

From Clicks to Caution: Informal Learning Experiences of Undergraduates in Obafemi Awolowo University Concerning Internet Fraud

BABALOLA Adejoke Clara (Ph.D)

Department of Adult Education and Lifelong Learning Faculty of Education
Obafemi Awolowo University, Ile-Ife, Osun State, Nigeria

DOI: <https://doi.org/10.51244/IJRSI.2026.1308000235>

Received: 30 August 2026; Accepted: 04 September 2026; Published: 17 September 2026

ABSTRACT

This research identified the types of internet fraud among undergraduate students at Obafemi Awolowo University; it examined the perceived reasons why undergraduate students at Obafemi Awolowo University participate in internet fraud; determined the informal learning experiences and coping strategies of undergraduate students at Obafemi Awolowo University concerning internet fraud. A case study research design was adopted for this study and twenty undergraduate students were selected from Obafemi Awolowo University using convenient sampling technique. An in-depth interview guide was used to collect data. Data were analysed using interpretive content analysis. The results showed that catfishing and Ponzi schemes among others schemes were the most common types of internet fraud amongst undergraduate students in Obafemi Awolowo University. Unsuspecting undergraduate students were scammed primarily through social media platforms like WhatsApp and Facebook. Additionally, some experienced scams related to fake investment platforms and fake online vendors. As a coping strategy, undergraduates have learned to verify the legitimacy of online offers and investments, avoiding impulsive decisions driven by peer pressure or enticing promises. Participants not only learned from personal experiences but also from observing the experiences of peers and family members. This study therefore emphasized the importance of safeguarding personal information, avoiding sharing sensitive details online, among others which were largely responsible for falling victims of fraudulent activities.

Keywords: Cyber Fraud, Online Scams, Social Media Platforms, Personal Experiences, Fraudulent Schemes

INTRODUCTION

With the growth of the internet and digital technologies, communication, learning, business, and social interaction have changed significantly. However, this growth has also increased the ability and opportunities for cybercrime, including internet fraud. Online fraud is the process of inducing someone or an organization to release financial or other assets for fraudulent purposes using the internet and internet-enabled technologies (Akinbowale et al., 2024). It occurs via email, social media, websites, messaging apps, telephone, and other digital channels, including phishing, impersonation, social engineering, identity theft, advance-fee fraud, and online shopping and investment fraud, among others (Akinbowale et al., 2024; Balogun et al., 2024). Thus, internet fraud is increasingly becoming a social, economic, and educational problem.

Fraud on the internet is more prevalent in Nigeria among the youths, including students at the tertiary institutions. Students use digital technologies for researching and learning, communicating with friends and family, financial planning and recreational activities. During the process, they may be targets of online fraud and can be perpetrators of online fraud. This has caused worry to educational institutions, families, communities, law enforcement and the policy makers (Balogun et al., 2024; Eke et al., 2024; Ukam, 2024).

Access to technology, however, is not a standalone determinant of participation. Studies have identified several factors associated with students' involvement, including financial problems, lack of economic opportunities,

peer influence, family background, material aspirations, and attraction to quick financial returns (Arogundade & Aderibigbe, 2020; Akinbowale et al., 2024; Balogun et al., 2024). Peer networks can also promote dishonest behaviour, while online environments can foster perceptions of low risk and a lack of accountability. An understanding of the phenomenon also needs to be matched by awareness of the modalities of fraud and how they are acquired and applied. Phishing, fake job or scholarship postings, false online shopping sites, investment fraud, impersonation, identity theft, and other types of online scams can be experienced by students. Some experience them as victims, while others witness them, learn about them, or engage in them through their social and online lives. Therefore, it is crucial to analyse these forms of internet fraud in order to identify the motivations, experiences, risks, and responses associated with internet fraud among university students.

There is an educational dimension to internet fraud, in addition to its criminal and technological dimensions. Learning knowledge, skills, attitudes and behaviours is not restricted to the formal educational system, but also occurs in everyday life, social interaction, observation, exposure to the media and engagement with social networks (Smith 2026). Informal learning is unstructured and spontaneous, and takes place when people engage in their daily activities and interactions (Combs as cited in Merriam, Caffarella, & Baumgartner, 2007). Merriam et al. (2007) describe three categories of learning, based on this: self-directed learning, incidental learning, and socialisation or tacit learning. These forms are applicable to internet fraud, as students may purposefully seek information relating to fraudulent practices, acquire unintentional knowledge about fraud through their experiences, and learn about fraud by observing and interacting with others. Such learning can enable students to engage in fraudulent activities or assist them in protecting themselves and avoiding victimisation.

There should also be a consideration of the students' reactions to internet fraud. Individuals who learn that they have been involved in, or affected by, fraud might be able to cope with the situation, in ways such as seeking help, reporting the incident, making the web safer, avoiding untrustworthy sites, or, not doing risky activities. These can be understood in conjunction with students' informal learning experiences in their everyday lives, providing insights into their understanding, their navigation and their reactions to internet fraud.

The informal learning approach has been given little attention in the context of the phenomenon of internet fraud among the Nigerian youths and university students; however, there is increasing concern about their involvement in engaging in such fraud. While the current debates have primarily centred on prevalence, causes, socio-economic consequences, and prevention, there has been less emphasis on how young people learn about internet fraud in their daily lives and social relations and how this learning affects their responses to internet fraud. This is an important gap because interventions that are mainly formal in nature may not address the informal contexts in which students are exposed to, understand, and react to internet fraud.

In this context, this study aimed to explore the nature of internet fraud among students of Obafemi Awolowo University (OAU), their informal learning experiences and coping mechanisms within the university, and the reasons for their participation. The study seeks to integrate these dimensions by viewing internet fraud not only as a technological and criminal issue but also as a social and educational phenomenon, in which learners' daily interactions, experiences, and learning contexts form the basis for the development and understanding of such forms of fraud. The study, therefore, set out to answer the following questions:

- i. What are the types of internet fraud among undergraduate students at Obafemi Awolowo University?
- ii. What are the perceived reasons why undergraduate students at Obafemi Awolowo University participate in internet fraud?
- iii. What are the informal learning experiences and coping strategies of undergraduate students at Obafemi Awolowo University concerning internet fraud?

THEORETICAL FRAMEWORK

The study is based on Social Learning Theory and Informal Learning Theory. Social Learning Theory helps

to elucidate the process of acquiring behaviour through observation, imitation, and social interaction, and Informal Learning Theory helps to explain the process of acquiring knowledge, skills, and attitudes through everyday experiences away from the formal educational system. The theories can be used together to explain the relationship among student involvement, learning about fraudulent practices, and responding to them in the context of Internet frauds.

Social Learning Theory

Social Learning Theory (Bandura, 1977) suggests that people learn behaviours from other people, by acting with them and observing the outcomes of what they do. Rewards, social models, and direct experience are thus modulating behaviours.

The theory applies to this study because students can be exposed to internet fraud if they use peers who commit, talk about, or model Internet fraud. The findings demonstrated that peer pressure, social validation, impressing others, and quick money are sources of social influence and perceived reward that might influence behaviour. Students can also get to know of fraudulent practices through watching peers, hearing from others, or seeing fraud on social media, betting, investment sites, and online vendors. Social Learning Theory thus elucidates the social influences, observation, perceived rewards and behavioural reinforcement factors that could help explain how students are involved in and understand Internet fraud.

Informal Learning Theory

Informal Learning Theory is based on learning that takes place in familiar situations, activities and interactions that are not part of formal learning (Marsick and Watkins, 2001). It is especially pertinent in the context of this study as students are exposed to Internet fraud mostly in the course of their daily interactions with the Internet and social media.

Scams shared via friends and interactions on platforms like WhatsApp, Facebook, betting and investment platforms were reported as means of learning about scams. These experiences will build students' knowledge and understanding of fraudulent practices and help to guide their responses. The strategies reported, like blocking suspicious contacts, protecting personal information, verifying information, avoiding suspicious links and using anti-virus software, are strategies acquired in the day-to-day world. Informal Learning Theory, therefore, helps to understand how students learn about Internet fraud and their awareness and coping strategies, both pro- and anti-fraud, in their life experiences.

The theories discuss various but related aspects of the study. Social Learning Theory is the theory involved in how social interaction and observation affect behaviour, whereas Informal Learning Theory is the theory involved in how everyday experiences help the acquisition of knowledge and the practical strategies it provides.

The combined use of these allows the study to explore internet fraud not only as a social phenomenon, but also a learning phenomenon. Social Learning Theory helps to understand students' engagement and the role of peers and perceived rewards, and Informal Learning Theory helps to understand their informal learning experience, awareness and coping. As a whole group, they offer a unified perspective on how pupils experience, learn about, and react to online crime.

METHODOLOGY

This study employed a qualitative research design, and the descriptive case study research design was used to provide information on the informal learning experiences of undergraduate students at Obafemi Awolowo University concerning internet fraud. The population for this study consists of undergraduate students of Obafemi Awolowo University, Ile-Ife, Osun State. The sample for the study comprises 20 undergraduate students. Convenient sampling technique was used to select participants who were frequent users of the

internet, who had spent at least one full academic session in Obafemi Awolowo University, and were available to grant the interview. For the purpose of this research, the participants were tagged as R1 to R20.

The interview guide named “Informal Learning Experiences of Undergraduate Students in Obafemi Awolowo University Concerning Internet Fraud” was used to gather information for the study. Each interview lasted for 10–15 minutes and was tape-recorded. At the commencement of the interview, the researcher explained the purpose of the research to each of the participants and oral consent was obtained from each of them before the interview was conducted. Their willingness to participate voluntarily in the study was also considered during the selection process. The interviews were conducted in English and were later transcribed.

To ensure the credibility and reliability of the findings, the interview recordings were carefully transcribed to maintain the accuracy of participants’ responses, and participants were selected based on their direct experience with internet fraud as undergraduate students in Obafemi Awolowo University to ensure the relevance of the data collected. Consistent interview procedures were followed across all participants to ensure the dependability of the findings of participants’ informal experiences as undergraduate students in Obafemi Awolowo University.

Ethical principles were observed throughout the study. Participation in the study was voluntary, and informed consent was obtained from all participants before conducting the interviews. Participants were assured of confidentiality and anonymity, and their responses were used strictly for academic purposes. In addition, participants were informed of their right to withdraw from the study at any stage without any penalty. The method of data analysis was content analysis, which involved coding and classification of verbal or behavioural data for the purpose of summarisation and tabulation. The responses were analysed according to the informal learning experiences, reasons for participation in internet fraud, types of internet fraud, and coping strategies reported by the participants.

RESULTS AND DISCUSSION

In this section, data collected through interviews, their interpretation, and discussion are presented.

Demographic Details of Participants

Table 1: Profile of Undergraduates of Obafemi Awolowo University

NAME	GENDER	DEPARTMENT	FACULTY	LEVEL
R1	Female	Biochemistry	Basic Medical Science	300
R2	Male	Geography	Social Science	400
R3	Female	Public Administration	Administration	400
R4	Male	Sociology	Social Science	200
R5	Female	English	Arts	300
R6	Female	Microbiology	Basic Medical Science	300
R7	Female	Mechanical Engineering	Technology	200
R8	Male	Economics	Social Science	300
R9	Male	Accounting	Administration	400

R10	Female	Pharmacy	Pharmacy	300
R11	Male	Nursing	Basic Medical Science	500
R12	Male	Dramatic Arts	Arts	300
R13	Male	Botany	Science	400
R14	Male	English Education	Education	300
R15	Male	English Education	Education	400
R16	Male	Pharmacy	Pharmacy	400
R17	Male	Chemistry	Science	300
R18	Male	English	Arts	300
R19	Male	Law	Law	400
R20	Male	Law	Law	300

The study involved twenty (20) undergraduate students of Obafemi Awolowo University, Ile-Ife. The participants comprised fourteen males and six females. The participants were drawn from different departments, faculties and levels of study, thereby providing experiences from a range of academic backgrounds.

For this study, the participants were undergraduate students who had spent at least one full academic session in Obafemi Awolowo University and were available to participate in the interviews. The participants were identified as R1 to R20 to protect their identities. The participation of fourteen males and six females suggests that more male participants were available and willing to discuss issues relating to internet fraud. However, this does not imply that female undergraduate students lack experiences relating to internet fraud.

Research Question One: What are the types of internet fraud common among undergraduate students at Obafemi Awolowo University?

Table 2: Types of Internet Fraud Common Among Undergraduate Students at Obafemi Awolowo University

Theme	Participants	Codes/Interview Responses
Theme 1: Catfishing (Yahoo Yahoo)	R8, R9, R20	R8: "Under catfishing we have like plenty types, like you impersonate someone, act as someone where they use other people's profile to exploit people online and get things from them." R9: "I think the common one as regards Internet fraud that I know is yahoo yahoo (catfishing)." R20: "Catfishing has been one of the most popular types of fraud out there because almost everybody knows what 'yahoo yahoo' means."
Theme 2: Ponzi Scheme	R14, R18	R14: "Also Ponzi scheme is also among; you know how they pay you with the investment of another as your profit. I have been scammed before so I know. You just get up one day and you realize that the site is gone with your money." R18: "I think the common ones that I know

		is yahoo yahoo (catfishing) and I think Ponzi schemes and all these bank hacking frauds.”
Theme 3: Impersonation	R11, R12, R17	R11: “My experience around it isn't that much but I know that most of the internet fraud has to do with impersonating someone using that random picture to extort from other people.” R12: “I encountered one personally. I was scammed by someone on Facebook who I thought was a girl not knowing the person was an impersonator and I keep sending money to a fake girl because of love.” R17: “I don't engage in it...but the popular one I am familiar with has to do with impersonating another person to deceive people online and exploit them.”
Theme 4: Online Vendor Scams	R2	R2: “...those who pretend as online vendors. They get scammed by buying their product and not getting it and you send the money to them.”
Theme 5: Fake Investment Platforms	R5	R5: “Internet fraud among undergraduate students is not a new thing to me. Scamming people online, dating scams, fake online investment platforms are the types of internet fraud I know.”
Theme 6: Hacking/Bank Hacking Fraud	R7, R15, R18	R7: “I don't know the general term they use for it but that of the BVN, and also sending you links online and asking you to click on the links to get a greater amount for them to be able to access your personal details. Mostly bank frauds.” R15: “And also hacking, fraudsters hack into government website or banking systems and steal money.” R18: Also identified bank hacking fraud among the common types of internet fraud.
Theme 7: Dating Scams	R10, R13, R19	R10: “Internet fraud to me is using different scam formats to extort money from people especially the white folks like dating scams. I have seen undergraduate students engage in it. I have seen how someone I know used a celebrity picture to collect more than \$200 from a client so he claimed.” R13: “Dating scams where you date people online in order to defraud them.” R19: Similarly identified dating scams as a form of internet fraud.

Source: Field interview data

Table 2 indicates that undergraduate students of Obafemi Awolowo University knew various types of internet fraud, with subthemes emerging from catfishing (Yahoo Yahoo), Ponzi schemes, impersonation, online vendor scams, fake investment platforms, hacking/bank fraud, and dating scams. The results suggest that there are social and financial aspects of online fraud and that undergraduate students are exposed to knowledge of this fraud through their social and daily online experiences.

The most well-known was Catfishing/Yahoo Yahoo. R8, R9 and R20 linked it to false identification and exploitation of an individual. R11, R12 and R17 also reported impersonation, R12 recounted a personal experience of being impersonated on Facebook. The results support the Social Learning Theory, which proposes that students acquire knowledge of these fraudulent practices by observing, interacting with, and hearing others discuss them. They also endorse the informal learning theory as students learn about identity-based fraud in their daily interactions with social media and other websites.

Dating scams, reported by R10, R13, and R19, were a type of fraud where victims were frequently asked for funds in a romance. This is related to catfishing and impersonation, as fake identities could be utilised to create emotional connections and to trick a victim. In the context of Social Learning Theory, students can learn to

identify these practices by watching the experiences of others and disseminating information to social networks. An Informal Learning Theory suggests that these experiences will give students first-hand knowledge of the nature of a dating scam and how it can be handled.

The economic aspect of internet fraud was demonstrated in the Ponzi schemes and fake investment platforms. R14 said that he had lost money on a fake investment platform, R18 said he lost money due to a Ponzi scheme, and R5 was scammed from a fake investment platform. The implications of these findings are related to the Social Learning Theory, where incentives for engaging in fraudulent activities appear to be perceived as such and drive behaviour, and students may learn about such activities through peers and social networks. In addition, they have personal experiences of fraud on the investment market, which are informal learning experiences that allow them to gain knowledge about financial fraud.

The other types of fraud that were reported less frequently were: Online vendor scams (R2) – where money was sent for items that were never received; Hacking/bank fraud (R7, R15 and R18) – fraudulent links or revealing personal or banking information. The results also provide evidence of the power of informal learning since undergraduate students' experience of online transactions, dubious links and requests for personal details can give them concrete knowledge about how to identify and prevent fraudulent activities.

Research Question Two: ii. What are the perceived reasons why undergraduate students at Obafemi Awolowo University participate in internet fraud?

Table 3: Perceived Reasons Why Undergraduate Students Engage in Internet Fraud at Obafemi Awolowo University.

Theme	Participants	Codes/Interview Responses
Theme 1: Pressure from Friends and Families	R7, R5, R6	R7: "Some do it because of peer pressure. Like my friend is doing it, I want to do it." R5: "Mostly due to economy pressure from their fellow guys seeing their fellow guys spend money and we ladies at times cause that type of things." R6: "As we know in this kind of society, the males are expected to do more to provide food on the table and more of things like that. So, they try to look for how to get sources to get money, whether it is possible legal or illegal. Even though in school, some of them are not fathers too, but they find it like a responsibility for them to be ahead and look for a means which they try fraud."
Theme 2: Quick Money	R3, R18	R3: "So people don't really have the choice, let me say. So, they resort to those kinds of things to get easy and quick money." R18: "Some undergraduate students may engage in it to make quick money because to them, that is the fastest way to make money and survive."
Theme 3: Financial Support	R7, R4, R8, R16	R7: "Most of these guys that are going to internet fraud, they do it to earn money basically for financial assistance or financial backup in school." R4: "Some participate to take care of themselves; some participate to sponsor themselves." R8: "Most times, it's usually about money and trying to make ends means." R16: "And sometimes in other cases, some undergraduate students engaged in fraud to support themselves in school but I don't endorse it."
Theme 4: Impression and Validation	R12, R11, R4	R12: "They want to acquire a lot of money and impress others, date the best girls on campus." R11: "While some were into it to get more validated by ladies or guys." R4: "Some are to show off."

Theme 5: Set Standards	R18, R8, R19	R18: "Also I think some people also do fraud to make some money and reach a certain standard they set for themselves; you know for example, some want to be riding a car and spending big every week so that's it." R8: "It's usually about money and trying to reach their own standards." R19: "Some do it to get luxurious lifestyles they cannot get through their income from parents thereby setting some standards they want to meet."
Theme 6: Lack of Contentment	R15, R8	R15: "Generally speaking, many undergraduate students are into fraud because they lack contentment and they are not satisfied with the money they are collecting at home, they want more and they are ready to go the illegal way to acquire it." R8: "And greed is part of it. Some people don't actually need it because they want to be more than what they are supposed to be."
Theme 7: Fun	R8, R4	R8: "Some do it for fun. I have heard people doing it for fun." R4: "Some just do it for fun."
Theme 8: Economic Situation of the Country	R2, R19, R3	R2: "It's the situation of the country now. Everybody needs money. So, undergraduate students always find ways to get money by all costs. So that's one of the reasons." R19: "Many reasons, the state of the nation is not encouraging, and the economy of Nigeria is bad, which in turn affects the financial status of undergraduate students from middle or low backgrounds." R3: "I found most of them on the issue of money, unemployment and stuff like that. So, undergraduate students don't really have the choice."

Source: Field interview data

Table 3 shows that undergraduate students indulge in internet fraud for economic, social, and personal reasons. The subthemes that arose were peer pressure, family pressure, need for quick cash, financial support, impression and validation, social standard, lack of contentment, fun, and the overall economic situation of the country. Based on these findings, it is submitted that there is a multi-factorial relationship among financial pressures, social influences, and personal motivations in shaping undergraduate students' involvement in internet fraud.

Financial need and economic pressure were the most salient explanations. Participants reported that fraud was committed to obtain personal needs, financial independence, or support studies (R4, R7, R8, R16). This behaviour was also seen to be reinforced by the challenging economic climate in the country, especially amongst learners from the lower income groups (R2, R3, R19). The respondents indicated that internet fraud could be seen by some undergraduate students as a shortcut to financial requirements ("easy, rapid money"). These results show economic motivations, whereas Social Learning Theory helps to predict how these motivations can be strengthened when students see those around them being rewarded financially for engaging in fraudulent practices. When the desired results of fraud manifest, the behaviour may be observed, and its rewards can promote the continuation of that behaviour and stimulate positive attitudes toward it.

The findings also reflect a significant social aspect, such as peer pressure, social expectations, and a need for recognition. Students can be swayed by peers engaging in fraud and the fact that they look wealthy and successful (R5, R6, R7). R4, R11, R12, R18, and R19 said that some of their motives included impressing others, gaining validation, meeting social standards, and maintaining luxurious lifestyles. These results directly corroborate the Social Learning Theory, which focuses on the importance of observation, social models, perceived reinforcement, and rewards on behaviour. Students can witness others who are committing fraud, and may link the action to money, status, or social recognition, which may increase the chances that they will develop similar attitudes and behaviours.

The results also indicate the possibility that the understanding and attitude of the undergraduate students may take shape from the informal interaction and experience which occurs in their daily lives. Informal learning experiences may occur during peer discussions, when undergraduate students have opportunities to observe lifestyles linked with fraudulent activities, and when undergraduate students learn stories about financial success. This helps to support Informal Learning Theory, which describes how knowledge, attitudes, and understandings of behaviours can be acquired outside of formal learning contexts, as a result of everyday interactions and experiences.

Also, personal motivations were identified, such as lack of contentment (R4), greed (R8), and involvement in fraud for fun (R15). The results suggest that economic hardship is not the only reason for engaging in internet fraud. However, other values and expectations can combine with personal desires and intentions. In the context of SLT, observed behaviours that lead to desirable outcomes have the potential to be reinforced, and in the context of ILT, repeated exposure to a practice or story of fraud in the normal environment surrounding the learner has the potential to foster the development of attitudes that enable and/or normalise that behaviour.

Research Question Three: What are the informal learning experiences and coping strategies of undergraduate students at Obafemi Awolowo University concerning internet fraud?

Table 4: Theme 3: Informal Learning Experiences

Subthemes	Participants	Codes/Interview Responses
Experience 1: Betting and Social Media Scams	R1, R10, R2	R1: “We got a message from one number that we don’t know; they were like okay, do you have a Sporty Bet account if you don’t have can you open the account. It is a betting platform so what they want you to do is you fund your betting account with your ATM card, after funding it they will give you a link to one website. You will then fill in your details, it felt so real actually because it was something one could easily fall into since you’re like currently broke and all that, so I was like this thing is too good to be true.” R10: “I was sent a message on WhatsApp for an irresistible offer to earn free money. All I needed to do was to fill my details (phone number and password of my Sporty Bet account) to the site the scammer sent me and submit and be awaiting payment. I don't know the site had hidden keylogger that can capture my account details and send it to the scammer. I almost submitted my details on the site... I left the site immediately that day and confronted the guy. He blocked me when he knew that I had known.” R2: “Someone on WhatsApp promised to double my money in my betting account, so I paid for it and nothing happened. The person I paid to blocked my number and I could not reach the person anywhere, that’s when I knew I got scammed.”
Experience 2: Fake Investment Platforms	R4, R5, R14	R4: “The name is News Payer. When I joined OAU, I guess when I was just becoming a student, I can't remember the year, I invested a little bit, planning to reap returns after a month, but I didn’t see any money they were just pressuring me to refer people.” R5: “There was this time, I decided to do a little investment into this Rackstarly stuff, It was really popular at that time I invested 40k, but I couldn't get my money back.” R14: “It was a post on Facebook. I thought the investment was legit and I was carried away. The scammer used the account of one of my friends to make the post so I thought it was my friend unknowingly to me that his account has been hacked. I was promised quick returns on my

		investment in few hours. I sent the money and it was after a while I knew I have been scammed when I didn't get any response again.”
Experience 3: Online Vendor and Giveaway Scams	R6, R1	R6: “I have a friend who has an experience. She sells skincare products from Oriflame. And then she met a link online. She was like, it's Oriflame, everybody does Oriflame. So, she ordered the products, close to two hundred thousand naira. they brought a wrong product for hers... it was not even the products she ordered for because it came with a very funny spelling.” R1: “I was told that I won a phone like that online and that I should pay shipping fee to Ife. That shipping fee was 5K. So, I was like, if the shipping fee is 5K, pay the 5K. When you give me the phone, I'll give you the 5K. Because they don't have an office address. It was just one person that was running it, so I told the person I was not interested.”
Experience 4: Bank Fraud and Impersonation	R8, R3	R8: “There was a case where someone told me he was scammed. A bank personnel member called the person and told him that something was wrong with his account and that he would help him to resolve it. He asked for the details of the account like account number, the numbers on the ATM, CVV, and the pin to their ATM. So, when the person sent it, he took all his money and he had to go to the bank to change the card or block the account.” R3: “My friend has been called more than once. Somebody called her and told her that her brother needed money. Then she had to go to a POS stand and then she transferred money to the person. Then she tried calling the number afterwards, but she was blocked.”

Table 4 reveals that the undergraduate students' learning about internet fraud mainly comes from experience and understanding of online fraud. Betting and social media scams, fake investment platforms, online vendor and giveaway scams, and bank fraud and impersonation were four big experiences. The fraudulent betting offers and unrealistic investment returns, fake vendors, giveaways, and requests for banking information were reported as issues. Students became familiar with common indicators such as strange links, unrealistic promises, requests for personal information, and unverifiable identities.

The results validate Informal Learning Theory because knowledge about internet fraud is acquired from "real world" experiences outside of the classroom. Undergraduate students learn through direct experience with scams, near victimisation, and exposure to fraudulent activities about how scams work and how they can be detected. undergraduate students do not learn most of this knowledge from a formal class, but from experiences they have in interacting with the social media, betting platforms, investment platforms and online marketplaces.

The findings also indicate the theory of social learning, especially as undergraduate students are learning indirectly from the experiences of their peers or other people. Undergraduate students can receive information on scams, signs of scams, and potential fallout from scams through the experiences of others who have been victims of a scam. Undergraduate students can thus learn information observed and socially gained that can affect their perception and reaction to similar situations.

The warning signs reported, like suspicious links, promises to wishes, requests for sensitive data, unconfirmed identities, and so on, are further evidence of the practical character of this learning. Repeated exposures, personal experiences, and information within undergraduate students' social networks can lead to the development of the ability to identify these indicators. In this context, the incidents a student might experience in everyday life are learning experiences, allowing him/her to become aware and to learn to fend for himself/herself against fraud.

Table 5: Theme 4: Coping Strategies

Subtheme	Participants	Codes/Interview Responses
1. Contentment and Avoidance of Quick Wealth	R1, R18	R1: “Well, I have always tried to guide my heart diligently like the Bible says against quick wealth. I am contented with what my parents give me and I know the kind of people I move with.” R18: “I’m not carried away and I’m contented with what I have through my legitimate source or hustle.”
2. Blocking Strange Numbers	R1	R1: “Once I see strange numbers these days, and I see that the messages that they are sending are like a broadcast message I would just block them immediately because the moment you start reading, you start thinking that it might be true.”
3. Safeguarding Devices and Passwords	R4, R18	R4: “For me, I don’t share my things, my password, I do safeguard my laptop with pins and patterns. I also have multiple security on my phone.” R18: “I password anything that needs to be passworded, I don’t engage in anything that looks like scam.”
4. Protecting Personal and Financial Information	R5, R17	R5: “I don’t share my data on other people’s systems. I don’t log in to my Gmail account on another person’s system.” R17: “I believe people should stand on their guard always when they are online doing things. Don’t go into much conversation with strangers and don’t send any codes from your phone to anybody online.”
5. Installing Antivirus Software	R6, R7	R6: “First thing I do is, in any of my devices, I install antivirus because that is one way you could get your information. Also, I try to check up the links and gather enough information. I don’t do anything that doesn’t have a sole name, something that I can trace you to.” R7: “...install antivirus on your system. Because all these links that they use for fraud, they are always a corrupt one. And also, I guess that there are some links that each link has HTTP... So, if some links don’t have S, that means it’s not security conscious or something. So don’t just click on any links.”
6. Verifying Information and Links	R9, R6	R9: “I don’t believe anything if it’s not coming directly from the original source. For example, I would reach out to my bank first to confirm if the information is from the bank.” R6: Similarly, we should emphasise the importance of obtaining information from direct and reliable sources.
7. Keeping Away from Known Fraudsters	R15	R15: “I can’t fall victim to them because I have always kept a distance from whoever I know that is into internet fraud or yahoo. Don’t say because they are your friends, they can’t defraud you.”

Source: Field interview data

Undergraduate students use different strategies to safeguard themselves against internet fraud as indicated in Table 5. These include being satisfied with what they have, not seeking easy money, blocking strangers, securing devices and passwords, safeguarding personal and financial data, installing antimalware, checking

information and links, and avoiding fraudsters. These are both personal precautions and the application of simple technological protections.

The results of this research strongly support the Informal Learning Theory, since many of the protective strategies seem to be based on undergraduate students' practical experience with risks on the internet, acquired through informal learning. Students' ability to check information, be wary of suspicious links, ensure that their passwords and personal details are kept safe, and recognise suspicious contacts shows that their knowledge could be developed through direct experience from near victimisation and witnessing others' experiences. This type of learning takes place outside the formal education system, and derives from student's daily digital interactions.

The results are also applicable to Social Learning Theory as it can be used to explain how protective behaviours can be learned by watching and communicating with others. Peer information regarding fraudulent activities, experiences of those who have been scammed, and observation of how other undergraduate students protect themselves can impact their own behaviours to potential online risks. Undergraduates can learn behaviours, such as blocking suspicious contacts, checking the information, avoiding anyone they know to be a fraudster, and so on, through observation and social interaction.

The approach of not seeking instant gain and remaining satisfied also demonstrates the impact students' perceptions and socialisation have had on their reactions to fraud. This implies that individuals' attitudes and behavioural practices regarding financial opportunities and risks can be as effective as technological measures in preventing the occurrence of internet fraud. The idea of using antivirus software, secure passwords, and safeguarding personal and financial information are also an example of how practical digital knowledge is used to minimise exposure to online threats.

DISCUSSION OF FINDINGS

This study selected twenty (20) undergraduate students of Obafemi Awolowo University, Ile-Ife, using convenient sampling technique. Only six females agreed to participate in the study. Therefore, we have more males than females as participants. This may be why Adewumi and Tella (2018) opined that male undergraduates were more prone to cybercrime than their female counterparts. However, this study cannot draw the same conclusion as undergraduate female students may not be interested in sharing their experiences about internet fraud.

Concerning the types of internet fraud among undergraduate students at Obafemi Awolowo University. Findings showed that undergraduate students of Obafemi Awolowo University knew various types of internet fraud, with subthemes emerging from catfishing (Yahoo Yahoo), Ponzi schemes, impersonation, online vendor scams, fake investment platforms, hacking/bank fraud, and dating scams. The results suggest that there are social and financial aspects of online fraud and that undergraduate students are exposed to knowledge of this fraud through their social and daily online experiences. This is in line with the findings of other authors who defined internet fraud, in context and types, as any fraudulent or deceptive activity that takes place on the Internet. It typically involves the use of email, social media, websites, or other online platforms to deceive or scam individuals or organizations for financial gain (Halder & Jaishankar, 2012). Common types of internet fraud include phishing, identity theft, advance-fee fraud (419 scams), online shopping scams, investment scams, and romance scams (Furnell, 2019). The overall results show that internet fraud is a multifaceted phenomenon that can be characterised as a situation of fraudulent investment, identity deception, financial or information theft, fraudulent commerce and emotional manipulation of students. These forms overlap, and scammers might have several tactics in one fraudulent activity. From the perspective of Social Learning Theory, the awareness and potential participation of students in internet fraud can be explained in terms of social interaction, observation, modelling, perceived rewards and reinforcement. Informal Learning Theory, on the other hand, is the learning that occurs through students' experiences with social media and other digital platforms in the real world.

On the reason why undergraduate students in Obafemi Awolowo University participate in internet fraud, findings shows that undergraduate students indulge in internet fraud for economic, social, and personal reasons. The subthemes that arose were peer pressure, family pressure, need for quick cash, financial support, impression and validation, social standard, lack of contentment, fun, and the overall poor economic situation of the country. Based on these findings, it is submitted that there is a multi-factorial relationship between financial pressures, social influences, and personal motivations in shaping students' involvement in internet fraud. In the same vein, Agbele, Adagunodo, & Aluko, (2018) identified the reason why some students are involved in internet fraud in Nigeria as the lure of quick and easy money. They identified several factors contributing to students' involvement in internet fraud to include peer pressure, financial needs, family background, and the desire for quick wealth (Agbele et al., 2018; Arogundade & Aderibigbe, 2020).

In general, the results showed that the factors causing students to engage in internet crimes were economic pressure, peer pressure, social pressure, and perceived benefits, and personal aspirations. While economic hardship seems to be a key motivation, the results indicate that internet fraud can also serve as a way to achieve social recognition, material status, and lifestyles felt desirable. Social Learning Theory thus offers a good account of how peer influence, observation, modelling, perceived rewards and social reinforcement can influence students' involvement in internet fraud, and Informal Learning Theory offers an account of how attitudes and understandings of fraud can be formed in students' everyday social and digital lives.

An attempt to document the informal learning experiences of undergraduates at Obafemi Awolowo University concerning internet fraud reveals that the students' learning about internet fraud mainly comes from experience and understanding of online fraud. Betting and social media scams, fake investment platforms, online vendor and giveaway scams, and bank fraud and impersonation were four big experiences. The fraudulent betting offers and unrealistic investment returns, fake vendors, giveaways, and requests for banking information were reported as issues. Students became familiar with common indicators such as strange links, unrealistic promises, requests for personal information, and unverifiable identities. Methods employed by fraudsters include the use of fake websites, malicious software (malware), social engineering, and impersonation (Griffith, C. E., Tetzlaff-Bemiller, M & Hunter, L. Y., 2023; Halder & Jaishankar, 2012).

The results show overall that student comprehension of internet fraud is built upon experiences and peer learning. Practical knowledge can be gained from personal encounters, near-victimisation, and through the experiences of friends, which are not necessarily learned in school. The informal Learning Theory, then, accounts for the acquisition of knowledge and coping strategies from daily experiences better than Social Learning Theory accounts for knowledge acquired through observation and interaction with peers. These theories demonstrate that student knowledge of internet fraud is acquired not just from formal, but also from informal, environments in which they exist, socially and digitally.

Findings also showed that undergraduate students in Obafemi Awolowo University use different coping strategies to safeguard themselves against internet fraud. These include being satisfied with what they have, not seeking easy money, blocking strangers, securing devices and passwords, safeguarding personal and financial data, installing antimalware, checking information and links, and avoiding fraudsters. These are both personal precautions and the application of simple technological protections.

Some authors have also recommended that training individuals to recognize phishing attempts, secure personal information, and practice safe online behavior contributes to reducing vulnerability. Moreover, international collaboration among law enforcement agencies, financial institutions, and tech companies is essential for tracking and apprehending fraudsters operating across borders (Kshetri, 2018).

The overall results suggest that undergraduate students react to internet fraud by using a mix of behaviour awareness, information verification and digital security practices. Informal Learning Theory is more convincing in explaining the process of students acquiring the practical knowledge and coping skills needed to identify and prevent online dangers in the context of everyday life. Social Learning theory extends this explanation by demonstrating that protective behaviours can also be learned by watching others and

interacting with peers. The theories show that students' reactions to internet fraud are influenced by what they learn from their daily life online and from their social surroundings.

SUMMARY OF FINDINGS

The findings indicate that undergraduate students' informal learning concerning internet fraud occurred largely through personal experiences, second-hand experiences, peer interactions and exposure to fraudulent activities on social media and other online platforms. The participants learned from being scammed, nearly being scammed, and observing friends or acquaintances who had been victims. The learning derived from these experiences included greater caution, verification of information, protection of personal and banking details, avoidance of suspicious links and platforms, and increased awareness of impersonation and fraudulent investment opportunities.

The coping strategies developed from these informal learning experiences included safeguarding devices, using passwords and antivirus software, blocking strange numbers, avoiding suspicious links and offers, verifying information with original sources, protecting personal and financial information, maintaining distance from known fraudsters, and being content with legitimate sources of income.

Overall, the findings suggest that internet fraud experiences served not only as negative experiences but also as sources of informal learning. Through these experiences, undergraduate students developed practical knowledge and behaviours that helped them become more cautious in their subsequent online activities.

LIMITATIONS OF THE STUDY

Findings are context-specific to Obafemi Awolowo University, Ile-Ife and may not be applicable to experiences in other universities with different socio-economic and cultural dynamics. Undergraduate students were impatient and were not willing to spend more than 15 minutes of engagement with them. The study relied on undergraduate students' accounts, which may be influenced by recall bias, exaggeration, or reluctance to disclose involvement in fraud fully. While rich in depth, the qualitative case study design limits the ability to generalise findings broadly. Some participants may have withheld critical details to avoid stigma, fear of judgment, or potential legal implications.

RECOMMENDATION

1. Universities should integrate cybersecurity awareness, digital literacy, and ethical online behaviour into general studies courses.
2. Counselling and peer-mentoring programs should be established to help undergraduate students resist peer pressure and cope with fraud-related stress.
3. University authorities should collaborate with ICT experts and law enforcement to create clear policies and workshops on internet safety.
4. The university authorities should organize periodic seminars, media campaigns, and interactive workshops to raise awareness of common fraud schemes among undergraduate students.
5. Future studies should expand sample size, include multiple universities, and employ mixed-method designs to strengthen generalizability.
6. Collaboration with telecoms, banks, and social media platforms can help develop targeted interventions and fraud-prevention tools for undergraduate students.

REFERENCES

1. Adewumi, A. O., & Tella, A. (2018). Prevalence of cybercrime among students of Obafemi Awolowo University, Ile-Ife, Nigeria. *International Journal of Research in Education and Sustainable Development*, 1(1), 1-10.

2. Agbele, K. K., Adagunodo, E. R., & Aluko, O. R. (2018). Cybercrime among Nigerian Youths: Causes, Consequences, and Remedies. *International Journal of Criminal Justice Sciences*, 13(2), 641-654.
3. Anaemena, I. C.¹, *Onyemaechi, C. I.², and Anaemena, C. E.³ (2025) Cybercrime and Nigerian Youth: A Growing Menace in the Digital Age. *Ojukwu Journal of Psychological Services*. 1(6), 1-15 <https://doi.org/10.5281/zenodo.17499287>
4. Akinbowale, O. E., Mashigo, M. P., & Zerihun, M. F. (2024). Understanding and mitigating cyberfraud in Africa. AVARSITY Books. <https://doi.org/10.4102/aosis.2024.BK485>
5. Arogundade, F. T., & Aderibigbe, S. A. (2020). Internet Fraud among Undergraduates in Nigerian Tertiary Institutions: A Case Study of Federal University of Technology, Akure. *Ilorin Journal of Social Science*, 18(2), 150-166.
6. Balogun, O. S., Akangbe, T. A., Fagbamila, O. D., & Aigbovbioisa, F. O. (2024). Internet users' perception of the prevalence of online investment fraud and victimisation in Nigeria. *Gusau Journal of Sociology*, 4(2), 169–181. <https://doi.org/10.57233/gujos.v4i2.13>
7. Bandura, A. (1977). *Social learning theory*. Englewood Cliffs, N.J.: Prentice Hall
8. Eke, C. (2024). Awareness And Perception of Internet Fraud Epidemics Among Nigerian Youths. *African Journal of Social and Behavioural Sciences* 14(3), 1370-1383. <https://www.researchgate.net/publication/382423788>
9. Furnell, S. (2003). Cybercrime: Vandalizing the Information Society. In: Lovelle, J.M.C., Rodríguez, B.M.G., Gayo, J.E.L., del Puerto Paule Ruiz, M., Aguilar, L.J. (eds) *Web Engineering. ICWE 2003. Lecture Notes in Computer Science*, vol 2722. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45068-8_2
10. Griffith, C. E., Tetzlaff-Bemiller, M & Hunter, L. Y., (2023) Understanding the cyber-victimization of young people: A test of routine activities theory. *Telematics and Informatics Reports*, (9) <https://doi.org/10.1016/j.teler.2023.100042>
11. Kshetri, N. (2018). The Role of Global Institutions in Addressing Cybercrime. *International Journal of Cyber Criminology*, 12(1), 1-25.
12. Marsick, V. J., & Watkins, K. E. (2001). Informal and incidental learning. *New Directions for Adult and Continuing Education*, (89), 25–34. <https://doi.org/10.1002/ace.5>
13. Merriam, S.B., Caffarella, R.S., & Baumgartner. (2007). *Learning in adulthood: A comprehensive guide* (3rd ed.). San Francisco, CA: Jossey-Bass.
14. Smith, M. K. (2026). 'What is pedagogy?', *The encyclopaedia of pedagogy and informal education*. <https://infed.org/dir/what-is-pedagogy/>. Retrieved: 01/09/2026
15. Ukam, P. I., Onuh, P. A., Nnaji, D. I., Egbo, E. I., & Ugwu, C. O. (2024). How engagement in internet fraud impact academic activities of undergraduate students in Nigeria: A socio-legal study. *Cogent Social Sciences*, 10(1). <https://doi.org/10.1080/23311886.2023.2280285>
16. Halder, D., & Jaishankar, K. (2012). *Cyber crime and the victimization of women: laws, rights and regulations*. Hershey, PA : Information Science Reference.