Chapter 17

Cybercrime's Toll on Education: Unravelling the Academic Fallout of Internet Fraud among Students

Ipinlaye A. B.

Corresponding author's email: ipinlayeab@aceondo.edu.ng

ABSTRACT

The study examined the impact of cybercrimes or internet frauds on the academic performance of students at Adeyemi Federal University of Education, Ondo. It explored various forms and causes of cybercrimes, offering solutions to this widespread issue. Data were gathered from 200 respondents across five Schools or Faculties within the University using a structured questionnaire consisting of 20 items. The analysis, conducted through one-way ANOVA statistics, led to the conclusion that there is no significant correlation between cybercrime and students' academic performance. However, the research identified key factors driving undergraduates towards cybercrimes, such as poor family backgrounds, peer pressure on campus, and the bleak outlook on future employment opportunities, among others. The recommendations from the study emphasize the role of parents in instilling good virtues and morals in their children and call for severe penalties for students engaged in cybercrimes to deter potential offenders.

INTRODUCTION

Internet fraud, as outlined by Wikipedia (2023), involves deceptive practices on the internet aimed at tricking individuals or organizations into relinquishing money, property, or personal information for financial gain. This form of fraud, also known as computer fraud, is characterized by the

exploitation of online platforms such as websites, emails, social media, and instant messaging to execute fraudulent schemes.

Eze-Michael (2021) suggests that Internet Fraud is a specific segment of the broader category of cybercrime, which includes various illegal activities conducted online, such as cyberstalking, cyberbullying, online trafficking, child pornography, and cyber terrorism. Internet Fraud itself manifests in several forms, including phishing or spoofing, ATM fraud, online fake shopping, scareware or malware, business email compromise (B.E.C.), data breach, email account compromise (E.A.C.), ransomware, identity theft, lottery fraud, social media frauds, and matrimonial dating fraud. In Nigeria, "yahoo boys" are notably involved in these computer fraud techniques to illicitly obtain money from victims, often causing substantial financial losses and undermining the trust in internet commerce (Chukwuka, 2022).

The scope of internet fraud is broad, covering various deceptive activities conducted through online platforms to illegally gain personal information, financial advantage, or other benefits. These fraudulent activities leverage the anonymity and expansive reach of the internet to target individuals and organizations. Danielet al. (2020), Omodunbi et al. (2016), and Akpan & Friday (2022) highlight several common forms and methods of internet frauds or cybercrimes, including but not limited to, those listed above.

Forms and Methods of Internet Frauds or Cybercrimes

Phishing

This entails dispatching misleading emails, messages, or websites mimicking reputable entities to deceive individuals into disclosing confidential details like passwords, credit card numbers, or access credentials.

Identity Theft

Cybercriminals misappropriate personal details, including names, addresses, Social Security numbers, and financial information, to assume the identities of others or engage in deceitful acts using their personas.

Online Shopping Scams

Swindlers establish counterfeit online storefronts or auction platforms, purporting to offer goods that are nonexistent or substandard. Unsuspecting customers make payments for merchandise they ultimately do not receive, culminating in financial detriment.

Advance Fee Fraud

This involves convincing victims to pay upfront fees or provide money with the promise of receiving a larger sum in return, which never materializes. Common examples include lottery scams and inheritance scams.

Investment Scams

Deceptive investment schemes advertise substantial returns with minimal risk. Investors pour money into sham projects and consequently suffer financial losses.

Romance Scams

Fraudsters fabricate fictitious online relationships to emotionally exploit victims, coercing them into parting with money under deceitful pretexts.

Ransomware

Cybercriminals employ malevolent software to deny victims access to their own systems or data, subsequently demanding a ransom to restore access.

Tech Support Scams

Scammers pose as technical support personnel, deceiving victims into believing their computers are infected with malware. They propose to resolve the issue for a fee or seek remote access to the victim's computer. Additionally, criminals engage in credit card fraud by stealing credit card details to conduct unauthorized transactions or sell the information on the black market.

Social Engineering

This process entails influencing individuals to disclose confidential information or undertake actions that jeopardize security, incorporating strategies such as impersonation, persuasion, and coercion.

Online Auction Fraud

Scammers create fraudulent auction listings or place bids on their own items to artificially increase prices or fail to deliver products to the winning bidders.

Data Breaches

Hackers unlawfully access databases storing sensitive data, including personal details and credit card numbers, for use or sale.

Charity Scams

Fraudsters establish counterfeit charity organizations to exploit individuals' altruism during crises or emergencies. Additionally, misleading advertising involves untrue or overstated claims in online adverts, potentially leading consumers to buy products or services that do not live up to their promotional portrayals.

Fake Job Offers

Scammers present fictitious job opportunities, frequently demanding advance payments for training materials or promising improbable salaries.

To safeguard against internet fraud, it is crucial to remain vigilant and adhere to recommended practices, including:

- Exercise caution with unexpected emails or messages requesting personal or financial information.
- Ensure the legitimacy of websites before disclosing sensitive information or conducting online transactions due to the prevalence of insecure websites.
- Employ secure, distinct passwords and enable two-factor authentication when feasible.
- Maintain updated computer and antivirus software.
- Familiarize yourself with prevalent scams and stay informed about new threats.

It's essential to notify the local law enforcement agency or the designated cybercrime reporting organizations in your country if you encounter or suspect internet fraud. In Nigeria, the Economic and Financial Crime Commission (EFCC) is tasked with combating cybercrimes.

Factors Contributing to Internet Frauds or Cybercrimes among Nigerian Students

Hassan et al. (2012) pinpointed several factors fueling the rise of cybercrimes in Nigeria, including urbanization, high unemployment rates, the quest for wealth, insufficient enforcement of cybercrime laws, inadequately equipped law enforcement agencies, and negative role models. Akwara et al. (2013) studied the interconnectedness between unemployment, poverty, and insecurity in Nigeria, uncovering that unemployment begets poverty, which subsequently has a direct correlation with increased insecurity. They further emphasized corruption and the susceptibility of the internet as additional accelerants for cybercrime.

Urbanization

Rapid urbanization in Nigeria, marked by a substantial population increase, presents a dilemma for policymakers. Akpan and Friday (2022) have noted that the advantages of urbanization are contingent upon the creation of quality employment opportunities within urban areas. Nevertheless, urbanization has been linked to a surge in cybercrimes, often associated with heightened criminal activities.

Unemployment

Nigeria grapples with a significant unemployment issue, with rates hitting 23.1% in the last quarter of 2018 and youth unemployment exceeding 47%. Omodunbi et al. (2016) have highlighted the wide-ranging socio-economic, political, and psychological impacts of such high unemployment levels. This scenario facilitates the emergence of street

youth and urban delinquents, fostering a culture that is prone to engaging in criminal activities.

Corruption

Nigeria's ongoing battle with corruption is starkly illustrated in international assessments, where it was placed 144th out of 176 countries according to Transparency International's 2018 report (Daniel et al., 2020). This environment, where unlawfully acquired wealth is not only tolerated but celebrated, fosters a culture that encourages the pursuit of quick financial gains, often through illicit means such as cybercrime.

Poverty

Poverty, defined by an inability to meet basic needs, is a primary catalyst for cybercrime (Jolaosho, 2016). The rampant poverty, coupled with high rates of youth unemployment and weak enforcement of cyber security regulations, cultivates an environment ripe for criminal undertakings. This is particularly evident in the significant number of young individuals engaging in cybercrimes.

Statement of the Problem

In recent times, the expansion of internet access has significantly transformed the educational landscape, granting students unparalleled access to information and resources. However, this progress has also introduced a significant concern affecting students' academic endeavors – internet fraud. The rising incidence of online fraudulent activities has overshadowed the digital learning environment. This study aims to explore the complex effects of internet fraud on students' academic performance. By delving into the consequences of falling victim to internet fraud, such as compromised personal and financial security, diminished trust in online platforms, and heightened stress levels, this research endeavors to highlight how internet fraud detrimentally impacts students' engagement in their studies. Through an in-depth examination of this issue, the study seeks to contribute to the formulation of effective strategies and awareness initiatives to protect students from the adverse effects of

internet fraud, thereby promoting a safe and supportive online learning environment.

Purpose of Study

This research was conducted to assess the impact of internet fraud among undergraduates and its effect on their academic performance at Adeyemi College of Education, Ondo. It aimed to identify the primary causes, the various methods employed in this illegal activity, and to propose solutions to address this issue in higher education institutions.

Significance of Study

This study is of importance as it sheds light on the factors contributing to internet fraud and its effects on students' academic performance. The findings will offer valuable insights that can aid government and educational stakeholders in combating the widespread occurrence of internet fraud in higher education institutions. Additionally, the results will support organizations such as the Economic Financial Crime Commission (EFCC) and the Department of State Services (DSS) in executing their duties more effectively and efficiently.

Research Questions

The study is guided by the following research questions:

1. What are the primary factors responsible for cybercrime among university undergraduates?
2. What are the significant consequences of cybercrime on university undergraduates' academic achievement?
3. What possible measures can be taken to reduce cybercrime among university undergraduates?

Research Hypotheses

For this research, the following null hypotheses were proposed and tested:

$H_0$1: There is no significant relationship between poverty and cybercrime.

$H_0$2: There is no significant relationship between peer pressure and students' involvement in cybercrime.

$H_0$3: There is no significant relationship between cybercrime and students' academic performance.

METHODOLOGY

A descriptive survey research design was utilized for this study, a method known for gathering data from a selected sample to represent a larger population. This approach facilitates the extrapolation of data analysis findings to the broader population, making it apt for our research goals.

Area of the Study

The study was conducted within Adeyemi Federal University of Education, Ondo, across five Schools: Arts and Social Sciences, Languages, Education, Sciences, and Vocational and Technical Education.

Population for the Study

The survey encompassed a population of over 4,000 undergraduates from Adeyemi Federal University of Education, Ondo.

Sample and Sampling Techniques

The study's sample consisted of 200 respondents. A purposeful sampling technique was employed to select 40 undergraduates from each of the five schools to ensure equal representation.

Data Collection

Data was collected using a researcher-structured questionnaire. The questionnaire was divided into two sections. Section A requested personal information such as School, Department, level, age, and gender. Section B comprised 16 items designed to address the research questions, utilizing a modified four-point rating scale: Strongly Agree (SA) = 4 points, Agree (A) = 3 points, Disagree (D) = 2 points, and Strongly Disagree (SD) = 1 point. Three experts from Adeyemi Federal University of Education, Ondo, validated the instrument for face and content validity.

DATA ANALYSIS

Data from the questionnaire items were presented in tables to facilitate analysis using tables that are as follows:

Table 17.1: Factors leading undergraduate students into cybercrime?

SN	Questions	SA	A	D	SD
1	Many students now pay more attention on how to make money rather than focusing on their studies.	138	54	6	2
2	The fear of unemployment is the major reason for students involvement in Cybercrime	72	116	18	4
3	Internet fraud is viewed as social exposure to new innovations and ideas	114	70	14	2
4	Peer pressure is responsible for students engaging in internet fraud				

Hypothesis ($H_0$1): There is no significance relationship between poverty and cybercrime

Table 17.1.1: ANOVA Table for $H_0$1

Source of variation	SS	df	MS	F_{ratio}	F_{crit}	Decision
Between Groups (Poverty)	74945-5	3	2498.5	26.10	3.490	REJECT
Within Groups (Cybercrime)	1148.5	12	95.708			

From the analysis presented, it's evident that the F-ratio exceeds the F-critical value at a 0.05 Alpha level of significance, leading to the rejection of the null hypothesis. This outcome indicates a significant relationship between poverty and cybercrime, suggesting that poverty is a contributing factor to students' involvement in cybercrime.

Table 17.2: What are the various means of executing these illegal acts?

SN	Questions	SA	A	D	SD
1	Online fraud can be through sale or advertisements of goods and services that do not exist	72	100	26	2

2	The fraudster sends spam mails to unsuspecting individuals to reveal their password and token	98	62	36	4
3	Phone calls are made with victims pretending to be from a financial or banking institutions that the victims uses.	92	86	20	2
4	Some social media networks like WhapApps, Facebook Instagram e.t.c. are majorly used in scamming unsuspected people	88	92	16	4

Research Hypothesis ($H_0$2): There is no significance relationship between peer pressure and students' involvement in cybercrime.

Table 17.2.1: ANOVA Table for $H_0$2

Source of variation	SS	df	MS	F_{ratio}	F_{crit}	Decision
Between Groups (Peer pressure)	5595.5	3	1865.17	65.349	3.490	REJECT
Within Groups (students involvement in cybercrime)	1148.5	12	28.5417			

Similarly, the results from Table 17.2.1 demonstrate that the F-ratio again surpasses the F-critical value at a 0.05 Alpha level of significance, resulting in the rejection of the null hypothesis. Consequently, this reveals a significant relationship between peer pressure and students' involvement in cybercrime, indicating that peer influence is a significant factor that drives some students towards engaging in cybercrime activities within the school environment.

Table 17.3: Effects of cybercrime on undergraduates' academic achievement?

SN	Questions	SA	A	D	SD
1	Attendance of lectures is at my own convenience	108	74	10	6
2	Internet fraud affects studying at night as internet fraud is	84	82	30	4

	mostly done at night				
3	Academic performance of students who are into internet fraud are better than those who are not	46	40	82	32
4	Students who are guilty of cybercrime should be rusticated out of School	40	54	70	36

Research Hypothesis ($H_0$3): There is no significance relationship between cybercrime and students' academic performance.

Table 17.3.1 ANOVA Table for $H_0$3

Source of variation	SS	df	MS	F_{ratio}	F_{crit}	Decision
Between Groups (cybercrime)	1483.5	3	494.5	2.788	0.08617	ACCEPT
Within Groups (students' academic performance)	2128.5	12	177.37			

The result of the table 17.3.1 above shows F_{ratio} is less than F_{crit} at 0.05 Alpha level of significance and thus the null hypothesis is accepted. This shows that there is no significant relationship between Cybercrime and students' academic performance.

DISCUSSION OF FINDINGS

The study illuminates the multifaceted factors contributing to cybercrime among university undergraduates, including economic background, poverty, unemployment, and peer influences. The consequences of cybercrime on students' academic achievements are severe, leading to poor attendance, academic underperformance, and in extreme cases, expulsion. The stigma attached to cybercrime tarnishes the reputation of not only the individuals involved but also their educational institutions and families. Cybercrime also leads to significant financial losses, loss of property, and in dire situations, can result in physical harm or loss of life through activities such as "Yahoo plus."

To address this pressing issue, a comprehensive approach is required. Providing employment opportunities, empowerment programs, and relief funds can alleviate the socio-economic pressures that propel individuals toward cybercrime. Furthermore, implementing severe penalties for those caught in such activities can act as a powerful deterrent.

In conclusion, effectively combating cybercrime among university undergraduates calls for a combination of socio-economic support, stringent punitive measures, and proactive prevention strategies. This comprehensive approach aims to mitigate the negative impact of cybercrime on students' academic performance and overall well-being. Some general findings on internet fraud and students' academic achievement are;

Negative Impact on Academic Performance

Several studies, including those by Igba et al. (2018), Adegbola & Ojo (2022), and Akpan & Friday (2022), have demonstrated a significant negative correlation between internet fraud and students' academic performance. Engaging in fraudulent activities online, such as cheating, plagiarism, or purchasing assignments, can seriously undermine the learning process and result in poor academic outcomes.

Increased Distraction and Time Mismanagement

Internet fraud can lead to significant distractions for students, including online scams, phishing emails, and fraudulent websites, which detract from study and coursework. Furthermore, engaging in fraudulent activities contributes to poor time management, thereby limiting the time available for academic pursuits.

Reduced Ethical Awareness

Internet fraud can lead to a decline in students' ethical awareness and moral values. Involvement in fraudulent practices can cause students to become desensitized to the significance of academic integrity, resulting in deteriorated ethical behavior in their academic pursuits.

Psychological Consequences

The exposure to internet fraud can result in psychological consequences for students, including feelings of guilt, anxiety, and stress stemming from the fear of being caught, tarnishing their reputation, or facing disciplinary actions. These emotional burdens can adversely affect students' mental well-being, concentration, and overall academic performance.

Long-term Consequences

Engaging in internet fraud during educational years can lead to long-term consequences. Students who develop unethical behaviors and engage in fraudulent practices may carry these habits into their professional lives, potentially affecting their future career prospects, professional relationships, and personal development.

CONCLUSION

The study concludes that cybercrime significantly endangers the educational system and the economy. In some universities, individuals involved in internet fraud, often referred to as "yahoo boys," receive preferential treatment due to their financial contributions and displays of wealth. Research by Igba et al. (2018) indicates that internet fraud leads many undergraduates to neglect their studies, as they are preoccupied with surfing the internet or engaging with their mobile phones, adversely affecting their academic performance. Adebisi, Oluwafisayo, & Adeyemo (2017) noted that students involved in internet fraud typically spend an average of four hours a day online. Factors such as poor family background, peer pressure, a desire to become wealthy, and a lack of employment opportunities are identified as primary reasons why many students engage in cybercrime (Igba et al., 2018).

The study suggests several strategies to mitigate the menace of cybercrime among university undergraduates. Enhancing internet security by telecommunication regulatory agencies and creating job opportunities for unemployed youth are among the recommended measures. Allowing the proliferation of cybercrimes to continue unchecked is untenable, as no nation can thrive without a strong moral foundation. This research indicates that students' involvement in cybercrime is motivated by various factors, and addressing these issues effectively can have a positive impact on the nation. The government, families, and students themselves play

critical roles in this effort. These findings support the research of Adegbola & Ojo (2022) and Akpan & Friday (2022).

RECOMMENDATION

Based on the study's findings, the following recommendations are made:

1. Parents must assume their responsibilities by instilling good virtues and morals in their children, as the students involved in cybercrimes come from families.
2. The government should bolster security agencies tasked with combating cybercrime by establishing mechanisms to track and investigate cybercriminal activities both within and outside educational institutions.
3. Stringent penalties, such as severe punishments, should be imposed on students engaged in cybercrimes to deter others from considering such activities.
4. Parents and religious organizations should proactively educate the youth about the dangers of cybercrime, emphasizing the importance of diligence and integrity.
5. The public should be adequately informed about the risks of cybercrime through various media channels to increase awareness.
6. Governments are encouraged to create job opportunities, provide empowerment programs, and offer relief funds to improve the livelihoods of the youth.
7. Academic achievements should be recognized and rewarded to promote a culture of excellence and integrity among students.

REFERENCES

Adegbola, I. A., & Ojo, F. O. (2022). Cyber crime among mathematical science students: Implications on their academic performance. *Journal of Digital Learning and Distance Education (JDLDE).* https://www.rju.publisher/ojs/index.php/JDLDE

Adebisi, F. T., Oluwafisayo, A., & Adeyemo, S. O. A. (2017). The impact of internet on undergraduates' study time. *Advances in Social Sciences Research Journal, 4*(11), 155–161.

Akpan, E. E., & Friday, E. P. (2022). The effect of cybercrime on the educational system of Nigeria. *Gaspro International Journal of Eminent Scholars, 7*(2).

Akwara, A. F., Akwara, N. F., Enwuchola, J., Adekunle, M., & Udaw, J. E. (2013). Unemployment and poverty: Implications for national security and good governance in Nigeria. *International Journal of Public Administration and Management Research (IJPAMR), 2*(1).

Chukwuka, O. U. (2022). Internet fraud: The menace of 'Yahoo Boys' and the deceitfulness of riches. *Sapientia Global Journal of Arts, Humanities and Development Studies (SGOJAHDS), 5*(2), 87–97. ISSN: 2695-2319; ISSN: 2695-2327.

Daniel, D. W., Adamu, B. I., Abdullahi, B. A., Mairiga, B. R., Ebenezer, A. A., & Danjumma, B. (2020). Combatting cybercrimes in the education sector. *International Journal of Engineering Applied Sciences and Technology, 5*(4), 108–117. Retrieved from http://www.ijeast.com

Eze-Michael, E. (2021). Internet fraud and its effect on Nigeria's image in international relations. *Covenant Journal of Business and Social Sciences (CJBSS), 12*(1). Retrieved from http://www.Journal.covenant.edu.ng

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *Journal of Science and Technology, 2*(7), 626–631.

Igba, D. I., Elizabeth, C. I., Aja, S. N., Simon, C. N., Egbe, E. U., & Ogodo, J. V. (2018). Cybercrime among university undergraduates: Implications on their academic achievement. *International Journal of Applied Engineering Research, 13*(2), 1144–1154. Retrieved from http://www.ripublication.com

Jolaosho, A. O. (2016). Some popular perception of poverty in Nigeria, quoted in UNDP Human Development Report on Nigeria. Lagos: UNDP.

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. O. (2016). Cybercrimes in Nigeria: Analysis, detention and prevention. *FUOYE Journal of Engineering and Technology, 1*(1). ISSN 2579-0617.

Wikipedia. (2023). Internet fraud. In *Wikipedia, the Free Encyclopedia*. Retrieved from https://en.wikipedia.org/wiki/Internet_Fraud