



---

## **Undergraduates' Perception of Factors Influencing Cybercrimes in Selected Universities in Anambra State, South-East, Nigeria**

**Okeke, Obinna Chukwudalu**

Department of Sociology/Anthropology, Faculty of Social Sciences, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.

**&**

**Oli, Nneka Perpetua**

Department of Sociology/Anthropology, Faculty of Social Sciences, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.

### **Abstract**

This study examined undergraduates' perception of factors influencing cybercrimes in selected universities in Anambra State, South-East, Nigeria. The study adopted mixed methods research design. The area of study comprised of public and private universities in Anambra State. The scope of the study is on investigating perception of undergraduates' involvement in cybercrimes in selected universities in Anambra State, South-East, Nigeria. The target population was 40,092 undergraduate regular students of Nnamdi Azikiwe University, Awka, Paul University Awka, Tansian University, Umuaya and Chukwuemeka Odumegwu Ojukwu University, Igbariam who were 16 years and above. The sample size for this study was 1,083 undergraduates was generated using Taro Yamane statistical method of sample size determination, while 20 participants were selected through purposive and snowball sampling techniques for the In-Depth Interview (IDI) session. The research used both probability and non probability sampling methods in the selection of respondents. Multi-stage sampling procedure which involved the use of different sampling techniques in the selection of respondents was employed in the study. Questionnaire and IDI guide were the quantitative and qualitative instruments used for data collection in the study, respectively. Data collected through quantitative instrument were processed using the Statistical Package for Social Sciences (SPSS) Version 2.0 software. Also, descriptive statistics such as frequency tables, simple percentages and graphic illustrations were used to analyse the quantitative data and research questions. The qualitative data collected from the IDIs were analysed using Nvivio analytical software. Four hypotheses were tested using Chi-square ( $X^2$ ). Findings in the study showed that avarice and peer pressure are the major factors that influence undergraduates' involvement in cybercrime. Therefore, the study recommends that government and stakeholders should organise programmes that will equip the undergraduates with enriching skill-acquisition programmes during holidays and vacations; in order to re-channel their attention and energy from cybercrimes to more worthwhile lucrative money-making ventures.

---

**Keywords:** cybercrimes, perception, socio-economic status, undergraduates, university.

## **Introduction**

The introduction of technology and internet has made the world a global village. This is due to the fact that, from the comfort of one's home, people can view what is going on in every other country and continents of the world, interact with people from another country or race and conduct business transactions with ease. The internet and its technologies have tremendous impacts on individuals and societies across the globe. These impacts have taken different shapes and forms over the years. Cyber activities have both positive and negative impacts on the users as individuals, organizations, groups, people and society at large. Due to the fact that there are insignificant barrier to the use of the internet and its technologies, it has become an open field for everyone, which makes people to use the internet for good and bad intentions. The internet, which remains one of the best elements of information technology human existence has experienced, continues to present humans with endless opportunities but the goodness of it has been hijacked by scrupulous human elements identified as cyber criminals who use the internet for mendacious and inimical activities.

According to Alansari, Aljazzaf, and Sarfraz, (2019), cybercrime is any Internet-related crime that is always directed against individuals, groups, and or state and its economy motivated by the criminal intention that can cause damage/destruction that may be of different types including physical, mental, loss of money and also it involves the unlawful accessing of information of the victims using electronic devices. Cybercrimes may vary based on the potential damages they might cause, its targets and the nature of its occurrence. Hence, cybercrimes may be harassment, cyber terrorism, child pornography, digital piracy, cyber stalking, computer hacking, or unauthorized access to computer databases, networks, and spam (Mshana, 2015).

Based on the aforementioned, cybercrime is viewed as crime committed through communication process on computer devices with the aid of internet and applications to extort victims of their hard earned money, property or reputation. Cybercrime can also be defined in this work as those crimes perpetrated through electronic communication network, particularly the internet. Rotimi (2015) averred that the menace is very rampant among the youths within the age of 18 to 35 years and it would be inappropriate to describe youths in Nigeria based on the temporal relation of age because of the timeline and multiplicity of opinion on this issue. Meanwhile, the Social Development Policy for Nigeria (SDPN, 1980) defines youths as those between the age of 18 and 35 years, which was later adjusted to be persons between the ages of 15 and 29 years of age, in line with The Commonwealth age categorisation. For the purpose of this study, the term youths simply refer to adolescents and young adults who are between the ages of 15 and 29 years as stated by The Commonwealth of Nations (SDPN, 1980). However, Olaide and Adewale

(2004) observed that suspected cyber fraudsters or cybercriminals in Nigeria fall within the youthful age. This is because the youths have revealed various ways of using the internet in perpetrating different types of criminal activities and also Nigerian youths are noted for being idealistic, adventurous, resourceful, inquisitive and proactive as envisaged by Adelamo (1999).

Conclusively, crimes vary significantly from society to society. As such, one cannot conclude in a hurry that crimes such as internet-based crimes are prevalent in every society. This is in consideration of the fact that various researches on the prevalence of internet-based crimes within the context of public and private universities in Anambra State have been relatively scarce. Hence, there is a gap in knowledge on the theme of this study within the context of this present study area. It is against this backdrop that this study is positioned to examine undergraduates' perception of factors influencing cybercrimes in selected universities in Anambra State, South-East, Nigeria.

### **Statement of the Problem**

A global concern today is the issue of cybercrime among youth. This social phenomenon has been constituting huge security, economic and mental health threats to individuals, corporate and government organizations in different countries. A global economic crime survey by Armin, Thompson, Ariu, Giacinto, Roli and Kijewski (2015) puts the annual cost of cybercrime to the global economy at more than €300 billion, while the cost of cybercrime for the European Union (EU) was estimated to be 0.4% of its GDP amounting to € 13 Billion per annum. This report claimed that Poland, Germany and United Kingdom, lost €377 million, €2.6 billion, and €2 billion per annum respectively (Armin, et al., 2015). These figures among others showed that cybercrime globally constitutes a serious financial threat to the economy and the wellbeing of their innocent victims. It also follows logically that a crime of this magnitude is possible when individuals remove self-censure and self-sanctions from their behaviour.

Cybercrimes have become serious problem in Nigeria, culminating in the listing of Nigeria as third on the roll of the top ten cybercrime hot spots in the world by a 2009 Internet Crime Report (Federal Bureau on Investigation, 2010). The seriousness of this problem can be better appreciated when we consider the fact that in spite of the several interventions made by Nigerian government and Non- Governmental Organizations (NGOs) in tackling cybercrime, such as the co-operation between Microsoft Corporation and the Economic and Financial Crimes Commission (EFCC) of Nigeria to fight cybercrime, the enactment of Cybercrime Laws by Nigerian government aimed at ensuring the security of computer systems and networks in Nigeria etc (Balogun & Obe, 2010), Nigeria has for four consecutive years (2006, 2007, 2008 and 2009) ranked third on the list of world cybercrime perpetrator countries Federal Bureau on Investigation (FBI, 2010). Thus, Debarati and Jaishanka (2011) stressed that cybercrimes are offences that are committed

against individuals or group of individuals with criminal motive to intentionally harm the reputation of their victims or cause physical or mental harm to their victims directly or indirectly using modern telecommunication networks such as internet (chat rooms, e-mails etc.) and mobile phones (SMS/MMS). The use of modern applications has enhanced cyber criminality such as facebook, yahoo messenger, tinder, twitter, instagram, snapchat, telegram, among others. However, there is no generally accepted typologies of cybercrime, but scholars of criminology typified two main kinds of internet related crime such as; (1) the Advanced Cybercrime (or high tech crime), sophisticated attacks against computer hardware and software; (2) Cyber Realm Enabled Crime (Interpol, 2016). What this implies is that many traditional crimes have taken a new turn with the emergence of the internet, such as crimes against children, financial crimes and even terrorism (Oyesanya, 2015).

The availability and the permissive (commercial) uses of the internet technologies have equally encouraged mass youth's participation and as well increased the depth of maladaptive uses of the technology globally. Besides, the victims of cybercrimes cannot be completely exonerated in the complicities involved in the crime. There is complementarily the demand-supply nexus. Also, in locating the causal factors promoting youth and cybercrime affinity literally, it is important to explore this from the platform where the group draws its existence—the society. The healthy state or otherwise of any society remains the determinant of both substantive and emerging challenges that are capable of impinging on the survival of such entities and concomitantly the occupiers. Most outstanding in this regard is the cultural, socio-economic, and the psycho-physical components of a society that are commonly affected by both internal and external influences and needed to promote national sectoral development.

However, with respect to the undergraduates in Nigerian universities, the contribution of the internet to the academic development of Nigerian undergraduates has been marred by the conscious evolution of new waves of crime. The internet has also become an environment where the most productive and safest offence thrives. Cybercrime has come as a surprise and a strange appearance that now lives with Nigerians with each passing day; we observe more and more alarming cases of cybercrimes perpetrated by Nigerian undergraduates, with each new case more shocking than the one before (Folashade, Okeshola & Adeta, 2013). Thus, the ubiquity of social media platforms in recent times has further aggravated the extent of cybercrime involvement among undergraduates in Nigeria (Akor, 2017). Indeed, the trend and patterns of this crime are fast changing with the increasing involvement of female students. For instance, in November, 2018, the Economic and Financial Crimes Commission (EFCC) arrested 34 undergraduates, including nine females suspected to be involved in cyber fraud perpetration at Awa-Ijebu, Ogun State (Akinkuotu, 2018). Moreover, Tade and Aliyu (2011) submit that cyber fraud, a form of cybercrime has literally become a way of life for many undergraduates in Nigerian

universities. Aghatise (2006) contends that 80% of cybercrime perpetrators in Nigeria are students in various institutions.

It is envisaged in this study that a way of averting this ugly crime is to scientifically examine its prevalence particularly among the undergraduate students of universities in Anambra State. This is due to the fact that, enough research efforts have not been made to focus on this area of research interest, particularly within the context of the universities in Anambra State, Nigeria. In view of the afore-mentioned problems, this study examines undergraduates' perception of factors influencing cybercrimes in selected universities in Anambra State, South-East, Nigeria.

### **Research Questions**

The following research questions were formulated to guide the study;

1. How prevalent are cybercrimes among undergraduates of universities in Anambra State, South-East, Nigeria?
2. What are the factors that influence cybercrimes among undergraduates of universities in Anambra State, South-East, Nigeria?

### **Review of Related Literature**

#### **Factors that Influence the Prevalence of Cybercrimes amongst Undergraduates**

There are various factors that influence the prevalence of cybercrimes among undergraduates of universities in Nigeria. In their empirical study titled "Public Perceptions on the Determinants of Youths' Involvement in Cybercrime in Enugu Urban, Enugu State: A Framework for Social Workers", Eya and Odo (2019) used questionnaire and Focus Group Discussions (FGDs) as the major instruments for data collection. The copies of questionnaire were administered to one hundred and forty-four (144) adults (18 years and above) in Enugu urban. Samples were selected using multi-stage sampling procedure. Statistical Package for Social Sciences (SPSS) software was used for processing the data. Findings from the study show that unemployment, poverty and lack of internet security are the major determinants of youth's involvement in cybercrime. Odo and Odo (2015) investigated the extent of involvement in cybercrime activities among students in tertiary institutions in Enugu State of Nigeria. Their findings showed that students of higher institutions in Enugu State are involved in cybercrime. It also showed that students' involvement in cybercrime is dependent on gender and institution type.

Tade and Aliyu (2011) carried out a study that examined the widespread and social organisation of electronic fraud among undergraduates of University of Ibadan, Nigeria. The study utilised snowball sampling technique to select 20 internet fraudsters. The main instruments for data collection were In-Depth Interview (IDI) Guide and Focus Group Discussion (FGD). The information obtained from the interviews were analysed manually

using content analysis. The findings showed that internet fraud in tertiary institutions is socially organised and highly networked, which is becoming highly specialised and sustained by informal networks. This however, involves the nefarious networking of fellow fraudsters in partnership with some dubious commercial bank staff. The study revealed that the commercial bank staff usually leak vital details of some affluent bank customers to these internet fraudsters, therefore facilitating payment without alerting security agencies; while the fraudsters arrange for a bailout options in periods of crises during the fraudulent transactions. The study also revealed how monies are paid through domiciliary accounts, cheques, credit cards, Money Gram, Western Union, etc.

In addition, Umeozulu (2012) conducted a research titled “Perception of Cybercrime among Nigerian Youths (A Study of Caritas University)”. The research design used for the study was the survey method. The area of study was Caritas University Amoji-Nike Emene of Enugu State. The target population comprises of male and female students who reside in the hostels of residence of Caritas University in Enugu State. However, 3282 is said to be population of the university, the sample tool used for the study was structured questionnaire, which was administered to 354 respondents who were undergraduate students of Caritas University, Enugu State. Quantitative data from the study was processed with the aid of SPSS version 2.0 software while the qualitative data was analysed using manual thematic method of data analysis. The finding reveals that poverty, peer pressure, unemployment and moral decadence are the factors influencing cybercrimes among youths in Nigeria.

Also, a descriptive survey was carried out by Eze and Ezedikachi (2021), on Internet Fraud and its Effect on Nigeria’s Image in International Relations at Covenant University Ota, Ogun State. A sample size of 630 was used in the study. A simple random sampling technique was employed to select undergraduates of the university. This study investigated the factors influencing internet fraud on Nigeria’s image in international relations. The data generated from the study were processed using SPSS software version 2.0. The findings showed that unemployment, poverty and peer group influence are the motivating factors that stimulate internet frauds among undergraduates of universities in Nigeria.

### **Theoretical Framework**

Strain theory was propounded by Robert K. Merton in 1968 in his work titled “Social Theory and Social Structure” built on Emile Durkheim’s theorization of anomie. Robert Merton developed strain theory to explain individuals’ varying patterns of deviation resulting from gaps within societies (Spiegel, 2006). Merton opined that normative breakdown and other deviant behaviours within societies are products of disjoints between culturally approved expectations or goals and socially structured or legitimized avenues to achieve success (Murphy & Robison, 2008). According to Merton, the structural imbalance between goal and approved means explains nonconformist behaviours not only

at societal levels but also at individual levels (Spiegel, 2006). He analysed how individuals adjust to the patterns of goals and means in one of the five different ways and this structure by Merton is generally referred to as adjustment patterns to anomic conditions. Spiegel (2006), opines that the gap between approved goals and the means creates strain.

In contemporary society, success is primarily measured in terms of material achievements and social standing. In a mixed economy such as Nigeria, individuals must choose their own path and work hard to earn a living. This leads to competitive nature of careers and employment. Borrowing from the idea of Emile Durkheim, Merton (1968) further analysed how individuals adjust to the patterns of goals and means in one of five different ways which he maintained that, when rules cease to operate, a situation of normlessness or anomie results. In this situation of “anything goes”, norms no longer direct behaviour and deviance is encouraged. However, according to him, there are five distinct ways through which people can adapt to social strain they include Conformity (++): in this condition, strained individuals would accept the cultural goal of success or wealth attainment, and often try to achieve it through legitimate means. This is the only non-deviant adaptation to strain according to Merton. Innovation (+-): this is the adaptive means for those who have accepted the cultural goal of success/wealth attainment but are trying to achieve it using illegitimate means. Innovation within the ambit of crime commission entails people devising innovative or novel ways to breakthrough in criminal actions. Ritualism (-+): this adaptive means is used by people who abandon the cultural goal of success/wealth attainment, but continue to use legitimate means to make their living. Retreatism (--): this is the condition whereby people who are strained reject the cultural goal of success/wealth attainment and also reject the legitimate means of attaining it, as a means of adapting the strain. Rebellion (--++): people who adopt this adaptive mechanism are classified as political deviants (Acharya & Taylor, 2012). They include people who do not play by the rules but work to change the system to their own liking. Thus, from the above classification by Merton, one can easily classify perpetrators of cybercrimes as ‘the innovators’ based on their belief system and modus operandi in pursuing positive goal (financial success) but employing a negative means to achieve a positive goal.

This theory is relevant in this study due to its ability to proffer insight in understanding that crime and deviance is not a matter of a few bad apples; it is a necessary condition of good social living. The theory maintains that to control crime, the government should enact laws and build institutional frameworks to enforce law, order and cyber security in Nigeria. However, judging from the assumptions of this theory, one may hastily conclude that crimes like cybercrimes are committed by lower-class individuals, the unemployed and miscreants in society. However, judging from the reality on the ground within the context of modern day cybercrimes, where it has been more of organised crime involving highly technically organised individuals; thus, the theory may be found to be deficient.

On the other hand, Edwin Sutherland (1883 – 1950) developed the Differential Association Theory (DAT) in 1939 in the third edition of his book titled: “Principles of Criminology”. The theory asserts that an individual is more likely to commit a crime when the individual learns favourable definitions towards violations of the law over the definitions unfavourable to violation of the law. That is people, learning to engage in crime, primarily through their association with others and weighs the benefits. The theory of differential association can be applied to cybercrime. This theory is premised on the fact that, criminal behaviour is learned through social interactions with others. The profile of cyber criminals is one who is very smart, highly knowledgeable and who is computer savvy. Their social interactions may come through electronic communications with other individuals who share similar technological interests. According to Sutherland (1939; 1960), criminal behaviour is learned in interaction with other persons in a process of communication. This would mean an individual is influenced to participate in criminal behaviour through watching and interacting with other individuals who are engaging in the criminal behaviour. The principal part of the learning of criminal behaviour occurs within intimate personal groups. When criminal behaviour is learned, the learning includes techniques of committing the crime, which are sometimes very complicated, sometimes simple and they learn the specific direction of motives, drives, rationalizations and attitudes for committing a crime.

Thus, in relation to the study, the undergraduate student views himself as young and innovative; therefore, he commits cybercrimes such as hacking, advance fee fraud, identity theft, flash bank credit alert, coding and outside or inside espionage as a way to express his creativity cum the anonymity nature of the cyber realm. This theory is relevant in explaining the emergence of cybercrimes among undergraduates because they learn these deviant behaviours from their interactions with others and the environment around them. Cybercriminals acquire deviant behaviour on cyber or computer-related crimes from people they associate with within their daily lives. Today, people rely on computer devices to do almost every daily activity including communicating, studying, researching and working. Consequently, this environment provides a suitable environment for undergraduates to engage in cybercrimes. Strain theory and differential association theory have been adopted as the theoretical framework in this study because they are the most suitable, adequate, appropriate, relevant and best explain the phenomenon of cybercrimes.

### **Materials and Methods**

This paper adopted mixed methods research design, which allowed the use of quantitative and qualitative techniques in gathering information. The design allowed the researcher to collect data on a one time basis from respondents with the purpose of providing answers to the study research questions, objectives and hypotheses. The quantitative method of data collection was adopted in order to draw information from a relatively large sample; while the qualitative design was employed in order to help the researcher gain deeper insight on



the problem under study. This research was conducted in Anambra State, specifically at Nnamdi Azikiwe University (NAU), Awka; Chukwuemeka Odumegwu Ojukwu University (COOU), Igbariam; Tansian University (TANU), Umunya and Paul University (PU), Awka. Thus, the justification for choice of the study areas (NAU, PUA, COOU and TANU) for this study is because there have been several incidences of cybercrimes among undergraduates of universities in Anambra State, South-East geo-political zone in particular and Nigeria in general. The population of the study is 40,092 undergraduates while the sample size is 1,083. This was generated using Taro Yamane (1967) formula for sample size determination. The multi-stage sampling procedure which involved successive sampling of probability and non-probability methods were used in selecting study participants. This involved the application of different sampling techniques like balloting, cluster, stratified proportionate and simple random sampling techniques at various stages. However, snowball and purposive sampling technique of non-probability sampling method were employed in selecting five students which include one yahoo-boy and four students who were knowledgeable of cybercrimes from each of the schools selected for the study. Data were collected using questionnaire and In-Depth Interview (IDI) guide. The researcher through the help of two research assistants used self-administered questionnaire; out of which 1020 copies were correctly filled, retrieved and used for analysis. The data were processed with the aid of Statistical Package for Social Sciences (SPSS) version 2.0 software and analysed using frequency distribution tables, percentages, mean ratings and graphic illustrations. The qualitative data were analysed thematically using quotes extracted from the interviews.

## **Findings/Results**

### **Socio-Demographic Characteristics of the Respondents**

This section dealt with the analysis of socio-demographic characteristics of the respondents such as gender, age, marital status, religious affiliation, place of residence, parental/guardian academic qualification and parental/guardian occupation.

Table 1 presented the socio-demographic characteristics of the respondents. It shows that 26.6% of the total respondents were males while 70.4% were females. This implies that the number of female respondents exceeds the number of male respondents. This may be attributed to the fact that males are no longer interested in education, but are more interesting in heinous and unconventional means to amass wealth at ease; while their female counterparts prefer to acquire formal education to empower themselves.

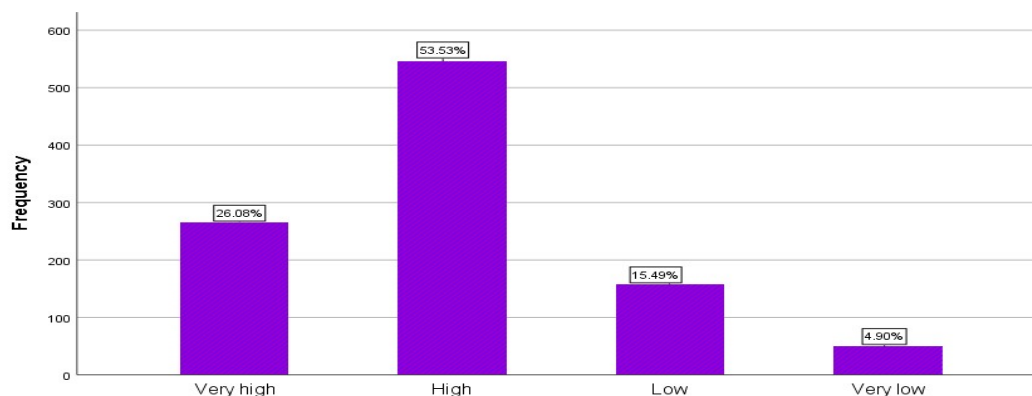
**Table 1: Socio-Demographic Characteristics of the Respondents (n = 1020)**

<b>Variables</b>	<b>Frequency (f)</b>	<b>Percentage (%)</b>
<b>Sex</b>		
Male	302	29.6
Female	718	70.4
Total	<b>1020</b>	<b>100.0</b>
<b>Age</b>		
16-20	334	32.7
21-25	525	51.5
26-30	108	10.6
31 and above	53	5.2
Total	<b>1020</b>	<b>100.0</b>
<b>Marital Status</b>		
Single	970	95.11
Married	24	2.35
Divorced	8	0.78
Separated	10	0.98
Widowed	8	0.78
Total	<b>1020</b>	<b>100.0</b>
<b>Religion</b>		
Christianity	854	83.7
Muslim	24	2.4
African Traditional religion	78	7.6
Others	64	6.3
Total	<b>1020</b>	<b>100.0</b>
<b>Place of permanent residence</b>		
Urban	928	91
Rural	92	9
Total	<b>1020</b>	<b>100.0</b>
<b>Parental academic qualification</b>		
None formal education	82	8
FSLC	68	6.7
SSCE/GCE	56	5.5
OND/NCE	256	25.1
HND/B.Sc.	512	50.2
M.Sc./Ph.D.	46	4.5
Total	<b>1020</b>	<b>100.0</b>
<b>Parents'/guardians occupation</b>		
Civil servant	286	28
Public servant	180	17.6
Artisan	118	11.6
Trading/Business	390	38.2

Farming	46	4.5
Total	<b>1020</b>	<b>100.0</b>
<b>Academic level</b>		
100 level	132	12.9
200 level	286	28.9
300 level	420	41.2
400 level	130	12.7
500 level	52	5.1
Total	<b>1020</b>	<b>100.0</b>

### Field Survey, 2023

Majority (32.7%) of the respondents fall within the age bracket of 16-20 years, while the least number (5.2%) of the respondents were within the age bracket of 30 years and above. The mean age of respondents was 21.37 years. This implies that majority of them are between the ages of 16-20 years. This is not strange since this is the age bracket for people to gain admission and graduate from the universities. Majority (95.1%) of the respondents were single while the least number (0.78%) of the respondents were either widowed or divorced. This implies that majority of them are single. This is as a result of the fact that they are majorly young adults and still of university age. Hence, they are not expected to be married at such young age. Majority (83.7%) of the respondents were Christians while the least number (2.4%) of the respondents were Muslims. This is not surprising because the study location is in Anambra State, South-East Nigeria dominated by Christians. Similarly, the majority (91%) of the respondents reside in urban areas, while the least number (0.9%) of the respondents reside in rural areas. This implies that most of the respondents live in urban centres which accounts for their level of knowledge and awareness of the use of internet and the perpetration of cybercrimes. Majority (50.2%) of the respondents reported that their parents had HND/B.Sc., while the least number (4.5%) reported that their parents had M.Sc./Ph.D. Majority (28%) of their parents were civil servants while the least number of them (4.5%) were farmers. This implies that their parental academic qualifications and occupation, most of the respondents' parents/guardians are educated up to Bachelor's level and Higher National Diploma but are mostly into self-employment or private businesses which account for the reason why they are usually preoccupied with their businesses and pay less attention to what their children/wards do on the internet while at home, as well as the kind of friends they keep at home and on campus. Majority (41.2) of the respondents were in 300 level while the least number (5.1%) were in 500 level. Thus, the academic levels of the respondents showed that majority of them are in their penultimate year in school, which makes them more informed about the activities of some students who are involved in the internet scam and other forms of cybercrimes. This is due to the fact that, with the number of years they have spent on campus, they can easily identify some yahoo boys and girls among them, as well as their mode of operations.



**Fig. 1: Respondents' views on the prevalence of cybercrimes amongst undergraduates of universities in Anambra State**

### Field Survey, 2023

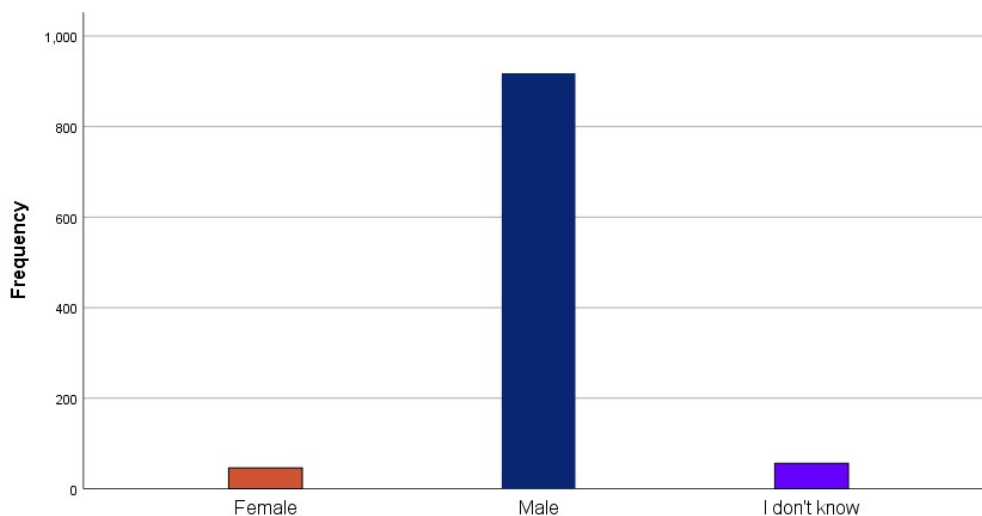
Fig. 1 shows that majority (53.53%) of the respondents admitted that cybercrimes are high amongst undergraduates while the least number (4.90%) of the respondents reported that cybercrimes are very low amongst undergraduates of universities in Anambra State. Thus, this implies that the prevalence of cybercrimes is high amongst undergraduates of universities in Anambra State. These findings corroborate data from the interviews that were conducted, where one of the interviewees stated thus;

I think that cybercrime is very high here on campus, especially among the male students. The students now see it as a means of survival and therefore see nothing wrong in indulging in it. In fact, for you to understand how prevalent this crime is in the campus I don't think that there is anyone in this school that is not aware of this crime, many of the students are involved in it, while others must have been victims one time or the other (Female, 21 years, 300 Level Student, Philosophy Department, NAU, Awka).

Also, another interviewee stated thus:

The issue of cybercrimes is a commonplace in Nigerian universities, which we usually call yahoo-yahoo. Ever since during Covid-19 lockdown, some students did not travel back to their homes, as well as during the last ASUU strike, including myself. These periods gave us enough time to stay indoors and concentrate on means of making money online through bitcoins, crypto-currency, etc. We pose as forex traders and used these online trade platforms to scam unsuspecting forex clients online. Then, when school resumed, a lot of guys returned to school with exotic flashy cars which are the evidence of our hardwork during lockdown and strikes

(Male, 25 years, 500 Level Student, Electronics and Computer Engineering Department, NAU, Awka).



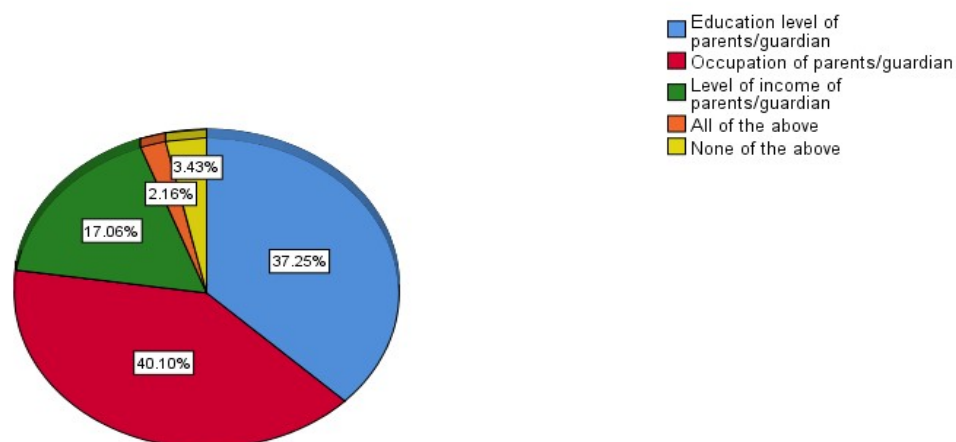
**Fig. 2 Respondents' views on the gender that is more likely to engage in cybercrimes. Field Survey, 2023**

Fig. 2 indicates that majority (90%) of the respondents indicated that males are more likely to engage in cybercrimes while the least number (4.5%) of the respondents said that females are more likely to engage in cybercrimes. Thus, it is obvious that males are more likely to engage in cybercrimes than their female counterparts among university undergraduates. This finding corroborates with data from the interviews that were conducted, where one of the interviewees stated thus;

I guess poverty and peer pressure are the prevailing factors encouraging this issue cybercrime. This is because I know one or two good guys when we enter year one, who out of desperation to live a flamboyant life, in order to impress their cliques and girlfriends ended up joining them in the act. They have always blamed it on their poor family economic background and all that. But the truth be told, they are simply lazy and lack good moral for positive hardwork for money (Male, 28 years, 500 Level Student, Law Faculty, COOU, Igbariam).

Additionally, another IDI participant opined that,

The major cause of the prevalence of cybercrime is fact that the Nigerian government has never been taking this issue of cybercrime serious. They are yet to be serious about it. That is what I think. No serious cyber laws yet with serious sanction (Male, 26 years, 300 Level Student, Accountancy Department, COOU, Igbariam).



**Fig. 3: Respondents' views on family's socio-economic factors that can encourage an undergraduate to indulge in cybercrimes**  
**Field Survey, 2023**

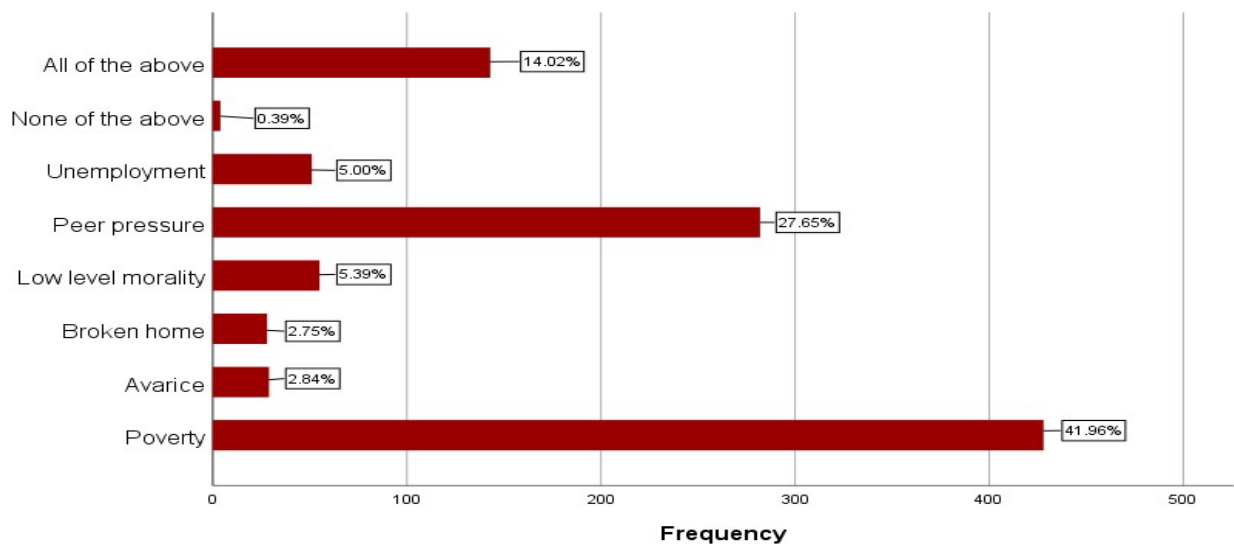
Fig. 3 above showed that majority (40.1%) of the respondents think that the occupation of parents/guardian can encourage an undergraduate to indulge in cybercrimes while the least number (2.79%) of the respondents think that all of the above-mentioned factors can encourage an undergraduate to indulge in cybercrimes. Thus, it is obvious that the occupation of parents/guardians is a major factor that influences cybercrime among undergraduates. This finding corroborates data from the interviews that were conducted, where one of the IDI participants interviewed stated thus; *'I will say that, failure in family system that is proper home training by parents is another cause of the prevalent cybercrime in Nigeria'* (Female, 25 years, 400 Level Student, Philosophy Department, NAU, Awka).

Another IDI participant also stated thus:

The major problem our society is facing currently is from the family. Some of our parents are illiterates and so pay less attention to what we their children do with our phones. As a result of that, some students use their phones for different things like watching pornography, doing online hook-up and going into romantic affairs with white women online with the intention to scam them. While some of our girls also do the same to white men on dating sites (Male, 23 years, 300 Level Student, Political Science Department, TANU, Umunya).

Also, another IDI participant expressed his opinion on the effects of socio-economic status of parents and the tendency of their children to engage in cybercrimes. He argued thus:

Due to the increasing hardship in Nigeria, parents who do not have high incomes pay more attention to means of making money to keep their homes and pay less attention to home training of their children. This has paved way for less attention to the monitoring of their children as well as trying to find out the kind of company they keep both online and offline (Male, 27 years, 400 Level Student, Electronics and Computer Engineering Department, NAU, Awka).



**Fig. 4: Respondents' views on factors that can lead to increase in cybercrime amongst undergraduates of universities in Anambra State.**

#### **Field Survey, 2023**

Fig. 4 shows that majority (42%) of the respondents believed that the major cause of cybercrime is poverty while the least number (0.4%) of the respondents indicated that none of the above-mentioned factors could lead to cybercrime. This implies that poverty is a significant factor that can lead to an increase in cybercrime among university undergraduates. This finding is corroborated by data from the interviews that were conducted, where one of the interviewees stated, thus: *'the high level of poverty and hardship in the country the things I can say are the major factors that push some most of the undergraduates into internet scam* (Male, 21 years, 200 Level Student, Industrial Chemistry Department, PU, Awka)'.

Another interviewee stated thus:

One of the major factors that encourage students like me to engage in internet-based crime, here in Nnamdi Azikiwe University is mostly the pressure from Friends, lodge mates and school mates. Everyone wants to have exotic cars, eat in the most expensive eatery and chill with the big boys, even flex with the expensive girls on campus. Although, poverty at family level also encourages some students to engage in internet criminal

---

activities (Female, 25 years, 400 Level Student, Political Science Department, TANU, Umunya).

Another participant noted that:

Peer pressure is one of the major causes of internet-based crime here in Paul University. Students are always on pressure from either their friends or course mate whom they are better than in academic endeavour living large in the school and at the same time sorting themselves out from poor grades, they sort lecturers for grades, so why won't one be intimidated and join them since with money everything is under control. Also moral decadence of our society is also a major cause of this menace since wealth is celebrated against hardwork (Male, 20 years, 200 Level Student, Mass Communication Department, PU, Awka).

### **Discussion of Findings**

It was found in this study that majority of the respondents testify that cybercrimes are prevalent among the undergraduates of universities in Anambra State, South-East, Nigeria. The very high rate of cybercrime among Nigerian students is on the increase. A good number of the participants in the in-depth interview agreed that the rate of cybercrime is very high among the students. This is in line with Asokhia (2010) findings that there is a prevalent indulgence of youth in cybercrimes; which the youths also see nothing wrong with it, but rather justify it as a way of survival amidst economic hardship in Nigeria. It was also seen in the study that majority of the respondents indicated that male students are the main perpetrators of cybercrimes among undergraduates of universities in Anambra State. Hence the interview results give reason why male students are more engaged in cybercrimes, stating that males are faced with many challenges, pressure from the society and peer groups to make money, unlike their female counterparts who experience less pressure with low expectation from the society as regards wealth creation. This contradicts the finding made by Tade and Aliyu (2011) where they found both genders as liable to cybercrimes, stating that neither male nor female gender is a major perpetrator of cybercrimes. The study also found that peer pressure is the major cause of cybercrimes among the undergraduates of universities in Anambra State. These findings are in conformity with Eze and Ezedikachi (2021) which found that peer pressure is the major cause of cybercrimes among undergraduates of universities in Anambra State. This corroborates Umeozulu (2012) finding which reveals that poverty tends to cause people's involvement in cybercrime. More so, the study established that moral decadence of our society led to cybercrime among the youth especially the undergraduates in institutions of higher learning. This implies that moral decadence encourages anti-social behaviour which can lead to crime, promotes the value of money over hard work, created get-rich-quick mentality and also lure the youth into accepting lifestyles that can be injurious to their present and future aspirations.



---

## Conclusion

Undergraduates' involvement in cybercrimes is a topical issue that is at the front burner of cyber security discourse, not just only in Nigeria, but also at the global village. This has become a global social problem since the invention of the internet and inception of globalization. Thus, it can be deduced from the foregoing that like in the human society, where crime has integrated into the system, cybercrime is an integral part of the virtual world. As the technology increases in terms of complexity and sophistication, cybercrimes are also on the increase. The problems of cybercrimes are associated with the fact that where the computer is not a target for cybercrime, it can also be the tool that can be used to facilitate cybercrime. One of the developing problems of the Nigerian economy is orchestrated by the prevalence of the financially-induced aspect of cybercrime; young people especially undergraduates constitute a large percentage of the population of people perpetrating this crime. Undergraduates across universities have turned cybercrimes into source of livelihood. Thus, there is a pertinent need for them to be retrained and updated on the latest ICT requirements, judging by the high level of cyber security knowledge possessed by the Nigerian youths involved in cybercrimes as opposed to the intermediate cyber security knowledge possessed by the average Nigerian security agents, who are saddled with the responsibility of detecting and arresting internet fraudsters.

## Recommendations

In line with the findings of the study, the following recommendations are made: -

1. Individuals in the society should observe simple rules such as; ensuring that they have a proper anti-malware protection in their computer system and individuals should be encouraged to avoid pirated software, also never to share their Personal Identification Number (PIN), bank account, email access code to unknown persons.
2. Management of universities should initiate the idea of periodic orientation of their undergraduate students on positive, safe and careful use of their phones, computers and the internet in general. This is to ensure they do not become victims of cybercrimes and also serve as a surveillance measure to discourage the students from abusing the internet by using it to learn internet scam and other forms of cybercrimes.
3. Authorities of Nigerian universities should encourage and impart entrepreneurial skills in their undergraduates. This will enable undergraduates to learn lucrative skills during vacations and as well provide them with the option of self employment on graduation, thus encouraging positive hard work and creating avenue to make money without getting involved in criminal activities. Rather than staying idle during the vacation because such could create an opportunity for them to learn illicit skills like cyber fraud, since an idle mind is a devil's workshop, as popularly said.

4. The government and the various university authorities in Nigeria should form a synergy and partnership in curbing cybercrimes on campuses in the country. This should be one of the proactive measures that will allow law enforcement agencies to track and investigate students involved in cybercrimes within and outside the institution. Besides, most of these students that practice such act can be easily tracked within their hostels in the institutions.
5. School management should be allowed to report students detected to be involved in cybercrimes as to avert its escalation, because by doing so it will reduce the perpetration of cybercrimes within the wall of the university. This can only be achieved through effective collaboration between the school management and the law enforcement agencies.

## REFERENCES

- Acharya, P., & Taylor, R. (2012). Innovative deviance: An investigation of the relationships between social control, creativity and innovation in organisations. *Academy of Business Research Journal*, 1, 49-58.
- Adelamo, I. A. (1999). *Youth and City: An Urban Environment Perspective, Workshop Proceedings on Youth and City: A Study of Lagos*. Development Researchers' Cooperative, Lagos.
- Akinkuotu, E. (2018). EFCC arrests 23 OOU students, 12 others for internet fraud. The Punch, Retrieved from <https://punchng.com/efcc-arrests-23-ouu-students12-others-for-internet-fraud> on 11th March, 2021.
- Akor, L. (2017). The social media, deviance and youth in Nigeria. In P. N. Ndubueze (ed.), *Cyber Criminology and Technology-Assisted Crime Control*, (pp. 47-64).
- Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In M. Sarfraz (ed.), *Developments in Information Security and Cybernetic Wars*, pp. 1-41. IGI Global, Hershey, PA, USA. doi:10.4018/978-1-5225-8304-2.ch001.
- Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). Cybercrime economic costs: No measure no solution. *10th International Conference on Availability, Reliability and Security. Cyber Road Project*, 701-710.
- Asokhia, M.O. (2010). Enhancing national development and growth through combating cybercrime/internet fraud: A comparative approach. *Journal of Social Sciences*, 23: 13-19.

- Balogun, V. F. & Obe, O. O. (2010). E-Crime in Nigeria: Trends, tricks and treatment. *The Pacific Journal of Science and Technology*, 11 (1), 343 – 355.
- Debarati, H. & Jaishankar, K. (2011). *Cybercrime and victimization of women: Laws, rights and regulations*. USA: Hershey, IGI Global.
- Eya, I. I. & Odo, I. C. (2019). Public perceptions on the determinants of youths' involvement in cybercrime in Enugu Urban, Enugu State: A framework for social workers. *International Journal of Innovative Research in Social Sciences and Strategic Management Techniques*, (1) 161-177.
- Eze & Ezedikachi. N. (2021) Internet fraud and its effect on Nigeria's image in international relations. *Covenant Journal of Business & Social Sciences (CJBSS)* 12 (1), 22-37
- Federal Bureau of Investigation (2010). Internet Crime Report. New York: Federal Bureau of Investigation. Retrieved from [www.fbi.gov/news/stories/2010/march/ic3031607](http://www.fbi.gov/news/stories/2010/march/ic3031607) on 26th May, 2022.
- Folashade B., Okeshola A. & Adeta, K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*. 3 (9), 106-118.
- Haralambos, M., Holborn, M. & Herald, R., (2008). *Sociology and perspectives*. (7<sup>th</sup> ed.) Hammer Smith: Harper Collins Limited.
- Interpol (2016). Cybercrime: connecting police for a safer world. Retrieved from <http://www.interpol.com> on 13<sup>th</sup> April, 2022.
- Merton, R. K. (1968). *Social theory and social structure*, enlarged edition. New York, Free press.
- Mshana, J. A. (2015) *Cybercrime: An empirical study of its impact in the society- a case study of Tanzania*. *Huria Journal of Open University Tanzania*, 19 (1), 72-87, 2015.
- Murphy, D.S. & Robinson, M.B., (2008). *The Maximizer: Clarifying Merton's theories of anomie and strain*. *Theoretical Criminology*, 12(4), 501-521.
- Odo, C. R., & Odo, A. I. (2015). The extent of involvement in cybercrime activities among students' in tertiary institutions in Enugu State of Nigeria. *Global Journal of Computer Science and Technology: Information & Technology*, 15(3), 1-6.
- Olaide, M. & Adewale, R. (2004). Cyber crime embarrassing for victims. Retrieved on 12<sup>th</sup> September 2021 from <http://www.heraldsun.com.au>

Oyesanya, F (2015). *Nigerian Internet 419 on the loose*. USA: Gettysburg PA.

Social Development Policy for Nigeria (1980). Federal Republic of Nigeria, Lagos. Retrieved from <http://www.womenaffairs.gov.ng> on 14th of January, 2022.

Spiegel, S.N., (2006). *Criminology*. Oxford: Blackwell Publishing Ltd.

Sutherland, E. H (1960). *A theory of differential association. Criminological theory: Past to present*. New York City: Columbia University Press.

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

Umeozulu, F. (2012). Perception of cybercrime among Nigerian youths, *Unpublished B.Sc. Project, Department of Mass Communication, Caritas University*.

Yamane, T. (1967). *Statistics: An introductory analysis*, (2<sup>nd</sup> ed.), New York: Harper and Row.