly, which could increase their susceptibility to online fraud.

Awareness of Online Fraud

Table 2   Awareness of Online Fraud among Students

S/N	Statement	SA (%)	A (%)	D (%)	SD (%)	Mean	Remarks
1.	I am aware of phishing messages (fraudulent emails or texts asking for personal Information)	160 (40.8)	120 (30.6)	90 (23.0)	22 (5.6)	3.92	High
2.	I know about fake investment schemes used by fraudsters	140 (35.7)	110 (28.1)	112 (28.6)	30 (7.6)	3.75	Moderate
3.	I am familiar with identity theft cases (someone using another person's details illegally)	130 (33.2)	100 (25.5)	130 (33.2)	32 (8.1)	3.70	Moderate
4.	I know that fraudsters use fake social media accounts to deceive students	170 (43.4)	130 (33.2)	70 (17.8)	22 (5.6)	4.00	High
5.	I have received scam messages or suspicious links online	150 (38.3)	120 (30.6)	100 (25.5)	22 (5.6)	3.85	High
6.	I know students who has lost money due to online fraud	120 (30.6)	110 (28.1)	130 (33.2)	32 (8.1)	3.65	Moderate
7.	I have personally lost money or property to internet fraud	50 (12.8)	70 (17.9)	170 (43.4)	102 (26.0)	2.90	Moderate

8.	I have reported fraud attempts to friends, authorities or online platforms	80 (20.4)	100 (25.5)	150 (38.3)	62 (15.8)	3.20	Moderate
	Grandmean					**3.62**	**Moderate**

Source: Researchers' Field Survey, 2025

Scale Used: 1.00–2.49 = Low, 2.50–3.49 = Moderate, 3.50–5.00 = High

Table 2 presents students' awareness and experiences of online fraud. The results show that students were generally aware of common online fraud schemes, particularly phishing (Mean = 3.92) and fake social media accounts (Mean = 4.00). Many students reported receiving scam messages (Mean = 3.85) and knew peers who had been defrauded (Mean = 3.65). However, personal experiences with fraud (Mean = 2.90) and reporting behaviours (Mean = 3.20) were relatively low. The grand mean of 3.62 indicates moderate to high awareness, but proactive engagement in preventing or reporting fraud remains limited.

Relationship Between Media Literacy and Online Fraud Awareness

Table 3 Correlation between student political self-efficacy and political participation

		Media_Literacy Competencies	Online_Fradu Awareness
Media_Literacy Competencies	Pearson Correlation	1	.460[**]
Online_Fraud Awareness	Pearson Correlation	.460[**]	1

Correlations is significant at the 0.001 level (2-tailed)

Source: Researchers' Field Survey, 2025

Table 3 showed the Pearson correlation efficient (r = .460, p < 0.01) which indicates a moderate positive relationship between media literacy and online fraud awareness. This revealed that student with stronger media literacy skills are more likely to be aware of online fraud schemes. The correlation is statistically significant, confirming that media literacy is an important predictor of fraud awareness.

Discussion of Findings

Research Question One: What is the level of media literacy among social media users in Kwara State University?

The findings indicate that students demonstrated high competency in accessing information (Mean = 3.92), but their skills in analyzing (Mean = 3.70), evaluating (Mean = 3.55), and creating content (Mean = 3.40) were only moderate. This pattern aligns with Adeleke (2020), who observed that Nigerian undergraduates are generally proficient in retrieving online content but often lack the critical thinking and evaluative skills necessary to judge information quality. Livingstone (2018) similarly noted that media literacy is inherently multidimensional, with many young users excelling in access but struggling with deeper cognitive skills such as evaluation and responsible content creation.

A critical reflection on this finding revealed that while students are comfortable navigating and accessing social media platforms, their moderate skills in analyzing and evaluating content may limit their ability to detect deceptive or fraudulent information, thereby increasing susceptibility to online fraud. This reflect broader educational gaps in Nigeria, where curricula often emphasize content consumption rather than critical analysis or digital ethics.

Research Question Two: To what extent are students aware of online fraud tactics?

The study revealed that students were highly aware of phishing (Mean = 3.92), fake social media accounts (Mean = 4.00), and scam messages (Mean = 3.85). However, fewer students reported personal experiences of losing money (Mean = 2.90), and the act of reporting fraud attempts was relatively low (Mean = 3.20). This indicates a gap between awareness and proactive protective behaviour.

These results echo the findings of Olayemi (2019), who observed that Nigerian youths are cognizant of internet fraud schemes but often lack the motivation or mechanisms to respond effectively. Similarly, Chiluwa and Ifukor (2019) highlighted that while awareness levels are generally high, students tend to underestimate their personal risk exposure, which may explain low reporting rates.

From a cultural perspective, factors such as peer influence, social trust, and risk perception shaped by societal narratives may contribute to this cautious but sometimes passive response. In Nigerian universities, students also fear reputational stigma or lack confidence in reporting mechanisms, which reduce the likelihood of taking corrective actions when encountering fraud.

Research Question Three: Is there a significant relationship between media literacy and internet fraud awareness?

The analysis showed a moderate positive correlation ($r = 0.460$, $p < 0.01$) between media literacy competencies and online fraud awareness. This indicates that students with higher media literacy skills are more likely to recognize fraud tactics and take precautionary measures. These results align with Adekunle and Aremu (2021), who reported that digital literacy improves students' ability to detect

fraudulent schemes, and Adeleke and Ayomide (2020), who emphasized that interventions enhancing analytical and evaluative skills reduce vulnerability to online fraud.

Critically, the correlation is moderate rather than strong, revealing that other factors influence students' awareness of fraud. Possible confounders include previous personal exposure to fraud, peer networks, trust in social media, socioeconomic background, and institutional support for digital education. For instance, students who frequently interact with tech-savvy peers learn informally about scams, independent of formal media literacy. Similarly, institutional initiatives such as awareness campaigns, orientation programs, and ICT support could enhance fraud recognition even among students with moderate literacy skills.

The Nigerian context also matters. Cultural attitudes toward risk, trust, and digital engagement shape how students interpret and act on fraud-related information. In KWASU, the blend of high social media usage with limited structured digital literacy programs may explain why awareness is high but protective behaviours and the correlation strength are moderate.

5. Conclusion and Recommendation

Based on the findings, it is concluded that media literacy plays a critical role in shaping students' awareness of online fraud. Students at Kwara State University are generally knowledgeable about common fraud schemes such as phishing, fake social media accounts, and scam messages. However, their moderate skills in evaluating and creating digital content, along with limited reporting behaviours, revealed persistent vulnerability. The study demonstrates that enhancing media literacy particularly analytical, evaluative, and content creation competencies

significantly improve students' ability to recognize and respond to online fraud, thereby reducing risk exposure in digital spaces.

Limitations of the Study

The study relied on self-reported data, which influenced by social desirability bias. The research was conducted in a single institution (Kwara State University), which limits the generalizability of findings to other universities or regions. Only quantitative methods were employed; deeper qualitative insights into students' perceptions and experiences were not captured.

Suggestions for Further Research

Other researchers should conduct multi-institutional studies to compare media literacy and online fraud awareness across different Nigerian universities. Use qualitative approaches such as interviews and focus groups to explore students' attitudes, motivations, and barriers in responding to online fraud. Examine the effectiveness of specific media literacy interventions, workshops, or campaigns in improving online fraud detection and preventive behaviours. Investigate the role of socioeconomic, cultural, and peer network factors as moderating variables in the relationship between media literacy and fraud awareness.

Recommendations

Based on the findings the following recommendations were made:

For Students:

Actively improve media literacy skills, with special emphasis on evaluating online information and reporting suspicious activities. Student should form peer-to-peer digital safety awareness groups to share knowledge, experiences, and strategies for safe online behaviour. Participate in university-led cybersecurity awareness programs and workshops.

For Kwara State University:

Integrate media literacy and digital safety modules into general studies and core academic programs. Organize regular workshops, seminars, and practical training on cybersecurity, highlighting real-life fraud cases and preventive measures. Establish a dedicated digital safety support unit to assist students in reporting and managing online fraud incidents.

Policy-Level Recommendations:

Federal and state education authorities should mandate the inclusion of digital literacy and cybersecurity awareness in tertiary education curricula nationwide. Collaboration with regulatory bodies such as the EFCC, NCC, and cybersecurity agencies to provide real-time fraud alerts, educational materials, and support for students. Promote national awareness campaigns focusing on youth-targeted online fraud and digital ethics, leveraging social media and mass media platforms.

References

Aba, E., & Ojo, S. (2021). Cybercrime and its socio-economic implications in Nigeria. *Journal of African Studies and Development, 13*(2), 47–55.

Adebayo, M. (2022). Role of social media in facilitating financial scams in Abuja, Nigeria: Development communication interventions for prevention. *African Journal of Stability and Development*. Retrieved from https://journals.abuad.edu.ng/index.php/ajsd/article/view/1812 journals.abuad.edu.ng

Adegbola, O., & Gearhart, S. (2022). Social media as a learning and networking tool among university students. *Journal of Applied Communication Research, 50*(3), 245–262.

Adeleke, A., & Ayomide, T. (2020). Social media use and vulnerability to internet fraud among undergraduates in Southwest Nigeria. *African Journal of Criminology and Justice Studies, 13*(2), 145–162.

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 (IJSSAR, 3)*. ijssar.com

Buckingham, D. (2019). *The media education manifesto*. Polity Press.

Chigozi, E. (2024). Awareness and perception of internet fraud epidemics among Nigerian youths. *African Journal of Social and Behavioural Sciences*. Retrieved from https://journals.aphriapub.com/index.php/AJSBS/article/view/2684 journals.aphriapub.com

Egielewa, P. E. (2022). *Yahooism or internet fraud in the Nigerian higher education system. Journal of Ethics in Higher Education, 1*, 75–101.

Esere, M. O., Idowu, A. O., Iruloh, B., Durosanya, A. T., & Okunlola, J. O. (2017). Factors responsible for students' involvement in internet fraud as expressed by tertiary institution students in Ilorin metropolis, Kwara State, Nigeria. *Zimbabwe Journal of Educational Research, 29*(3).

FBI. (2025). *Internet Crime Complaint Center (IC3) report: 2024 annual internet crime report* [Press release]. Federal Bureau of Investigation.

Hobbs, R. (2017). *Create to learn: Introduction to digital literacy*. Wiley.

Igwe, D. O. (2024). Students' involvement in social media fraud: A case study of Lagos State University. *African Journal of Social and Behavioural Sciences, 13*(2). journals.aphriapub.com

Islam, A. K. M. N., Laato, S., Talukder, S., & Sutinen, E. (2020). Misinformation sharing and social media fatigue during COVID-19: An affordance and cognitive load perspective. *Technological Forecasting and Social Change, 159*, 120201.

Jeong, S. H., Cho, H., & Hwang, Y. (2025). Media literacy interventions: A meta-analytic review of 40 years of research. *Human Communication Research, 51*(2), 57–79.

Katz, E., Blumler, J. G., & Gurevitch, M. (1974). Utilization of mass communication by the individual. In J. G. Blumler & E. Katz (Eds.), *The uses of mass communications: Current perspectives on gratifications research* (pp. 19–32). Sage.

Livingstone, S. (2014). Media literacy and the challenge of new information and communication technologies. *The Communication Review, 7*(1), 3–14.

Okeshola, F. B., & Adeta, A. K. (2022). Internet fraud in Nigeria: Patterns, causes, and consequences for young people. *International Journal of Cyber Criminology, 16*(1), 185–201.

Okunola, S. A., & Adesina, O. S. (2021). Patterns of social media usage and exposure to cybercrime among undergraduates in Nigeria. *International Journal of Cyber Criminology, 15*(2), 480–497.

Olatunji, O. (2022). Social media use and online safety practices among Nigerian undergraduates. *African Journal of Information and Communication, 27*(1), 65–82.

Potter, W. J. (2013). *Media literacy* (7th ed.). Sage Publications.

Ruggiero, T. E. (2000). Uses and gratifications theory in the 21st century. *Mass Communication & Society, 3*(1), 3–37.

Statista. (2023). *Most popular social media platforms in Nigeria as of 2023*. Retrieved from https://www.statista.com

Tandoc, E. C., & Maitra, J. (2022). Digital literacy and resilience against misinformation: A critical review. *Journalism, 23*(5), 1125–1142.

Ulo, E. (2025). Mediated realities and internet fraud among juveniles in Nigeria. *Journal of Social Theory and Research, 4*(2), 303–311

Urien, J. (2025). Cognitive dissonance and cyber-fraud behaviour among university students in Nigeria. *ESUT Journal of Social Sciences, 10*(1). ESUT Journal of Social Sciences.