ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Communicating Cybercrime Proliferation in Nigeria's Recession Since 2015: A Study of Youths Awareness, Knowledge and Attitude in Enugu State.

Chioma Njoku (PhD)

Senior Lecturer, School of Media and Communication. Pan-Atlantic University, Km 52, Ibeju-Lekki, Epe, Lagos State, Nigeria

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1408000194

Received: 17 Aug 2025; Accepted: 23 Aug 2025; Published: 24 September

Abstract: This paper is on "Communicating Cybercrime Proliferation in Nigeria Economic Recession since 2015: a case of Enugu State Youths." The general objective is to ascertain the level of knowledge of respondents towards cybercrime engagements in Enugu state Nigeria. It is a cross-sectional study of 384 respondents. The total population of the study is 1.380,000 across various local governments in Enugu State, Nigeria. The work was anchored on "Social Learning Theory". The data was collected using questionnaires. The instrument was administered purposely and analyzed using SPSS version 25.0. The results were presented on simple tables and percentages. The data showed respondents' level of knowledge on cybercrimes was moderate and majority of the respondents believe the inflation rate fluctuations since 2015 in Nigeria necessitated cybercrime engagement intensification by Youths in these regions. Despite the death punishments for cybercrimes culprits globally, many Nigerian youths in this region still engage in various cybercrime activities. The respondent's adoption of several cybercrimes reflects wealth chase and lack of contentment by young people. The various issues resulting in dependence on cybercrimes as a lifestyle is fueled from greed, unhealthy competition, peer pressure, poor institutional management and all these have attributed prevalence nature of deep cybercrime culture. Although the social issues constituted to the reason for cybercrime engagements, the consequences and adverse effects of cybercrimes can shortchange youths' prospects. The work recommends a mailable policy that enshrines crime consequences in school curricular from Primary schools to help curb inherent crime culture in the teeming youths.

Key Words: Cybercrime, proliferation, youths. Cyberspace, online scamming, recession

I. Introduction

Cybercrime in recent times is fast posing more threats across the globe and nations are battling tirelessly to curb its glaring damages. Unfortunately, more youths are caught on the web of cybercrimes especially since more businesses are tilting towards the digital space. The rampant fraudulent e-commerce transaction phenomenon adopted by youths globally poses a serious security threat to governments, institutions, all and sundry. Ironically, many young Nigerians have mastered various crime arts since the advent of technology. The various crafted niches in online activities majoring in swindling millions across board from innocent individuals across border has become a celebrated culture in today's world.

Prevalent of cybercrimes reflects how fast our culture values are easily eroded. News of crimes committed by Nigerians youths have become a bothering concern to many. Sadly, millennia and Gen-Z's have mastered various cybercrime acts with ease. The FBI Internet Crime Complaint Center (IC3) recently documented that 2024 highlighted about $16.6billion loss resulting from internet crimes and this report added to a 33% increase on internet with respite to the 2023 statistics.

About $16.6billion loss of $19.372 per complaint is the record on FBI file. The top crimes outlines are phishing/ spoofing recording about 193,407 complaints, extortion 86,415 complaints, personal data breaches of 64,882 complaints, cryptocurrency related crimes statistics are about 150,000 complaints accounting for $9.3 losses. Investment fraud losses exceeded $6.5 billion, especially digital assets related to fraud.

Sadly, cybercrime targets all demographics including the elderly groups who are most vulnerable and easily fall victims as their entire pension and retirement benefits are usually swept in splits of seconds by fraudsters.

Unfortunately, about 147,127 retirees are affected with $4.8 billion losses to cybercrimes. Each year an avalanche of dynamic cybersecurity exploitations opens. Recently, Ransomware variants of 67 variants were identified in 2024 including FOG, Lynx, Cicada 3301, Dragon force and frag all targeted at healthcare sector in 2023, (2024 FBI Internet Crime Report).

The annual incessant culture of Nigerian higher institution's strike seems to encourage more young people in losing hopes in the relevance of acquiring education, hence the greater and deep necked involvement in cybercrime activities in Nigeria.

Ridiculously, despite global society's online weaponry and sophistication, combating cybercrimes has posed a daunting task with all the available security apparatuses and arsenals. The huge consequences of online theft sapping different economies have become a unifying force for fighting cybercrimes worldwide. Some common online crimes practiced in this region include hacking people's bank accounts, privacy invasion to take over their social media platforms and swindle money from their mutual friends, sending codes to WhatsApp groups to extort money from vulnerable individuals, swindling money from heavy online stores clients,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

scamming vulnerable online daters, naïve online reliance groups, online client's dependence, etc. Although the COVID-9 pandemic paved way for online reliance, dubious youths' have created rooms for themselves in leveraging online opportunities for other crimes.

With huge records of numerous online cases negatively featuring youths' indulgence in daily crimes, it has become imperative for Nations to devise better ways of resolving the cybercrimes narratives peculiar to their terrain. Although crime is universally defined but the advent of internet has brought a new tweak to the way young people commit crimes today. Globally, it has become imperative to consider efficient measures of curbing cybercrime menace threatening many Continents today. The trend in criminality and online display of wealth seem to be more rampant amongst young people of African descent. The global image of Nigeria is a serious worldwide discuss as more youths are captured daily in diverse crimes.

With the oil crash in 2016, Nigeria economy suffers huge loss as an oil dependent Country as the Nation contracted 2.06% between April and June 2016. As crude oil sales account for 70% of government revenue, the fall of oil prices from $112 per barrel to $50 per barrel in 2014 accounts for the recession. (BBC August 31, 2016).

The exchange rate in Naira to dollar on February 12, 2015, jumped to N204.3373 as against N162.66 on January 31, 2014. The incessant leap of dollar to naira became an issue many Nigerians had to battle with. These sad incidents crept subtly, and many youths started looking for ways to survive and with their quest to amass more wealth, the need to explore online platforms to make more money became a culture spread across many.

Ironically, the Nigerian environment where government negate relevant sectors that engage youths' especially the educational sector that design more proactive curricular for young minds constantly fail in their role of tackling internal and external crisis that constantly erupts in the way needs of the staff are not handled. The sad narrative that thrills Nigerian government and the Labour Party as the perennial Academic Staff Union of Universities (ASUU) absorbing millions of teeming young people. The culture of disregarding integrity and hard work, however, erodes with ease as society continually applauds wealth displays rather than throwing weight behind individuals whose consistency and track record over the years can be trusted in doing quality business. In Africa, the celebration of wealth not minding how it was acquired has become as integrity seems to be downplayed. Unfortunately, youths all over are more captivated by the avalanche display of luxurious lifestyle seen on the internet.

The Federal Bureau of Investigation (FBI) arrest of famous Nigerian Instagram sensation, Ramon Olorunwa Abbas called (A.K. A) Hushpuppy opened more grounds for lots of dubious activities indulged by more Nigerian youths. Sadly, the #ENDSARS# controversies were instigated by Nigerian police concern of churns of youths' involvement in crime. Eventually, the jet age online culture has succeeded in paving way for diverse cybercrimes. Unfortunately, the accolades given to people who amass wealth in questionable manners predispose many youths to online crimes. Although cybercrime focus seems to appeal more to young people, there are also advanced people who appear to target mostly scamming vulnerable groups and organisations through well-crafted mechanisms. Statistically, the financial crime committed mostly seems to be common amongst young people within 22- 35 years. The most common internet crime across borders of the world is alarming and have been normalised in certain regions of which Africans seem have more prevalent cases of. The offshoot of cybercrime increases more during the COVID-19 era where internet became the only potent tool of survival by many. Sadly, society's role in applauding wealth more than character and hard work gave room for more crime. The online display of properties and money acquisition as the relevant measuring scale of success contributed hugely to attracting more youngsters in internet crime. Celebrating those lavishly stolen money or ill-gotten as trend as basis measure of successful life created avenue for incessant cybercrime the world over. The general practice and promotion of online activities has ruined the major objective of electronic communication interconnectivity agenda of the global village ideology. World of today's computer age, a global universal trend unifying all mortals, is causing more crime than yielding positive results. This seems to be against the anticipated desire of the global village ideology channeled by Marshall McLuhan, (2017), the propounded of the theory. In his infamous phrase, 'the medium is the message' views the media which is basically human recent internet dependency as completely overtaking man. The promotion of cybercrime in voracious magnitude with high severity trickling down to societies at the speed of light especially in this global marketplace of ideas propagated by the digital communication of ITU and global village ideology of Marshal McLuhan,

More so, it has become a world of fierce battle with each concerned nation deliberately strategizing on how best to handle this phenomenal disruption. The proliferation of cybercrime recorded in recent times within the globe has created major and disturbing concern for individuals, families, organisations, industries, religious groups, Li, Z. and Lioa, O. (2018).

Furthermore, investors, learning institutions, security departments, intelligent agencies and the world at large result in high crime rate. The effect has taken a sharp negative shift distilling in such a geometric magnitude beyond men's expectation. The impact of such crime escalation is in triple folds as experienced on daily basis across societies with an everyday increasing typo by the youths who are the most active users in this cybercrime involvement and norm, Wolf, J. (2013).

In this paper provided an over-view of cybercrime practices amongst youths within the Southeast geo-political zone of Nigeria who are actively reliant of all forms of crime to survive in the biting economy, especially those who are the most active on the internet. This inquiry sort to know how the level of knowledge and awareness youths have as regarding cybercrimes and its implications. It explored how Internet knowledge has helped shaped online attitudes and involvement of Nigerian youth currently hearing the myriads of death sentences pronounced on culprits all over the world, (Journal of law and globalization, 2014).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Enumerating the most common trending online businesses in today's world brings to focus that about 90 percent of businesses are basically traded online ranging from forex trading, financial transactions, communication of variant forms, etc. calls for deliberate attention to handle pertinent issues to ensure cyber related issues are adequately curtailed. (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014).

There are many victims of the popular Ponzi scheme called "MMM" that drained Nigeria finances in 2015 rendering many bankrupts. However, studies have proven that lots of other online gambling still exists as youths hugely get involved. According to the Nigeria's communication commission in 2015, Nigeria ranks among the worse Countries suffering from cybercrimes as about 91.6 million of the population are certified active internet users. This critical factor hinders Africa's economic growth (Vanguard, August 8, 2017).

It is no news that Nigerian youths dominate the cyber space doing all manner of activities but there is also a huge disconnect from those young minds who leverage on the web space for personal developmental projects and positive activities. Ironically, there are others who engage in fraudulent activities of all kinds. Nigerian youths seem to be playing big roles in the crime scene especially with the Ramon Abbas Federal Bureau of Investigation (FBI) case currently. Such negative big role has continually damaged the image of Nigerians in diaspora and would continue to raise more controversies until critical measures is put into place to checkmate the ill activities. Smith, (2015). Again, there has been a change in the people who attack computer networks away from the "bragging hacker" towards those driven by monetary motives. A deeper analysis of the phenomenon itself has taken place as more sophisticated technical tools have emerged, making the detection of hackers quite difficult for law enforcement authorities globally. In recent times, Nigeria seems to have ranked ridiculously poor in various global ratings of corruption and crime cases. The money laundering saga of most public office holders adds A study by Institute of Digital Communication, (2001) market research based in South Africa reveal Nigeria lose about $80 million dollars annually to software piracy alone as about 90 % of online crimes are traceable to the same Country. Also, there is a high record of impact crime rate per capital ranked exceptionally high. As Nigeria imagine is questionable on the global sphere annually, there is need to redeem the tarnished identity resulting from her citizens gross involvement in all manner of cybercrime annually. Some of this engagement includes email scams where deceptive pictures are painted to the victims to lure them into getting involved in financial scams. (McCusker, 2006). Furthermore, illustrates that the synergy between the Internet and organized crime is a natural tendency and is likely to develop further in the future. In a bid to curb this abnormality in our Nation Nigeria, there is need for urgent and deliberate tactics to handle this evil. Hence putting into consideration proactive and strategic measures in place of this growing phenomenon becomes essential. There appear to be little or no effort to proffer solution to this harassment causing great damage to the Nation. This study therefore looks at the awareness, knowledge and attitudes of youths in Enugu South-east on this issue, which is wreaking havoc.

More so, technology and communication become a global affair shifting peoples' value and regard from intra and interpersonal communication systems to a more web dependent lifestyle because more people increasingly take internet indulgence more serious than live and one-on-one relationships, (Lavorgna, 2015). It therefore surfaces to easily say that the Internet appears to be the most potent platform in man's history. It presents the need to manage various forms of cyber abuses that generally flow on the internet especially, as the youths, who seem to be the most difficult to satisfy keep engaging and perpetrating more abominable evil in their quest of making gains to satisfy their curiosity not minding "whose ox is gorged." (Lusthaus, 2013).

Nations of the world now see the need to fight cybercrime escalating from different quarters because the youths who instigate this evil damn the consequences of their actions. This growing trend has become a norm posing global problems and leading to loss of lives and resources in measures innumerable to quantify, (Hutchings, 2014; Lavorgna, 2015; Leukfeldt et al., 2016; Lusthaus, 2013).

This influx of crime dissipating from the West is posing too many dangers to lives, loss of privacy as hackers become more dubious, devising unfathomable strategies as means of extorting, duping innocent people and enriching themselves regularly via aggressive attacks, breaking into terrain of security classified information just to get rich fast, (Lavorgna & Sergi, 2016).

Scamming, the most common among cybercrime has become the order of the day. It is important to point out that millions of resources have been lost globally to Internet fraudulent activities with each nation having a share in peculiar manner. In Nigeria, various fraudsters are being paraded at intervals occasionally, an approach that have not resolved the temerity of the crime. It becomes more obvious that crime increases daily not minding the present recession faced by Nigeria economy since 2016. The most notable of them all is the most popular "Ponzi scheme" "MMM" which took the lead amongst other schemes defrauding Nigerians of millions in December 2016 an issue still ongoing even at this moment, partially in the cyber landscape (Broadhurst et al., 2014; Leukfeldt et al., 2016).

Notwithstanding, the advent of information and communication technology (ICT), has undoubtedly brought ample improvements in our day-to-day activities and involvements. It is a major factor on which the world depends to build economic growth, innovation and social development. Worldwide people utilize electronic communications in trade and development across different nations and continents effectively with minimal human displacement, McGuire (2012).

Over the years, electronic commerce (e-commerce) has increased tremendously with remarkable positive impacts on diplomatic, trade and developmental ties between different nations, (Sui, Caverlee, & Rudesill, 2015).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Furthermore, consumers of ICT are extensive and diversified in attitude and usage. Those with perverse minds have not ceased working to exploit the innovation of ICT for selfish and wicked purposes at the detriment of others who must have cooperated on mutual trust basis in e-business or otherwise. Their activities are illegal and deserve urgent attention as all nations are vulnerable with adverse consequences on global economy, (Ciancaglini, Balduzzi, Goncharov, & McArdle, 2013).

In Nigeria, perpetrators of illegal activities via irresponsible or abusive use of ICT, have shifted or augmented their attention from cyber watching of illicit videos to young people especially female youths being involved in internet fraud (scamming), both of which are very devastating criminal acts, (Sui et al., 2015).

Our economic and development relationships with nations whose residents have fallen victims are unsafe or at stake. Thus, the cheap mobile data and almost zero broadband have necessitated the increased cybercrimes activities in Nigeria, Ciancaglini et al. (2013)

The ease of access and availability of data has created more room for scamming in Nigeria, and we cannot deny the deplorable damages scamming has inflicted on us. Such data on the present and future destructions on citizens and the State, induced by internet crimes and frauds (ICF) is acute.

It is also vital to buttress the assessments on levels of contamination, involvement, participation and adoption of variant degrees of cybercrime in operation today in Nations of which Nigerian youths have become globally famous and experts in an outrageous manner beyond human comprehension. This ugly trend requires an urgent approach to redress to bring sanity into our system and secure the cyber space if Nigeria image can be redeemed globally. It is pertinent to address such criminal acts, eating deep into our system and capturing the most vibrant and active brain upon which our society's potential depends, Kigerl, (2016).

This singular reason calls for alternative activities to distract their attention and engage them in more meaningful skills to secure their future. (Cyber Crime Assessment, 2016).

Statement of The Problem

The active involvement of Nigerian youths in scamming activities has become the reason many global investors seem not to spread their businesses towards the African most populous regions. It is no news that Nigeria has lost her crown from the Big Brother it is known for in recent times. The major reason is the rate at which cybercrimes are celebrated in a "get rich culture of many youths today. Record has it that Nigerian terrain is prone to vulnerable demographics who are easily susceptible to the porous nature of cyber activities.

Record has it that an estimation of about $1trillion is lost to cybersecurity annually globally. About $568, 654, 974 is lost yearly to various cybercrimes including the healthcare sectors. Several reports on cybercrimes are spread across various news channels amounting to $239,247 losses scores contributing to over 12.1% inclusive on yearly statistics of cybercrime proliferations. Cybercrimes range from financial investment scams, dating & romance, privacy invasion, financial compromise of online transactions, false billing, phishing, remote access scams, threats to lives, identity thefts, jobs & employment scams, classified scams, rebate scams, etc.

In Africa alone, there seems to be high prevalence of this virus eating deep into the fabrics of our society, particularly as young people actively engage in online activities and have devised measures of swindling money from people with ease. Ironically, cybersecurity targets all demographics and many easily fall prey to their gimmicks for several reasons and dynamic presentations of the invaders. Cybercrime victims are trapped daily in all manners and curbing menace has become a daunting tasks security agencies the world-over are not able to tackle. Sadly, most online users are not sensitized properly regarding how to navigate through the internet with caution. A lot of users do not understand the dynamic nature of invades so, the incessant invasive nature of privacy breach needs to be addressed especially in Nigerian. Hence, this worked looked at the ways to ascertain the level of knowledge of respondents towards Communicating Cybercrime proliferation in Nigeria economic recession since 2015: A case of Enugu State Nigeria". This inquiry Investigate trends of cybercrimes indulgence amongst youths in Enugu State, Nigeria; evaluate common cybercrime engagements amongst respondents; assess economic impact of recession necessitating cybercrime proliferations amongst respondents. The following research is explored; What is the level of awareness of Enugu youths towards cybercrimes. What is the level of knowledge of Enugu youths on cybercrimes? What is the perception of Enugu State Youths towards online cybercrimes?

Significance of The Study

Nigeria is the commercial nerve center of Africa and the most populous nation with horrible history of endemic leadership corruption from time immemorial. The environment of hardship presents options of survival which range from anything that can sustain one's life. Such inquisitive nature appears hereditary in an average Nigeria's ideology. The corruption in governance in this part of the world propels individuals to survive under any hash condition including making cybercrime the most lucrative avenue to resort to.

Individuals willingly take any form of risk to earn a living especially as recession that hit Nigeria since the administration of President Mohammadu Buhari is still lingering. it is so easier for an average Nigerian to devise means of survival not minding the consequences of the indulgence, yet at the beginning of internet developmental stage, there were already the existence of the popular

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

"419" trend which keeps waxing strong daily as youths seem to be the most active internet users who dominate the online sites scouting for people to defraud, Beran and Li (2005).

Several reports have associated variety of scams with Nigerian as the origin. Laws that cover ICF in general and scamming in particular are minimal and not marked with stringent penalty even there is any existing at all in the Country. Studies on ICF to find out the extent to which students and youths have been contaminated by the 'scamming syndrome' and putting in place appropriate intervention strategies to enhance existing measures via diverting attention are exigent at this point.

Looking at the rate Nigerian democratic aspirants promote cybercrime through throwing money to lure electorates and vote buying, it becomes pertinent to caution young people on the essence of upholding their cultural values. Corruption practices seem to be part of the encouraging factors that promote corruption in Nigeria.

The Study Location

This work was carried out in Southeast geo-political zone of Nigeria. It is a very popular ancient city known as "Cold city" because of the temperate nature of the terrain. As a peculiar region of Nigeria is on the South pole of the African most populous nation, the people are known for their trading and business investment of all times. The people are referred to as the Israelis of Nigeria as they constantly position themselves in ways that distinguishes them as the most envied in the entire Country. This location is strategically chosen because it is primarily dominated by the Igbo tribe who are known typically for doing business and engage in various trades. This region has population of over 80 million with majority of their youth actively engaged in both online and offline e-business. However, this location has an approximate population of 4.9 million people as of 2025 with an annual growth rate of 3.5%. The population is broken down as follows: 0-14 years, 1.5 million, 15-24, 1.2 million, 25-54 1.8 million and 55 years and above estimated at 400,000. Gender statistics shows male at 2.35 million whereas, female are projected to be 2.55 million. It is a relatively peaceful region known for commercial activities contributing to the Countries' Gross Domestic Product extensively and voraciously. The choice of this region is because of its business inclination which ultimately makes it susceptible and prone to cybercrimes.

Brief History of Ponzi Schemein Nigeria

After the MMM Ponzi scheme crashed in 2016, several other investment schemes promising high interest rates were liquidated making Nigerians the most prone to unverifiable subscribers to illegitimate with massive financial losses. Sadly, few months after MMM, "Ultimate cycle came onboard with a mouthwatering rate on investments pegged at 400%. This promise did not last as was shut down abruptly after collecting funds from thousands of Nigerians who paid $9 each in their cluster.

Twinkas also came on board with a promise of 400% return on investment but suddenly packed up after new sign-ups softly peddled and this left many participants frustrated as they could not cash out their investments.

"D9" sprang up after the collapse of Twinkas. However, it came with different strategies of global sports betting to generate profits and share amongst participants. But it also collected about $7.8million dollars and fizzled out like air.

Then, "MBA Forex Trading and Capital Investment Limited surfaced with 15% returns on investment but also crashed after collecting $138.45 million from vulnerable Citizens. However, the Chairman Executive Director of MBA Forex Trading and capital, Maxwell Odum was declared wanted by Economic and Financial Crimes Commission (EFCC) but the money was never refunded to the victims.

- *MBA Forex Trading and Capital Investment Limited*: Promised 15% returns on investment but crashed after collecting N213 billion from Nigerians. The CEO, Maxwell Odum, was declared wanted by the Economic and Financial Crimes Commission (EFCC). "Famzhi Interbiz Limited also came with its baggage of 30% monthly returns. Although this was deemed illegal by the Security and Exchange Commission, (SEC), the outlets had already swindled Nigerians of over $19.5 Million losses.

"Chinmark Group" also resurfaced with a promise of 3% monthly returns but was found guilty as he could not pay up the money he promised, and this led to a massive loss of $26m Million of Nigerians hard earned monies. The CEO Mark Chinedu faced public backlash and scrutiny that was eventually not fruitful because the public fund was not recovered.

Then came the most strategic scheme known as "Ovaioza Farm Produce Storage Business. This farming scheme came with a lucrative positioning to carter for the most concerning needs and sector of the economy which was the food industry to feed the teeming hungry Nigerians. This was a welcome investment by many because of what it promised to offer. It ended up becoming statistics like others and recorded a loss of over $1.95 million from vulnerable Nigerians. Although it came with huge promises that was an illusion after the 70% promised was not delivered and people were swindled as usual.

Then "Brisk Capital promised 30% monthly return on investment yet liquidated within months abandoning investors with huge loss of $1.3 Million. Unfortunately, Nigerian never get a hold of themselves as each Ponzi always get investors. Crypto Bridge Exchange popularly known as "CBEX" launched its AI powered crypto trading and captured almost the active users. It came with unflinching promises but came crashing withing months of its existence. Sadly, it also crashed in April 2025 trapping many whose losses is counted in over six figures accounting to about $848,111.111. This last stride is the most traumatic investment downturn for Nigerians in general.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Internet Crimes and Frauds

The exact meaning of cybercrimes (ICF) may be very cumbersome, but being a popular term, it has been used by many authors to describe the illegal activities related to the internet world or cyber space while others define cybercrimes using the various constituent aspects (Olowu, 2009).

For example, according to the Federal Bureau of Investigations (FBI), cybercrimes span across a diverse scenario including crimes against children (usually involving child pornography or child rape); theft of intellectual properties, publications, intentional dissemination of malware to national and international internet fraud (FBI, 2005).

Casey (2004) considers internet crimes and frauds to be "any crime that involves computers and networks, including crimes that do not rely heavily on computers". Considering the Internet crime complaint center (ICCC), "internet crime is any illegal activity involving one or more components of the Internet, such as websites, chat rooms, e-mail and any other platform that connect people who do not know themselves live nor have had personal connection or any form.

Internet crime involves the use of the internet to communicate false or fraudulent representations to consumers. These crimes may include, but are not limited to, advance-fee schemes, non-delivery of goods or services, computer hacking, or employment business connections, human emotional relationships especially that which exist between the opposite sex, any form of online transaction that cannot be verifiable, opportunity schemes" like Ponzi and the likes etc.., Anti- Phishing Working Group, (2016).

Consistent with the above definition, the legal dictionary of The Free Dictionary website by Farlex, defines internet crime as "a crime in which the perpetrator develops a scheme using one or more elements of the internet to deprive a person of property or any interest, estate, or right by a false representation of a matter of fact, whether by providing misleading information or by concealment of information".

According to the former President of Nigeria, Olusegun Obasanjo, West Africa (BBC, 2003) the various financial scams known as "419" fraud or internet scam which is originating but not limited to Nigeria (Oriola, 2005) are the event where people overseas willfully provide their bank account details in response to promises of huge non-existing riches, which are resultantly liquidated.

Meanwhile different authors and scholars have definitions for Internet Crime Fraud (ICF) depending on their context and cultural underpinnings. Sadly, the context have different connotations in Africa and in Nigeria because it appears the terrain is a safe site for cyber-criminals (Mutume, 2007) probably because of the cheap cost of site registration and inadequate security awareness (McAfee, 2010), making it safer for perpetrators. Also lack of awareness of existing policies and procedures to protecting privacy is a serious battle many faces in Nigeria

After Nigeria topped the list as Worlds' most malicious site for internet browsing (Ribadu, 2007), it was the fair share of Cameroon in early 2010 (McAfee, 2010). The ever-increasing unemployment rate in several African countries (most of whom are graduates, very proficient in the use of computer and Internet) is probably the influencing factor of the existence and growth of cyber-crimes (Olowu, 2009).

According to the WB (2008), instability in Africa will continue to be on the rise but might be arrested or controlled by generating an estimated 100 million new job opportunities by the year 2020. In Nigeria, illegal activities propagated by negative exploitation of the ICT have several characteristics (with new types emerging every day) depending on who and where the target is located on the globe. For example, there are numerous people mostly youths being paraded at intervals by the Economic and Financial Crime Commission (EFCC) culprits of cyber violations of variant magnitude ranging from rape, murder, money laundering, hacking and such crimes are described in range of versions; scamming originating from the popular fraudulent generally called "419." There is also the child adoption scams rampant in big cities in Nigeria where the domestic helps are the most involved; the rampant job scams where the unemployed youths are been extorted and business scams (involving vegetable oils wishing to supply raw materials for bio-fuels industries), car dealings that are posted regularly by acclaimed customer officials with never-ending strings requesting money from the victims on constant basis, (APWG, 2016).

We may further classify scams stemming from Nigeria according to their targets as external target scams (scamming people abroad) in business and marriage proposal especially the younger men promising more advanced white women of marriage and internal target scams (aimed at scamming Nigerians at home). Recently, over 120 suspected fraudsters have arrested by Economic and Financial crime commission (EFCC) with 95 males and 25 females in Lagos and about 26 exotic cars and expensive jewelry. The popular Cynthia… that was killed in FESTAC town Lagos Nigeria went viral and lots of others been duped by Internet scammers who easily brain wash the women most vulnerable and lots of other heinous crimes committed. Internet impersonation scams (claiming to be either government officials or approved by government of Nigeria), identity scams (fraudulent phone calls to people in different nations using telephone codes of different nations while calling from Nigeria giving the impression of being elsewhere).The activities are numerous including sending mails of bank updates and jobs, asking jobless youths to pay certain amount of money to get a job, amongst others.

On the other hand, internal target scams (ITS) to which several citizens are victims include amongst others telephone scams (fraudulent phone calls), computer hacking, e-mail address impersonation scams (hijacking someone else's e-mail account,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

changing the password and use it to extort money from available contacts), hypnotic scams. The crimes are uncountable which every day springing up of new techniques of defrauding people, Smith, Smith & Smith, 2011).

Cybercrime: Crimes that use computer networks or devices to advance other ends include Fraud and identity theft, (although this increasingly uses malware, hacking and phishing, making it an example of both "Computers as target" and "computer as tool "crime) Information warfare. Phishing scams, (APWG, 2016).

Economic Recession

It is a period of general economic decline and is typically accompanied by a drop in the stock market, an increase in unemployment and decline in the housing market. Generally, a recession is less severe than depression.

Ponzi scheme: A form of fraud in which belief in the success of a non-existent enterprise is fostered by the payment of quick returns to the first investors from money invested by later investors. "A classis Ponzi scheme built on treachery and lies." (Jaishankar,2008, pp. 292-296; Jaishankar, 2018).

Effects of Cybercrime

The evolving significance of cyber security calls for the practice of protecting computer systems from cybercrimes attacks from both physical and digital by unauthorized sources or humans who constantly launch attacks on innocent online users. It is pertinent to reduce the risk of cybercrimes as hackers strategically find new ways of accessing, changing or deleting sensitive information and scamming anyone who falls into their trip. Hence, this investigation would add to the body of existing and sensitize more people to the tricks and tactics employed by fraudulent groups online. Ironically, people are swindled at an alarming rate and need to be properly educated on what signs to detect when any form of smart mental play is carried out by cybercrimes. Again, internet policy makers should focus on areas that protect users' privacy or alert them when an activity is dubious.

This study investigated extent of cybercrime engagements of Nigerian youths with relevance to the implications it poses to the Nigerians' if left unattended to seeing the danger it poses to the owing to the trickling statistics of Nigerian youths' indulgence. Ironically, the present hardship that has persisted for a decade has taken its turn in promoting myriads of cybercrime involvement as a survival strategy seeing the rate at which unverified investments infiltrate the economy with scrutiny by the financial regulations. The crash of the popular "MMM" that failed in 2016 fostered cybercrime activities on a different pedestal. It was recorded that the MMM Ponzi swindled Nigerians over $50 million before its crashed in December 15, 2016, (NDIC International fair, 2017). The scheme founded by Russian fraudster, Sergei Mavrodi promised investors 30% return on investment in a peer-to-peer donation model. This model attracted over three million Nigerian investors. Various on accounted crimes have occurred without checks on the financial institutions in Nigeria paying attention to the protecting the interest of the public. However, the Central bank of Nigeria estimated the lost at 12 billion naira.

In Nigeria however, there appear to be numerous cybercrimes ranging from "yahoo boys" phenomenon, online account hacking, software piracy, pornography, credit card or ATM fraud, denial of service attacks, virus dissemination, phishing and lots of others.

II. Methods

To calculate the sample size for a population of 1.380 million using Onwuamalam Sampling calculator.

$n = (Z^2 * p * (1-p)) / E^2$

Where:

- n = sample size

- Z = Z-score (confidence level)

- p = population proportion (0.5 for maximum variability)

- E = margin of error

Using 95% confidence level (Z = 1.96) and a 5% margin of error (E = 0.05).

$n = (1.96^2 * 0.5 * (1-0.5)) / 0.05^2$

$n = (3.8416 * 0.25) / 0.0025$

$n = 384.16$

For a population of 1.380 million, the sample size would be approximately 384.

However, if the population is finite, we can use the formula:

$n = (N * Z^2 * p * (1-p)) / (N * E^2 + Z^2 * p * (1-p))$

Where N = population size (1,380,000).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Plug in the numbers:

$n = (1{,}380{,}000 * 1.96^2 * 0.5 * (1-0.5)) / (1{,}380{,}000 * 0.05^2 + 1.96^2 * 0.5 * (1-0.5))$

$n \approx 384$

Data Analysis and Discussions of Findings

III. Results

Table 1: Frequencies and Percentages of the Demographic Information of Respondents.

SN	Age of Respondents	Frequency	Percentage (%)
1	18-24 years	85	22.1%
2	25-30 years	115	30.0%
3	31-35 years	101	26.3%
4	36 years and above	83	21.6%
	Total	**384**	**100%**
SN	**Gender of Respondents**	**Frequency**	**Percentage (%)**
1	Male	189	49.2%
2	Female	195	50.8%
	Total	**384**	**100%**
SN	**Educational Level**	**Frequency**	**Percentage (%)**
1	Secondary school	44	11.5%
2	Diploma/NCE	96	25.0%
3	Bachelor's degree	132	34.4%
4	Master's degree and above	112	29.1%
	Total	**384**	**100%**
SN	**Occupation**	**Frequency**	**Percentage (%)**
1	Employed	99	25.8%
2	Unemployed	121	31.5%
3	Student	84	21.9%
4	Trader	50	13.0%
5	Remote	30	7.8%
		384	**100%**

From Table 1, the demographic characteristics of the respondents indicate that the sample was largely composed of young adults, with 30.0% aged 25-30 years and 26.3% within 31-35 years, while 22.1% fell between 18-24 years and 21.6% were 36 years and above. The gender distribution was almost evenly balanced, comprising 49.2% male and 50.8% female respondents. In terms of education, the findings reveal a relatively high level of attainment, as 34.4% possessed a bachelor's degree, 29.1% held a master's degree or higher, 25.0% had a diploma/NCE, and only 11.5% had completed secondary school. With regard to occupation, the result shows that 31.5% of the respondents were unemployed, 25.8% were employed, 21.9% were students, 13.0% were traders, and 7.8% worked remotely, reflecting a diverse occupational spread but with unemployment constituting the largest category.

Research Question One: What is the level of awareness of Enugu youths towards cybercrimes?

Table 2: Mean and standard deviation on the level of awareness of Enugu youths towards cybercrimes

	STATEMENT	N	Mean	SD	Remark
1	I am aware that cybercrimes are online activities like fraud, scamming, fake romantic promises, hacking, and identity theft.	384	4.53	0.50	A

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

2	I am aware that many cybercrimes are carried out through emails, social media, and online banking platforms.	384	4.60	0.49	A
3	I am aware that some youths justify cybercrimes as a way of surviving unemployment.	384	4.42	0.49	A
4	I often come across news, social media posts, or campaigns that talk about cybercrimes in Nigeria.	384	4.47	0.55	A
5	I am aware of the negative consequences of cybercrimes on victims such as financial loss or emotional distress.	384	4.45	0.52	A
6	I know that cybercrimes damage Nigeria's reputation internationally.	384	4.52	0.50	A
7	I am aware that youths in Enugu State are commonly involved in different forms of cybercrimes.	384	4.62	0.48	A
	Cluster Mean	**384**	**4.51**	**0.21**	**A**

The results presented in Table 2 provide insight into Research Question One, which sought to determine the level of awareness of Enugu youths towards cybercrimes. The findings show that respondents demonstrated a very high level of awareness about cybercrime proliferation in Enugu State, with mean scores ranging from 4.42 to 4.62. Notably, the cluster mean of 4.51 with a standard deviation of 0.21 indicates that, on average, respondents strongly agreed with the statements measuring awareness. This suggests that Enugu youths are highly aware of the nature of cybercrimes, the platforms through which they occur, the justifications often given, and their consequences on individuals, society, and Nigeria's global reputation. Therefore, the result affirms that the youths in Enugu State possess a high level of awareness regarding cybercrimes.

Research Question Two: What is the level of knowledge of Enugu youths on cybercrimes?

Table 3: Mean and standard deviation on the level of knowledge of Enugu youths on cybercrimes

	STATEMENT	**N**	**Mean**	**SD**	**Remark**
1	I can correctly identify different types of cybercrimes such as hacking, identity theft, and online scams.	384	4.46	0.49	A
2	I know that online impersonation (using another person's identity) is considered a form of cybercrime.	384	4.51	0.50	A
3	I understand that creating or spreading harmful software (viruses, malware) is a cybercrime.	384	4.51	0.50	A
4	I am knowledgeable about the penalties for committing cybercrimes under Nigerian law.	384	4.55	0.58	A
5	I know that cybercrimes can have both financial and psychological impacts on victims.	384	4.46	0.58	A
6	I can differentiate between legitimate online activities (e.g., e-commerce) and fraudulent ones (e.g., fake websites, Ponzi schemes).	384	4.48	0.58	A
7	I know that reporting suspected cybercrimes culprits to legitimate authorities is the right action to take.	384	4.56	0.58	A
	Cluster Mean	**384**	**4.50**	**0.26**	**A**

The results presented in Table 3 address Research Question Two, which sought to determine the level of knowledge of Enugu youths on cybercrimes proliferation. The results reveal that respondents exhibited a very high level of knowledge, with mean scores ranging from 4.46 to 4.56 across all items. Specifically, the respondents indicated strong knowledge of the various types of cybercrimes, their methods, associated penalties under Nigerian law, and the impacts these crimes have on victims. They also demonstrated awareness of the need to differentiate between legitimate and fraudulent online activities, as well as the importance of reporting cybercrime offenders to appropriate authorities. The cluster mean of 4.50 with a standard deviation of 0.26, further confirms that, on average, respondents strongly agreed with the statements measuring knowledge about cybercrime in Enugu State. This finding suggests that Enugu youths possess a high level of knowledge regarding cybercrimes, both in terms of their nature and the legal and social implications.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Research Question Three: What is the perception of Enugu State Youths towards online cybercrimes?

Table 4: Mean and standard deviation on the perception of Enugu State Youths towards online cybercrimes

	STATEMENT	N	Mean	SD	Remark
1	I believe that society indirectly encourages cybercrimes by celebrating wealthy fraudsters.	384	4.66	0.56	A
2	Engaging in online cybercrimes is seen as an acceptable way of making money.	384	4.35	0.56	A
3	I believe that cybercrime negatively affect an individual's image in differently in the society.	384	4.46	0.56	A
4	Cybercrimes is a smart way of making money rather than committing a known crime like criminal gang indulgence.	384	4.40	0.57	A
5	Cybercrimes is a quicker and easier way to make money than legitimate work.	384	4.48	0.56	A
6	I believe that society indirectly encourages cybercrimes by giving accolades and traditional titles as a way of recognizing wealthy fraudsters.	384	4.40	0.60	A
7	Engaging in cybercrimes is no different from other corrupt practices in Nigeria.	384	4.45	0.49	A
	Cluster Mean	**384**	**4.45**	**0.26**	**A**

The results presented in Table 4 address Research Question Three, which examined the perception of Enugu State youths towards online cybercrimes. The findings indicate that respondents generally held strong views on the issue, with mean scores ranging from 4.35 to 4.66. The highest-rated perception was that society indirectly encourages cybercrimes by celebrating wealthy fraudsters ($\bar{x}$ = 4.66, SD = 0.56), while respondents also acknowledged that cybercrimes are often viewed as a quicker or easier way to make money ($\bar{x}$ = 4.48, SD = 0.56) and as comparable to other corrupt practices in Nigeria ($\bar{x}$ = 4.45, SD = 0.49). However, a considerable proportion also perceived cybercrimes as negatively affecting an individual's image in society ($\bar{x}$ = 4.46, SD = 0.56). The cluster mean of 4.45 with a standard deviation of 0.26 indicates an overall strong agreement with the perception statements. This suggests that Enugu State youths recognize both the societal factors that may indirectly promote cybercrimes, and the negative implications associated with engaging in such activities.

IV. Conclusion/ Recommendations

Ironically, cybercrime has become a culture well normalized by youths the world over. It is imperative to secure cyberspace through advocacies on different channels. Having seen that about 80 percent of online users are attacked regularly across the global by the cyber perpetrators according to available data, (NCC, 2017), this calls for urgent need to create more awareness on cyber security, a reason for this work. There seems to be the need for a homogenous legal regulatory framework that will tackle all crime-related fraudsters by attaching stiff and stringent measures to nab perpetrators of cybercrimes. There is need to close the porous cyber space that easily makes people prey to online hackers. Involving cyber experts and stakeholders across the world to deliberate on the best effective approach to curb the crime is expedient. Seeing to it proficient computer experts oversee data protection to ensure all relevant documents and assets are adequately secured. To also deliberately ensure the ease of promotion of cyber security especially with systems and programs that are not highly sophisticated. This work recommends deliberate need for media literacy on impending cybercrime in existence. There is need to launch strategic media campaigns on the dangers trickling from cybercrime indulgence.

References

1. Adesina, O.S. (2012). The negative impact of globalization on Nigeria. International Journal of Humanities and Social Science, 2(15), 193-201.
2. AICPA. (2013). The top five cybercrimes. Durham, NC: AICPA.
3. AICPA. (2017). Top cybercrimes white paper. How CPAS can protect themselves and their clients. Durham, NC:
4. AICPA. APWG. (2014). Phishing activity trends report, APWG, 2nd quarter 2014. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf.
5. Baek, H. (2018). Computer-Specific Parental Management and Online Deviance across Gender in South Korea: A Test of Self-Control Theory. International Journal of Cyber Criminology, 12(1), 68-83.
6. Banathy, B.H. (1994). "Designing educational systems: Creating our future in a changing world". In Systematic change in education, (Eds.) Reigeluth, C.M. and Garfinkle, R.J.27-34. Englewood liffs, NJ: Educational Technology Publications.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

7. Belsey, B. (2004). Cyber bullying. Retrieved from www.cyberbullying.ca. Journal of communicational computing Research, 32(3):265-277.
8. Beran, T. and Li, Q. 2005. Cyber-harassment: A new review of old behaviour.
9. Besag, V.1989. Bullies and Victims in Schools Milton Keynes, England: Open University Press.
10. Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). Organizations and cyber-crime: An analysis of the nature of groups engaged in cyber-crime. International Journal of Cyber Criminology, 8(1), 1-20.
11. Ciancaglini, V., Balduzzi, M., Goncharov, M., & McArdle, R. (2013). Deep web and Cybercrime. Trend micro report. Retrieved from https://www.trendmicro.de/cloudcontent/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf.
12. Cross, D. (2008). Cyber bullying: International comparisons, implications and recommendations. Wurzburg, Germany: Paper presented at the 20th biennial meeting of the International Society for the study of Behavioural development.
13. Cyber Crime Assessment. (2016). Need for a stronger law enforcement and business partnership to fight cyber-crime. NCA Strategic Cyber Industry Group. Davis, R. (2012). Organized crime in a network society. Journal of International Affairs, 66(1), 145-149.
14. Ehimen O. R and Bola A, 'Cybercrimes in Nigeria', Business Intelligence Journal-January 2010 Vol. 3(1): 95
15. Espelage, K. and Holt. (2001). "Bullying and victimization in early adolescence: Peer influences and psychosocial correlates". In Bullying behaviour: Current issues, research and interventions, (Eds.) Geffner, R. and Loring, M. 123-142. New York, NY: Haworth.
16. 2024 FBI Internet Crime Report: American Hospital Association.
17. Fischer, H. (2006). Digital shock: Confronting the new reality, Montreal, Canada: McGill-Queen's University Press.
18. Journal of Law (2014). Policy and Globalization. 23(24).3240-32.
19. Maitanmi, Olusola et' al (2014). "Impact of cyber-crimes on Nigerian Economy" The International Journal of Engineering and Science (IJES).2(4): 47 Available at https??www.theijes.com
20. Olowu, D. (2009). Cyber-crimes and the boundaries of domestic legal responses: Case for an Inclusionary Framework for Africa. Journal of Information. Law and Technology (JILT). 1, 1- 18
21. Ribadu, N. (2007). Cyber-crime and commercial fraud: A Nigerian perspective. Presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL (United Nations Commission on International Trade Law. Vienna- Austria. 9-12 July retrieved from http://www.cnudmi.org/pdf/english/congress/Ribadu_ibrahim.pdf.
22. Sheri A. Dillon et al (1998). "Computer Crimes" National Institute of Justice, U.S. Department of Justice. Criminal Justice Resource Manual 2 (1989)).
23. Wall, D. (2001). Cyber-crimes and the internet. In D. Wall (Ed), Crime and internet. London: Routledge.
24. Oriola, E.O. (2000)." Flooding and Flood Management" In H.I. Jimoh and I.P. Ifabiyi (eds.) Contemporary Issues in Environmental Studies.
25. Vanguard August 8, 2017.
26. Sheri, A. Dillon et al., (1998). "Computer Crimes" National Institute of Justice, U.S. Department of Justice. Criminal Justice Resource Manual 2 (1989).
27. Ehimen O. R and Bola A, 'Cybercrimes in Nigeria', Business Intelligence Journal-January 2010 Vol. 3(1): 95
28. BBC August 31, 2016, https://www.bbc.com/news/business-37228741