Influence of peer pressure and Social Media on Cybercrime Involvement among University Students in South-South Nigeria

Osugba Sylvester

Faculty of Social Science, Department of Sociology Delta State University Abraka Nigeria

Abstract:

This study explores the sociological drivers behind the trend, focusing on peer pressure and social media as dual enablers of cyber fraud among Nigerian university students. Anchored in Social Learning Theory, Differential Association Theory, and Strain Theory, the research examines how peer dynamics and online influence normalize fraudulent behaviors and facilitate their propagation within academic environments. Using a multistage sampling technique, data were collected from 300 students across three universities in South-South Nigeria. Quantitative data were analyzed using descriptive statistics and Pearson correlation matrices. Results indicate that peer influence significantly affects students' likelihood of engaging in cyber fraud, with 70% of respondents acknowledging peer pressure as a motivating factor. Additionally, social media platforms especially TikTok and Instagram were identified as major arenas for the glamorization and execution of cyber fraud schemes. A striking 71% of respondents reported exposure to fraudulent content online, and over 72% agreed that social media contributes to the normalization of cybercrime among their peers. The correlation analysis revealed that materialism is positively associated with cybercrime engagement (r = 0.58, p < 0.001), while social acceptance negatively correlates with both materialism and cybercrime. These findings underscore how students' desires for wealth, status, and peer validation can override ethical considerations. The study concludes that cyber fraud among university students is not merely a criminal issue but a sociological phenomenon rooted in evolving cultural values, peer validation mechanisms, and digital exposure. The study recommends a multidimensional intervention strategy encompassing digital literacy, peer-led ethical education, curriculum reform, and strengthened campus counseling services. Such initiatives are essential to counter the cultural and technological forces enabling cybercrime and to foster a value-based student culture in Nigeria's higher institutions.

Keywords: Cyber Crime, Peer Pressure, Fraud, Nigerian Universities, Nigeria

1. Introduction

In the digital age, cyber fraud has emerged as one of the most pressing security and social issues globally, particularly in developing countries like Nigeria. The widespread adoption of digital technologies, increased internet penetration, and the proliferation of social media platforms have created fertile ground for cybercriminal activities. Among the most active perpetrators of these cybercrimes are young people, especially university students. While cyber fraud is a multi-faceted phenomenon, peer pressure and social media have been identified as key sociological factors influencing the increasing participation of university students in Nigeria. This research seeks to critically examine the role of peer pressure and social media in promoting cyber fraud among this demographic. Cyber fraud, often referred to as "yahoo" in Nigerian popular parlance, involves the use of deceit, identity theft, phishing, and other manipulative digital strategies to defraud individuals or organizations, primarily for financial gain. Over the past decade, the prevalence of internet fraud in Nigeria has skyrocketed, despite national and international efforts to curb the trend. University campuses, meant to be centers for learning and intellectual development, are increasingly becoming breeding grounds for cybercriminal activities. This disturbing trend calls for urgent sociological inquiry into the underlying factors encouraging such deviance, especially among educated youths.

Peer pressure is a well-established concept in sociological and psychological literature. It refers to the influence exerted by a peer group in encouraging an individual to change their attitudes, values, or behaviors in order to conform to group norms. In the university setting, students are often exposed to intense socialization processes, including the desire to "belong" to influential or affluent circles. Many university students, particularly those from lower socio-economic backgrounds, are vulnerable to peer pressure that glamorizes cybercrime as a fast and easy route

to wealth and social status. Peer groups often play a pivotal role in shaping an individual's ethical boundaries, particularly in environments where societal values are in flux or corrupted by materialism.

The influence of social media is another powerful factor driving the rise of cyber fraud among students. Platforms such as Instagram, Facebook, TikTok, and Snapchat, among others, have created a digital culture where ostentatious displays of wealth and luxury are normalized, even celebrated. Many university students, especially in Nigeria's consumerist and image-conscious society, are exposed to images and narratives that promote a 'get-rich-quick' mentality. These platforms often serve as both the stage and the tool for cyber fraud, enabling perpetrators to scout victims, execute scams, and flaunt their illicit gains. The constant comparison with peers online who seem to be living lavishly can create feelings of inadequacy and desperation among students, pushing them toward unethical means of acquiring similar lifestyles.

The convergence of peer pressure and social media creates a potent mix that normalizes cyber fraud as not only acceptable but aspirational. This normalization is compounded by the erosion of moral standards, lack of effective regulation, and weak enforcement mechanisms. The glamorization of cybercriminals—who are often seen as role models in their communities—further emboldens young people. Stories of cyber fraudsters driving exotic cars, traveling the world, and living flamboyantly dominate social conversations, particularly in university environments where success is often measured by material possessions rather than academic achievements or personal integrity.

In many Nigerian universities, students are exposed to an environment where ethical boundaries are blurred, and success is increasingly measured by superficial indicators. The lack of effective

ethical education, mentorship, and socio-economic support systems within educational institutions contributes to the vulnerability of students to peer pressure and cybercrime culture. Moreover, the digital divide and poor awareness of cyber ethics among the student population create fertile ground for manipulation and exploitation. Another factor worth considering is the sociocultural evolution of values in Nigeria. The transition from communal, value-driven societies to individualistic, materialistic cultures has weakened traditional structures of accountability. With the weakening of moral authority from parents, religious institutions, and community leaders, students increasingly look to peers and digital influencers as guides for behavior. This change in value systems makes it easier for students to rationalize deviant behavior, including cyber fraud, especially when it yields quick rewards.

The Nigerian government, in partnership with international organizations, has launched several initiatives aimed at curbing cybercrime, such as the establishment of the Economic and Financial Crimes Commission (EFCC) and the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015. However, these measures have often focused on punitive responses rather than preventive strategies. Very little effort has been made to address the social and psychological drivers of cybercrime, particularly among university students. A more holistic approach that incorporates educational reform, youth empowerment, peer mentorship, and digital literacy is needed to tackle this problem effectively.

This study aims to fill a gap in existing research by exploring how peer influence and social media exposure interact to shape students' perceptions and involvement in cyber fraud. It will employ a sociological framework to understand how group dynamics, identity formation, social comparison, and media consumption contribute to the normalization and proliferation of cybercrime among

students. By focusing specifically on university students in Nigeria, the study seeks to offer contextually relevant insights that can inform policy, education, and intervention strategies.

The choice of university students as the focal population is strategic. University students represent a critical segment of Nigerian youth, often considered the intellectual and future leaders of the nation. Understanding how and why some of them become involved in cybercrime despite their education and potential can provide invaluable lessons for society at large. Moreover, university environments offer a microcosm of wider Nigerian society, making them ideal for sociological inquiry into broader societal trends and transformations.

Cyber fraud among Nigerian university students is not merely a criminal issue but a deeply rooted sociological phenomenon influenced by peer dynamics and digital culture. Social media platforms and peer pressure do not only serve as enablers of cybercrime but also as tools for its justification and glorification. This study intends to explore the influence of peer pressure on university students' involvement in cyber fraud; assess the role of social media platforms in normalizing and facilitating cyber fraud among students and compare the relationship between social acceptance, materialism and engagement in cybercrime within the university communities A comprehensive understanding of these factors is essential for developing effective interventions that target the root causes rather than just the symptoms of cyber fraud. This study will therefore investigate the depth and nature of these influences, offering recommendations for stakeholders in education, policy, and law enforcement on how to address the problem at its sociological core.

Literature Review

Conceptualization

The increasing incidence of cyber fraud among university students in Nigeria has become a subject of growing concern for scholars, law enforcement agencies, policymakers, and educators. While economic hardship and unemployment are often cited as drivers of this phenomenon, deeper sociological influences, such as peer pressure and social media, have proven to be more subtle yet powerful enablers. These two factors do not only encourage engagement in cyber fraud but also contribute to its normalization and perceived legitimacy among students.

This conceptual framework outlines the key variables, theories, and interrelationships necessary to investigate how peer pressure and social media contribute to the rise of cyber fraud among Nigerian university students. The framework is grounded in sociological and psychological theories such as Social Learning Theory, Differential Association Theory, and Strain Theory, which help explain how behavior is learned, justified, and normalized within specific social contexts.

Key Concepts Defined

Cyber Fraud

Cyber fraud refers to the criminal exploitation of information and communication technologies (ICTs) to manipulate or deceive individuals, businesses, or government entities, typically for financial benefit. It encompasses a wide range of illegal activities such as phishing, identity theft, online romance scams, financial fraud, and business email compromise. In the Nigerian context,

cyber fraud has taken on a particularly widespread and socially recognized form, often referred to colloquially as "Yahoo Yahoo." This term is commonly associated with various fraudulent activities perpetrated online, particularly by young individuals who use fake identities to deceive victims, frequently targeting foreigners through social engineering techniques.

Nigeria has become a notable hotspot for cybercrime in Africa, driven by high youth unemployment, inadequate enforcement of cybercrime laws, and a rising culture of glorifying wealth acquired through dubious means. These factors have contributed to the popularity of internet fraud as a perceived shortcut to economic empowerment (Tade & Aliyu, 2011). Phishing scams, where individuals are tricked into revealing sensitive information such as bank details, are widespread. Similarly, romance scams involve fraudsters building fake emotional relationships with victims online to solicit money or gifts (Okeshola & Adeta, 2013). In response, the Nigerian government has taken steps to combat cyber fraud, including the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act in 2015, which outlines offenses and penalties related to cyber activities (Olumide & Olayemi, 2018). However, enforcement remains inconsistent, and cybercriminals continue to adapt their methods to evade detection. Ultimately, tackling cyber fraud in Nigeria requires a combination of stronger legal enforcement, public education, and the promotion of ethical use of digital technologies. Combating this menace also calls for international cooperation, as many victims reside outside Nigeria, making it a transnational crime issue.

Peer Pressure

Peer pressure refers to the social influence exerted by individuals within the same age group or social status, often encouraging others to conform to specific behaviors, attitudes, or lifestyle choices. In the context of higher education, particularly within universities, peer groups play a

significant role in shaping students' behavior, either positively or negatively. While peer influence can promote academic motivation and ethical conduct, it can also lead to undesirable outcomes, including involvement in deviant activities such as cybercrime. Among university students in Nigeria and other parts of the world, peer pressure has been identified as a contributing factor to the rising participation in cybercriminal activities. The desire to gain social acceptance, maintain status within a peer group, or emulate peers who appear successful through illicit means can drive students toward internet fraud and other forms of cybercrime (Adeniran, 2008). In many cases, students are introduced to cyber fraud, locally known as "Yahoo Yahoo," by close friends or roommates who serve as both mentors and motivators (Tade & Aliyu, 2011). The glorification of quick wealth and the normalization of fraudulent behavior within certain student circles further compound this issue (Ojedokun & Eraye, 2012).

Social Media

Social media refers to a collection of digital platforms such as Instagram, Facebook, TikTok, Snapchat, and X (formerly Twitter) that enable users to interact socially, share content, express identities, and access or disseminate information rapidly across the globe. While these platforms were primarily designed to enhance communication, social connectivity, and information sharing, they have also become tools misused for illicit purposes, including cyber fraud. In contemporary society, especially among youth populations, social media has become deeply integrated into everyday life. Unfortunately, this integration has also extended into the digital underworld of cybercrime. Social media platforms are often exploited by cybercriminals not only as tools for conducting fraudulent schemes but also as public stages for showcasing the spoils of their criminal activities. For example, fraudsters may use fake accounts to lure unsuspecting victims into online romance scams, phishing schemes, or investment fraud. Additionally, cybercriminals often flaunt ill-gotten wealth on platforms like Instagram or Snapchat, displaying expensive cars, luxury items, and lavish lifestyles, which can glamorize cybercrime in the eyes of impressionable users (Tade & Aliyu, 2011). This glamorization fuels a cycle of digital peer influence, where others—especially

young people—may be drawn into fraudulent activities in the hope of achieving similar financial success. Social media also facilitates anonymity, making it easier for perpetrators to hide their identities and evade law enforcement (Ojedokun & Eraye, 2012). Moreover, the global reach of these platforms enables cybercriminals to target victims across borders, turning local schemes into international operations (Olaifa, 2013). Addressing the misuse of social media in cyber fraud requires a multifaceted approach. This includes digital literacy campaigns, stricter platform regulations, and collaborations between tech companies and law enforcement agencies. Raising awareness about the dangers and consequences of cybercrime is crucial to reducing its appeal, particularly among youth populations.

University Students

University students are individuals enrolled in tertiary education institutions. As digital natives, they are highly engaged with online spaces and social networks, making them both potential victims and perpetrators of cyber fraud.

Theoretical Underpinnings

Social Learning Theory (Albert Bandura, 1977)

Albert Bandura's Social Learning Theory (1977) is a psychological framework that emphasizes the role of observation, imitation, and modeling in the learning process. According to this theory, individuals do not learn behaviors solely through direct experience or trial-and-error but also by watching others, particularly role models, and imitating their actions, especially when those actions are seen to be rewarded. Learning, in this context, becomes a social and cognitive process, where reinforcement (both positive and negative) influences whether a behavior is adopted or rejected.

In university settings, this theory is especially relevant in understanding how and why students become involved in cyber fraud. Many students, while not initially inclined toward cybercrime, are often introduced to it through close peers who are already engaged in such activities. When these peers are seen enjoying material success—such as expensive gadgets, fashionable clothing, or financial independence—others may begin to perceive cyber fraud as a viable or even admirable path to upward mobility. The perceived rewards (e.g., wealth, respect, popularity) act as reinforcements, increasing the likelihood that the observer will imitate the fraudulent behavior

(Adeniran, 2008). Social media plays a significant amplifying role in this process. Platforms like Instagram, Snapchat, and TikTok allow users to share curated and often exaggerated portrayals of their lives. For cybercriminals, this becomes a stage to flaunt their illicit gains, reinforcing the glamorization of fraud. This continuous exposure to seemingly successful fraudsters builds a culture of normalized deviance, especially among youth who may lack alternative role models or economic opportunities (Tade & Aliyu, 2011). The more these behaviors are rewarded socially—through likes, shares, and followers—the more they become attractive to observers, thus reinforcing Bandura's concept of vicarious reinforcement.

Strain Theory (Robert Merton, 1938)

Strain Theory explains deviance as a response to the gap between societal goals and legitimate means of achieving them. Nigerian university students often face high expectations for success but limited economic opportunities. This strain can push students to seek alternative (illegitimate) means—such as cyber fraud—to achieve social and financial success.

Peer Pressure and Cyber Fraud

Peer pressure plays a significant role in the behaviors adopted by students, especially during their formative years in university. Research shows that peer groups often become substitutes for familial or societal guidance, especially when traditional institutions are weakened or absent (Akpan & Udofia, 2021). In environments where cybercrime is portrayed as "smartness" or survival, students feel pressure to conform. Those who refuse may face exclusion, mockery, or marginalization, reinforcing the incentive to join.

In many Nigerian campuses, cybercriminals are often admired or even envied. Their flashy lifestyles—made possible through fraud—can set the standard for success within peer circles. As a result, students may feel compelled to imitate such lifestyles or at least show material success, even if it means engaging in illegal activities. The normalization of fraud within peer groups reduces the psychological barriers to participation.

The Role of University Environment

The university environment itself can either mitigate or reinforce the influence of peer pressure and social media. Institutions with poor monitoring systems, lax disciplinary frameworks, and little emphasis on ethics education provide a permissive atmosphere for cybercrime. Conversely, universities that integrate digital literacy, ethical reasoning, and career development into their curricula are more likely to reduce students' vulnerability.

Unfortunately, many Nigerian universities are underfunded, overcrowded, and lack functional guidance and counseling systems. This creates a void often filled by deviant peer groups and misleading online communities.

Material and Methods

Study Area

Nigeria, Africa's most populous nation, gained independence from British colonial rule in 1960. Since then, the country has experienced significant social, political, and technological changes. With the advent of the internet in the late 1990s and early 2000s, Nigeria witnessed a digital revolution that opened doors for global connectivity, especially among youths in tertiary institutions. However, this digital boom also contributed to the emergence of cybercrime. In the early 2000s, Nigeria became internationally known for "419 scams"—a form of internet fraud named after a section of the Nigerian Criminal Code. These scams laid the foundation for more sophisticated forms of cybercrime, which have evolved with advances in technology. The country's growing population of tech-savvy youths, high unemployment rates, and economic instability created fertile ground for cybercrime to flourish. University students, in particular, are often drawn to cybercrime due to financial pressure, peer influence, and the appeal of social media. Peer pressure plays a significant role in the adoption of cybercrime among students. In many Nigerian campuses, students who flaunt wealth obtained through dubious means are often admired, creating a culture that pressures others to emulate them. This normalization of internet fraud among peers reinforces criminal behavior and makes it more socially acceptable.

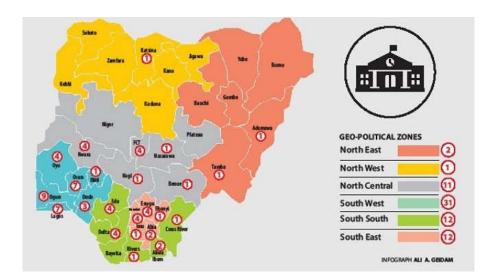


Fig 1 Map of Nigeria Showing Tertiary institution (Anyawu 2016)

Sampling Techniques

This study adopts a rigorous multistage sampling strategy to investigate university students' engagement with and understanding of cyber-related issues across South-South Nigeria, a region encompassing six states: Akwa Ibom, Bayelsa, Cross River, Delta, Edo, and Rivers. However three Universities was purposively selected from Delta, Bayelsa and Edo States Respectively. The sampling methodology unfolds in three systematic phases to ensure comprehensive regional representation and data validity. The cluster sampling technique ensures that each state contributes equally to the sample pool, which enhances the generalizability of the findings across the region. (Creswell & Creswell, 2018).

Following the cluster sampling, the study advances to the second stage using stratified sampling by faculty or department. From each selected university, two faculties are chosen, such as the Faculty of Social Sciences and the Faculty of ICT or Engineering. These faculties are targeted because they are more likely to offer courses related to digital literacy, cybersecurity, and communication technologies. The third stage of sampling also applies stratified sampling, this time based on students' academic levels. Students from 200 to 500 levels are included, while 100-level students are excluded due to their relatively limited exposure to university curricula. Stratifying by level (200, 300, 400, and 500 levels) ensures a diverse range of academic maturity

and experience, enabling the study to assess knowledge progression and differences across year groups. This multistage approach enhances the representativeness and robustness of the sample, allowing for nuanced insights into cyber-related awareness among university students in South-South Nigeria (Etikan & Bala, 2017).

A total of 300 undergraduate students were sampled as participants in this study, drawn from three carefully selected universities located within the South-South geopolitical zone of Nigeria. To ensure balanced representation and academic diversity, 100 students were randomly selected from each of the three universities. The selection process involved a multistage sampling approach that prioritized randomness and inclusiveness while also considering the academic relevance of the students' fields of study to the research topic. The participating universities were chosen based on their regional location, academic capacity, and the presence of departments offering programs related to digital literacy, cybersecurity, and information and communication technology. Within each university, students were drawn from both social science and ICT-related faculties, ensuring a comprehensive cross-section of respondents who are likely to have varying levels of exposure to digital tools and cybersecurity concepts.

Table 1: Sample size Determination

Stage	Sampling Technique	Details
Stage 1	Cluster Sampling	Selection of 3 universities from the South-South zone of Nigeria: DELSU NIGER DELTA UNIBEN
Stage 2	Stratified Sampling	From each university: - 2 faculties selected (Social Sciences & ICT/Engineering) - 2 departments per faculty (e.g., Mass Comm, Comp Sci)
Stage 3	Stratified Random Sampling	From each department: - 12 students selected - Only 200–500 level full-time students included - Total: 48 students per university
Total	_	4 departments × 12 students = 48 per university 48 × 3 universities = 144 + 5% oversample (~15 students) = ~300 students total

Source: Author's compilation (2025)

Result And Discussion

Table 2: Influence of Peer Pressure on University Students' Involvement in Cyber Fraud (4-Point Likert Scale, N = 300)

Statement	Strongly Disagree (1)	Disagree (2)	Agree (3)	Strongly Agree (4)	Mea n
1. I engaged in cyber fraud because my peers were doing it.	60 (20%)	90 (30%)	105 (35%)	45 (15%)	2.45
2. Peer pressure makes it hard to say no to online fraud opportunities.	45 (15%)	75 (25%)	120 (40%)	60 (20%)	2.65
3. Most of my friends support or are involved in cyber fraud.	90 (30%)	105 (35%)	75 (25%)	30 (10%)	2.15
4. I feel more accepted by peers when I engage in cyber fraud activities.	105 (35%)	90 (30%)	60 (20%)	45 (15%)	2.15
5. Peer influence increases my likelihood or participating in cyber fraud.	f 30 (10%)	60 (20%)	135 (45%)	75 (25%)	2.85

The Likert scale results in Table 1 reveal important insights into how peer pressure influences university students' involvement in cyber fraud. The statement with the highest mean (2.85) was "Peer influence increases my likelihood of participating in cyber fraud", indicating a strong perception among students that peers play a significant role in their decision-making regarding online fraud. Nearly 70% (agree + strongly agree) acknowledged this influence.

Similarly, the statement "Peer pressure makes it hard to say no to online fraud opportunities" recorded a mean of 2.65, reinforcing that many students struggle to resist peer-driven temptations. These two items suggest that peer norms and social belonging contribute significantly to decisions to engage in cyber fraud. Conversely, statements such as "Most of my friends support or are involved in cyber fraud" and "I feel more accepted by peers when I engage in cyber fraud activities", both with a mean of 2.15, showed relatively weaker agreement. This suggests that while direct peer involvement in cyber fraud may not be widespread, perceived approval or subtle encouragement might still influence behavior.

Interestingly, 50% of respondents (agree + strongly agree) admitted to engaging in cyber fraud because their peers were doing it (mean = 2.45), pointing to conformity-based influence. These findings are consistent with the Social Learning Theory, which posits that individuals adopt behaviors observed in others, especially in peer groups. A similar study by Olowu and Adebayo (2020) found that peer pressure significantly predicted cybercrime involvement among Nigerian university students. Likewise, Chukwudi and Nwankwo (2018) concluded that students influenced by deviant peer groups were more likely to engage in digital fraud.

These results underline the critical role of peer influence in shaping students' involvement in cyber fraud and highlight the need for targeted interventions and peer-led education to curb this growing issue.

Table 3: Role of Social Media Platforms in Cyber Fraud Among Students

Variable	Category	Frequency (n)	Percentage (%)
1. Social media platforms where cyber fraud is commonly seen	Facebook	45	15.0%
	Instagram	72	24.0%
	WhatsApp	48	16.0%
	Telegram	60	20.0%
	TikTok	75	25.0%
2. Have you ever received fraudulent messages/links via social media?	Yes	213	71.0%
	No	87	29.0%
3. Do you believe social media normalizes cyber fraud among peers?	Yes, frequently	102	34.0%
	Occasionally	129	43.0%
	Rarely	51	17.0%
	Never	18	6.0%
4. Have you ever been tempted to participate in online fraud due to peer influence?	Yes	57	19.0%
	No	243	81.0%
5. Types of fraud observed on social media	Fake giveaways	90	30.0%
	Investment scams (e.g., crypto, forex)	75	25.0%

Variable	Category	Frequency (n)	Percentage (%)
	Job scams	54	18.0%
	Phishing links	81	27.0%
6. Do you think social media makes it easy to commit cyber fraud?	Strongly agree	114	38.0%
	Agree	108	36.0%
	Disagree	60	20.0%
	Strongly disagree	18	6.0%

The descriptive data in Table 2 highlights the significant role social media platforms play in facilitating cyber fraud among students. The findings reveal TikTok (25%) and Instagram (24%) as the leading platforms where cyber fraud is commonly observed, followed by Telegram (20%), WhatsApp (16%), and Facebook (15%). This suggests a higher prevalence of fraud on newer, fast-growing platforms, possibly due to their younger user base and less stringent security measures. This aligns with the study by Olumide et al. (2022), which found that image-based platforms like Instagram and TikTok were increasingly being exploited by scammers targeting youths with fake promotions and investment offers. Furthermore, 71% of the respondents reported having received fraudulent messages or links via social media, emphasizing the ease and pervasiveness of these tactics. A considerable portion of students also acknowledged the normalization of cyber fraud among peers, with 34% saying it happens frequently and 43% stating it occurs occasionally. This normalization effect reflects findings by Chen and Smith (2021), who explored how repeated exposure to fraud-related content can desensitize users and lower their guard against online scams.

Despite the widespread exposure, only 19% admitted being tempted to participate in cyber fraud due to peer influence, indicating that while social influence is a factor, a majority resist the pressure. As for the types of fraud observed, fake giveaways (30%) and phishing links (27%) are the most common, followed closely by investment and job scams. These patterns mirror the observations in Adebayo and Musa (2020), where phishing and impersonation scams were found to be the most reported among Nigerian university students.

Table 4: Pearson Correlation Matrix of Social Acceptance, Materialism, and Cybercrime Engagement (n = 300)

Variable	1. Social Acceptance	2. Materialism	3. Cybercrime Engagement
1. Social Acceptance	1.000		
2. Materialism	-0.32** (p = 0.001)	1.000	
3. Cybercrime Engagement	-0.41** (p < 0.001)	0.58** (p < 0.001)	1.000

The findings from the Pearson Correlation matrix revealed notable relationships among the variables studied. Specifically, social acceptance exhibited a significant negative correlation with both materialism and cybercrime engagement. This implies that individuals who report higher levels of social acceptance are less inclined to adopt materialistic values or participate in cybercrime-related behaviors. In contrast, materialism demonstrated a strong positive correlation with cybercrime engagement, suggesting that individuals who prioritize material possessions and wealth are more likely to become involved in cybercrime activities. These correlations were found to be statistically significant, with p-values equal to or less than 0.001, reinforcing the robustness of the results. The implications of these findings align closely with previous research, particularly the study conducted by Enwa, Osugba, and Agbeyi (2023), which concluded that materialistic tendencies can significantly influence an individual's likelihood to engage in criminal behavior and other forms of social deviance. Therefore, the present study supports the notion that societal values and interpersonal acceptance play crucial roles in shaping behavior and deterring involvement in illegal or unethical digital practices.

Conclusion and Recommendations

This study has provided an in-depth sociological examination of the roles that peer pressure and social media play in promoting cyber fraud among university students in Nigeria. The findings affirm that both factors significantly contribute to the normalization and proliferation of cybercrime on campuses. Through the lens of Social Learning Theory and Strain Theory, it becomes evident that students are not merely passive participants but active agents influenced by their social environments and internalized cultural narratives that glorify illicit success. Peer groups, acting as immediate reference communities, foster environments where cyber fraud is

increasingly seen as acceptable even aspirational. The data suggests that while not all students directly experience pressure to engage in cybercrime, a substantial number are influenced by peers who are either involved in or supportive of such behavior.

Equally critical is the influence of social media platforms, particularly TikTok and Instagram, which serve as both tools and stages for fraudulent activity. These platforms facilitate exposure to cyber fraud schemes and propagate materialistic ideals that lure impressionable students into fraudulent behavior. The study also reveals a strong positive correlation between materialism and cybercrime engagement, and a negative correlation between social acceptance and such deviance, suggesting that students who feel socially included and grounded are less likely to resort to unethical means of acquiring wealth. Moreover, the university environment, often lacking in adequate ethical guidance and digital literacy, inadvertently provides a permissive atmosphere for deviance to flourish.

Recommendations

There is a need for educational institutions and policymakers to implement holistic, preventive strategies that address not just the symptoms but the root causes of cyber fraud among students. Combating this issue effectively requires a multi-pronged approach that incorporates ethics education, peer-led mentoring, stronger cybercrime awareness, and socio-economic empowerment programs.

Universities should integrate digital ethics and cybercrime awareness into their curricula, while establishing peer mentorship and counseling programs. Government and tech platforms must collaborate to strengthen cyber regulations and promote digital literacy.

Socio-economic support systems should also be enhanced to reduce students' vulnerability to materialistic pressures and online criminal influence on undergraduate students of the university

References

Agbo, A. A. (2019). Youth Unemployment and Cybercrime in Nigeria: A Study of Cyber Fraud in Lagos State. African Journal of Criminology and Justice Studies, 12(1), 123–140.

Akpan, U. & Udofia, A. (2021). Peer Group Influence and Deviant Behaviours among University Students in South-South Nigeria. Journal of Sociology and Development, 4(2), 98–114.

Adeniran, A. I. (2008). The Internet and Emergence of Yahoo-Boys Sub-Culture in Nigeria. *International Journal of Cyber Criminology*, 2(2), 368–381.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly, 34(3), 613–643.

Adebayo, T., & Musa, K. (2020). *Cybercrime and youth vulnerability on social media: A study of university students in Nigeria*. Journal of Cybersecurity and Information Integrity, 5(2), 98–110.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588–608.

Bandura, A. (1977). Social Learning Theory. Englewood Cliffs, NJ: Prentice Hall.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.).

Chen, R., & Smith, J. (2021). *Peer influence and normalization of cyber fraud among adolescents*. Journal of Digital Youth Culture, 9(1), 43–59.

Chukwudi, F., & Nwankwo, I. U. (2018). Peer influence and youth involvement in cybercrime in universities in South-East Nigeria. Journal of Social Sciences, 5(2), 45-56.

Etikan, I., & Bala, K. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal*, 5(6), 00149. https://doi.org/10.15406/bbij.2017.05.00149

Enwa S. Osugba S, and Agbeyi M. (2023), Implication of Terrorism/farmers-herders Conflict Amongst Crop Framers in Agatu Local government area of Benue State Nigeria, Journal of Environmental Biosciences, 25 (4)

Merton, R. K. (1938). *Social Structure and Anomie*. American Sociological Review, 3(5), 672–682.

Internet World Stats (2022). Nigeria internet usage and telecommunications reports.

Okeshola, F. B., & Adenaike, F. A. (2018). *The Nature, Causes and Consequences of Cybercrime in Tertiary Institutions in Nigeria*. International Journal

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state of Nigeria. *American International Journal of Contemporary Research*, 3(9), 98–114.

Olumide, A. O. (2020). Exploring Social Media Influence on Youths' Engagement in Cybercrime in Nigeria. Journal of Youth Studies in Africa, 2(1), 45–60.

Olumide, S. O., & Olayemi, M. (2018). Evaluating the Nigerian Cybercrimes Act 2015: Challenges and prospects. *Journal of Law, Policy and Globalization*, 77, 1–8.

Ojedokun, U. A., & Eraye, C. M. (2012). Socioeconomic lifestyles of university students and involvement in cybercrime in Nigeria. *Journal of Law and Conflict Resolution*, 4(1), 1–10.

Olaifa, T. (2013). Media and the escalating cybercrime culture in Nigeria. *Journal of Information and Knowledge Management*, 3(5), 82–89.

Olowu, A. A., & Adebayo, S. O. (2020). Peer pressure and involvement in internet fraud among university undergraduates in southwestern Nigeria. African Journal of Criminology and Justice Studies, 13(1), 89-102

Olumide, O., Adeyemi, A., & Fatima, S. (2022). Social media platforms as enablers of cybercrime among youth: An exploratory study. African Journal of Cyber Psychology, 3(4), 112–129.

Sutherland, E. H. (1947). Principles of Criminology (4th ed.). Philadelphia: Lippincott..

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, 5(2), 860–875.

National Bureau of Statistics (2021). Youth unemployment and social trends in Nigeria.

Uche, E. A., & Osezua, C. (2022). Social Media and the Rising Culture of Cybercrime in Nigeria: A Youth Perspective. Journal of Digital Society Research, 5(1), 101–120.

Yar, M. (2005). *The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory*. European Journal of Criminology, 2(4), 407–427