

An Empirical Analysis of Youth and Cybercrime in Benin Metropolis, Edo State Nigeria**Omigie Godson Godwin¹ & Chukwudi Priestley Ego²**

1. Department of Social Work, Faculty of Social Sciences, University of Benin, Benin City, Nigeria.

2. Department of Sociology and Anthropology, Faculty of Social Sciences, University of Benin, Benin City, Nigeria
chukwudi.ego@uniben.edu**Abstract**

This study analyses the phenomenon of youth and cybercrime in Benin metropolis. The study sought to examine the various cybercrime committed by youths in Benin metropolis; find out the effect of access to internet technology on cybercrime among youths in Benin metropolis, and examine the control measures of cybercrime among youths in Benin metropolis. The study adopted the routine activity theory to serve as the basis of the research. A cross-sectional research design was adopted for the study. A sample size of 500 respondents was determined and drawn using Taro Yamane sample size determination formula. Multistage sampling technique was employed to select the targeted respondents. The findings of the study revealed that romance and dating scam are the most common forms of cybercrime among youths in Benin Metropolis. The findings further revealed that corruption, bribery, and information leaks within some law enforcement agencies undermine cybercrime control effort by providing protections and advance warning to cyber-criminal syndicates. The study concluded that addressing cybercrime effectively will require more than punitive measure and law enforcement actions; it will necessitate deliberate effort to tackle the root cause of cybercrime. The study therefore recommends, among others measures, that effort should be made to encourage youths who possesses digital literary and internet access to channel this skills into legitimate online ventures and strict monitoring mechanism should be introduced to ensure accountability among law enforcement personnel and officers found engaging in bribery, collusion or leaking operational information should face appropriate disciplinary and legal sanctions.

Keywords: Benin Metropolis, Cybercrime, Theoretical analysis, Nigeria, Youth.**INTRODUCTION**

Cybercrime is any illegally action relating to an information technology infrastructure; including unlawful access; illegal interruption that involves technical means of non-public transmissions of computers data to, from or within a computer system; data meddling that include unauthorised destruction, obliterating, deterioration, modification or clampdown of computer data; system prying that is interfering with the functioning of a computer by inputting, transmitting, damaging deleting, waning, altering or quashing computer data; misuses of devices, falsification (identity thief), and electronic fraud (International Actions Against Cybercrime, 2007). For Maitanmi *et al.*, (2013), cybercrime refers to all activities done with criminal intent in cyberspace, which can be

categorised into crimes against persons, crimes against business and non-business establishment and crimes against the government.

In Nigeria, cybercrime has become the commonest means through which some youths make quick money with little or zero effort at hard work (Omokhabi, 2024). Cybercrime is no longer seen only as a criminal activity. In many cases, it has become part of a growing youth subculture, influenced by access to digital technology, financial hardship, and the need for social identity. In contemporary societies, especially among digitally connected youth populations who are actively online, this constant exposure creates opportunities for learning, sharing, and normalising different online behaviour including cybercrime. Involvement in cybercrime is sometimes shaped by friends, social groups, and the desire to achieve quick financial success. Wall (2021) explains that cybercrime reflect a transformation of traditional criminal behaviour into digitally enabled practices that are often learned, shared, within online and offline social networks. This means cybercrime is not only an individual act but can also develop into a collective cultural practice within certain youth groups.

Akinyemi and Osunwoko (2022) posit that socio-economic factor is one of the driving forces that contribute to youths' involvement in cybercrime as high rates of unemployment and underemployment, combined with limited opportunities for legitimate income generation, create a fertile ground for internet criminal activities. In a culture that often prizes financial success, the lure of quick monetary gain from cybercrime can be particularly appealing, as many youths perceive cybercrime as a viable alternative to traditional employment, often viewing it through a lens of opportunity rather than illegality (Ojedokun, 2017). Also, cultural influences and peer pressure play an instrumental role in shaping the attitudes of youth towards cybercrime as they often form online communities that normalise and even glamorise illicit activities, and the perception of cybercrime as a *modern hustle* is reinforced by popular media and social networks which further exacerbate the activities of cybercrime among the youth in Nigeria (Oyenuga, 2020). Obaro (2014), stated that weak institutional structures and corruption can create an enabling environment for cyber-related crimes to thrive. Many youths possess digital skills but face limited employment opportunities, particularly in urban areas. As a result, some youths perceive cybercrime as a faster and more profitable alternative to conventional employment (Adeniran & Johnson, 2012).

Statement of the Problem

Globally, fraudulent activities have continued to rise alongside the rapid digitalisation of financial systems and everyday transactions. Cybercrime has become one of the most pervasive forms of digital crime in the 21st century and is widely recognised as one of the fastest-growing cyber-enabled offenses worldwide. The transnational and technologically facilitated nature of cybercrime has made it increasingly difficult for law enforcement agencies to control (United Nations Office on Drugs and Crime [UNODC], 2021; European Union Agency for Law Enforcement Cooperation [EUROPOL], 2023). The expansion of internet connectivity, technological innovation, and the widespread use of online financial platforms have significantly increased opportunities for crime. (Leukfeldt & Yar, 2016; Holt, 2020). These technological innovations have lowered the cost and technical barriers to committing crime, allowing offenders to target victims remotely and across national borders. Cybercriminals can reach large and diverse populations while employing various cybercrime scam techniques such as phishing, identity theft, and advance-fee crime (Wall, 2021). Consequently, the growing anonymity associated with global digital networks has contributed to the rapid expansion of cybercrime as a transnational crime. The nature of digital platforms allows cyber offenders to conceal their identities and operate across national boundaries, enabling them to target victims in different countries through schemes such as romance scams and fraudulent investment proposals. These cybercrime activities are further sustained by victim-related factors, including emotional vulnerability, misplaced trust, and financial greed, which increase susceptibility to deception and allow such crimes to flourish within the digital environment (Button, 2017).

Cybercrime among Nigerian youths gained significant momentum in the early to mid-2000s, with its peak occurring around 2010 to 2015 (Omokhabi, 2024). Prior to this time, advance free fraud (popular known as “419 fraud”) in Nigeria was largely carried out by adults, especially men in their late 30s to 50s who used letters, fax machines, and latter telephones to deceive victims. This form of cybercrime became internationally recognized in the 1980s and 1990s, long before internet became common among young people, cybercrime had been prevalent among older generations during this period, when internet cafes and email became widespread in Nigeria in the early 2000s younger individuals aged 15-29 years became increasingly involved, particularly as internet access and email communication grew more widespread. This transition transformed traditional advance-fee fraud into internet based scams commonly referred to as *yahoo yahoo* (Tade & Aliyu, 2011).

There are so many mechanisms adopted by the Nigerian Government to combat cybercrime, which are anchored on a combination of legal institutional, regulatory, and international measures such as the cybercrimes (prohibition, prevention, etc.) Act of 2015, EFCC Act (2004), the money laundering prohibition and prevention act (2022) and the Nigeria data protection act (2023), all these acts strengthen enforcement by targeting financial crimes, tracking illicit financial proceeds, and protecting personal data to reduce identity theft risks (Alemika & Chukwuma, 2020). Despite increased global and national efforts to combat cybercrime, the crime continues to expand, particularly among youths in Benin Metropolis.

Objective of the Study

The study is guided by the following objective which are to:

- i. identify the various cybercrimes committed by youths in Benin Metropolis;
- ii. find out how access to internet technology influence cybercrime among youths in Benin Metropolis;
- iii. examine the control measures of cybercrime among youths in Benin Metropolis.

LITERATURE REVIEW

Concept of Youth

The word Youth is a relative term, which has no universal meaning. In general conception, it connotes the state of being young. The concept varies across societies, cultures, groups, organisations and countries. Youths are young people who are neither psychological adolescent nor sociological adult (Adeniran, 2020). The food and Agricultural Organisation (FAO) used the concept of youth to mean young men and women between the ages of 15 and 24 years. African Union (AU) defines youths as people between the age of 15 and 35. In Nigeria, youth refer to the period of life characterised by development, exploration and growth, typically encompassing individuals from adolescence to early adulthood.

According to National Youth Policy of Nigeria (2009), the youth shall comprise of all male and female aged 18-35 years who are citizens of the Federal Republic of Nigeria. Young people in this age group require social, economic, and political support to realise their full potentials. Young people are characterised by energy, enthusiasm, ambition, creativity and promise. However, they are also faced with high level of socio-economic uncertainty and volatility thereby becoming the

most vulnerable segment of the population. They represent the most active, the most volatile and yet the most vulnerable segment of the nation's population.

Concept of Cyber Crime

The concept of cybercrime covers a broad spectrum of illegal activities conducted through the internet or other computer networks, which is made possible through the increasing integration of digital technology into daily life. This dynamic field includes offenses such as identity theft, cybercrime, cyberbullying, hacking and the distribution of illegal content, affecting individuals, businesses and government worldwide, coupled with emergence of new technologies that continuously reshape the landscape of cybercrime, necessitating ongoing academic and practical exploration.

Wall (2021) defines cybercrime as certain criminal acts that are committed through the use of computers and the internet which include traditional crimes carried out in new environments, as well as offenses that are unique to online transactions. Cross (2019) argues that cybercrime is defined as the intentionality to commit an illegal act that targets or uses a computer network or device as a means of perpetration. Their views emphasise the purposeful nature of cybercrime, characterising it as a deliberate act rather than an incidental occurrence. In the context of African and Nigerian settings, cybercrime is the use of digital technology to exploit individuals, organisations, or state resources through deceitful methods (Oyenuga, 2020).

Various Forms of Cybercrime Committed by Youth

Cybercrime has become an important social problem with the rapid expansion of information and communication technologies, particularly the internet, smartphones, social media and electronic financial services. It refers broadly to criminal activities carried out through computers, digital devices or computer networks, as well as conventional crimes facilitated through digital technologies (Wall, 2021). The increasing accessibility of digital technologies has created opportunities for young people to communicate, learn and participate in economic activities, but it has also provided new avenues for criminal behaviour. In Nigeria, the growth of internet access and the increasing use of digital platforms have been accompanied by different forms of cybercrime, with young people constituting an important group involved in some of these activities (Olofinbiyi, 2021).

One of the most prominent forms of cybercrime associated with youths in Nigeria is internet fraud, popularly referred to as *Yahoo-Yahoo*. Internet fraud involves the use of internet-based platforms to deceive individuals or organisations for financial gain. It may involve the creation of false identities, deceptive communication and manipulation of victims through social media, email and other online platforms. According to Adeniran (2020), youth involvement in cyber fraud is influenced by the attraction of quick financial returns and the perception that internet fraud provides an alternative means of achieving economic success. Ojedokun (2017) similarly explains that the Nigerian youth cybercrime phenomenon is closely connected with motivations for financial gain and the social environment within which fraudulent activities are sometimes tolerated or normalised.

Another important form is advance-fee fraud, which involves deceiving a person into making an initial payment or providing valuable information based on a false promise of receiving a larger financial benefit. Although advance-fee fraud existed before the widespread adoption of the internet, digital technology has expanded the means through which it can be perpetrated. Tade and Aliyu (2011) explain that internet fraud among Nigerian youths can be organised through social networks in which individuals share knowledge and experiences relating to fraudulent activities. The increasing use of email, social networking platforms and instant messaging applications has therefore made it easier for fraudulent schemes to be initiated and maintained across geographical boundaries.

Identity theft and impersonation are also significant forms of cybercrime. Identity theft involves the unauthorised acquisition or use of another person's personal information, while impersonation occurs when an individual falsely presents himself or herself as another person for deceptive purposes. The increasing amount of personal information available through social media and other digital platforms can create opportunities for such activities. Cross (2019) notes that the digital environment has transformed conventional forms of fraud by providing offenders with new ways of targeting and deceiving victims. In the Nigerian context, impersonation has also been associated with youth cybercrime because offenders may create false identities or assume the identity of other persons to gain the trust of potential victims (Ojedokun, 2017).

Mobile banking and electronic payment fraud represent another dimension of cybercrime associated with the expansion of digital financial services. The increasing use of mobile phones,

electronic banking and online payment platforms has transformed financial transactions in Nigeria. However, these developments have also created opportunities for the fraudulent manipulation or misuse of electronic financial systems. Ogunleye and Adeyemi (2017) identify mobile banking fraud and impersonation among the forms of illicit activities associated with youths. The increasing dependence on digital financial services therefore makes electronic payment systems an important area in the study of contemporary cybercrime.

Hacking and unauthorised access constitute another form of cybercrime. Hacking involves gaining access to computer systems, networks, online accounts or digital resources without authorisation. Unlike fraud, which often relies primarily on deception, hacking directly targets digital systems and accounts. Bossler and Burruss (2011) explain that computer hacking among young people can be associated with individual characteristics and social influences. Holt and Bossler (2014) further note that cybercrime can be facilitated through online environments where information and knowledge about offending behaviour are shared. Consequently, young people who have considerable exposure to digital technologies may potentially acquire technical knowledge that can be misused for unauthorised access to digital systems.

Tade and Aliyu (2011) conducted a study on the social organisation of internet fraud among university undergraduates in Nigeria using qualitative methods, including in-depth interviews. The study revealed that cybercrime, particularly advance fee fraud, is structured and organized within peer networks. The findings indicated that economic hardship, unemployment, and the desire for financial success were the primary motivations driving youth involvement in cybercrime.

Ngo and Paternoster (2011) conducted a quantitative study and found that association with deviant peers significantly increases the likelihood of engaging in cybercrime. Similarly, Bossler and Burruss (2011) examined computer hacking behaviour among youths and reported that low self-control and peer influence are strong predictors of cybercrime involvement. The study concluded that individuals who interact with cybercriminal peers are more likely to adopt similar behaviours due to reinforcement and shared knowledge.

Holt and Bossler (2014) found that exposure to online communities that normalize hacking and fraud significantly increases the likelihood of youth participation in cybercrime. Leukfeldt and Holt (2020) also emphasised that cybercrime is often learned through social interactions within digital environments, where individuals share techniques, tools, and experiences. These findings

underscore the importance of both offline and online social networks in shaping cybercriminal behaviour among youths.

Sani *et al.*, (2024) conducted a survey among undergraduate students in Nigeria and found that while students demonstrate high levels of digital competence, their awareness of cybercrime laws and ethical standards is relatively low. The study concluded that inadequate cyber ethics education contributes to the increasing involvement of youths in cybercrime. Similarly, Ahmead, *et al.*, (2024) used a cross-sectional research design to examine risky online behaviours among university students and found a significant relationship between low cybercrime awareness and increased exposure to cyber risks, including both perpetration and victimization.

Effect of Assess to Internet Technology on Cybercrime among Youth

The rapid expansion of internet technology has significantly changed the social and economic environment within which young people interact. Access to smartphones, computers, social media platforms and internet-based services has provided youths with opportunities for communication, education, entrepreneurship and access to information. At the same time, increased digital connectivity has created opportunities for cybercriminal activities by expanding the number of potential targets and providing platforms through which offenders can operate. Nzeakor and Nwoke (2023) note that internet access has become widespread in Nigeria, with social media representing one of the major purposes for which individuals use the internet. However, their findings suggest that frequency of internet access does not necessarily determine cybercrime victimisation, indicating that access alone may not be sufficient to explain cybercrime experiences.

The availability of internet-enabled devices is an important dimension of technological access. Smartphones and computers enable young people to remain connected to online platforms for extended periods and to participate in different forms of digital interaction. Such accessibility can provide opportunities for legitimate activities but may also expose young people to online environments where fraudulent and other criminal behaviours occur. Nwocha, *et al.*, (2025) observe that the proliferation of social media in Nigeria has facilitated communication, networking and business activities, but these same platforms have also been exploited for digital fraud, identity theft, phishing and other cybercrimes.

Social media access is particularly relevant to youth cybercrime because social networking platforms provide opportunities for interaction between large numbers of users. The platforms can

facilitate the creation of relationships, exchange of information and communication with individuals outside one's immediate geographical environment. According to Obi *et al.*, (2025), the accessibility, anonymity and global reach of social media platforms can create conditions that some youths exploit in perpetrating cybercrime. Their study indicates that features such as ease of account creation, weak identity verification and the wide reach of social media can make such platforms attractive for fraudulent activities.

Access to internet technology may also increase exposure to cybercriminal networks and deviant peer groups. Online platforms allow young people to interact with individuals who may share information and attitudes that normalise cybercriminal behaviour. Kpae (2026) argues that social media can function as a channel for criminal socialisation among Nigerian youths through peer networks, exposure to fraudulent schemes and the dissemination of knowledge associated with cybercrime. This suggests that the effect of internet access may extend beyond the technical ability to use digital devices to include exposure to social environments that can influence attitudes towards cybercrime.

In Nigeria, the growing availability of internet technology has therefore produced a dual effect. On one hand, it has created opportunities for education, entrepreneurship, employment, communication and social development. On the other hand, it has expanded the technological environment within which cybercrime can occur. Odoyi and Olatunji (2025) argue that social media possesses considerable potential for entrepreneurship and employment generation but can also be misused by young people for cybercrime and other antisocial activities. This reinforces the need to examine how technological access is translated into actual online behaviour among youths.

Control Measures of Cybercrime among Youth

The increasing incidence of cybercrime among young people has created the need for effective measures to prevent, control and reduce their involvement in cyber-related offences. The complex and rapidly changing nature of cybercrime means that its control requires more than conventional law-enforcement approaches. Effective cybercrime control involves a combination of legislation, law enforcement, cybersecurity awareness, digital literacy, institutional monitoring, parental supervision, employment opportunities and technological safeguards. Wall (2021) argues that the transformation of conventional crime through information technology requires corresponding changes in the ways crime is understood, prevented and controlled. Therefore, measures for

controlling youth cybercrime should address both the technological environment and the social conditions that facilitate participation.

Effective legislation and enforcement: constitute important measures for controlling cybercrime. Appropriate cybercrime laws provide the legal foundation for investigating and prosecuting individuals involved in illegal online activities. However, the existence of legislation alone may not be sufficient if enforcement institutions lack the technical capacity and resources required to investigate cyber-related offences. Obaro (2014) notes that weak institutional structures and ineffective governance can create an environment in which criminal activities thrive. In relation to cybercrime, effective enforcement requires trained personnel, adequate technological resources, digital forensic capabilities and consistent prosecution of offenders. The literature reviewed in the present study also identifies weak cybercrime enforcement and inadequate monitoring as factors that may reduce the perceived risk associated with cybercrime.

Strengthening law enforcement and institutional capacity: is particularly important because cybercrime is often committed across geographical boundaries and may involve sophisticated technologies. Law-enforcement agencies require specialised training in cybercrime investigation, digital forensics, electronic evidence management and online surveillance within legal limits. Tade and Aliyu (2011) demonstrate that youth internet fraud can be socially organised through networks in which knowledge and experiences are shared. Consequently, effective control requires agencies to understand not only individual offending but also the social networks through which cybercriminal behaviour can be learned and reproduced.

Youth employment, skills development and economic empowerment: are also relevant to cybercrime control. Economic hardship, unemployment and limited legitimate opportunities have been identified as factors associated with youth involvement in cybercrime. Sani, *et al.*, (2024) argue that unemployment and underemployment, together with limited opportunities for legitimate income generation, can create conditions that encourage some youths to participate in cybercrime. Providing vocational training, entrepreneurship opportunities, digital employment and other legitimate sources of income can therefore help reduce the economic attraction of cybercrime. However, economic empowerment should be combined with legal and ethical education because economic factors alone do not explain all forms of cybercriminal behaviour.

Public awareness and community-based prevention: can further contribute to cybercrime control. Awareness campaigns can educate young people, parents and the wider public about common forms of cybercrime, the consequences of participation and appropriate online safety practices. Such campaigns may be implemented through educational institutions, government agencies, financial institutions, telecommunications organisations and civil society groups. Ojedokun (2017) emphasises the importance of understanding both the motivations behind youth cybercrime and the deterrent measures that can discourage participation. Therefore, community awareness should combine information about cyber risks with clear information about the legal consequences of cybercrime.

Technological and cybersecurity measures: are necessary for reducing opportunities for cybercrime. Financial institutions, telecommunications companies and online service providers can strengthen authentication systems, transaction monitoring, fraud detection and other security mechanisms. Technological safeguards can make it more difficult for offenders to obtain unauthorised access to accounts and digital resources (Olayemi, 2014). The importance of capable guardianship is particularly relevant here because stronger monitoring and security systems can increase the likelihood of detecting suspicious activities and reduce opportunities for offenders to exploit vulnerable users.

THEORETICAL FRAMEWORK

The study adopted the Routine Activity Theory (RAT), developed by Cohen and Felson (1979). The theory argues that crime occurs when there is a motivated offender, a suitable target, and the absence of capable guardians converge in time and space. RAT helps explain youth involvement in cybercrime because the online environment provides unique conditions that facilitate crime, particularly anonymity in the global cyber space, create room for anonymity which make many vulnerable to cybercrime. The global cyberspace allows offenders to conceal their identities, locations, and digital traces, reducing the risk of detection and increasing the perceived safety of committing crime (Cohen & Felson, 1979). This anonymity, combined with minimal regulation and limited law enforcement supervision, significantly increases the number of vulnerable targets individuals or institutions whose information or resources can be exploited (Tade & Aliyu, 2011). For example, many adults are unemployed or underemployed this have already created room for a motivated offender seeking for youth who are active on social media and online banking platforms

but may lack sufficient digital literacy or awareness of cybersecurity this make them become suitable target. That can be easily exploited, as cybercriminals can operate remotely and remain largely undetected. The perception of anonymity also lowers the psychological barrier to committing cybercrime, as offenders feel insulated from immediate social or legal consequences.

Consequently, the convergence of motivated offenders, vulnerable targets, and weak guardianship in digital spaces creates an environment where cybercrime becomes both possible and attractive (Alemika & Chukwuma, 2020). In this way, RAT not only emphasises opportunity structures but also highlights how technological affordances like anonymity amplify vulnerability, creating fertile conditions for cybercrime. Motivated offenders: High youth unemployment, poverty, and social pressure motivate youths to seek rapid financial gain (Alemika & Chukwuma, 2020). Suitable targets: Online banking users, e-commerce platforms, and social media accounts become “targets” due to the availability of personal or financial information. Absence of capable guardians: Weak cyber law enforcement and cybersecurity, limited digital literacy among potential victims, and inadequate monitoring of online activities reduce the risk of detection (Tade & Aliyu, 2011). No strict adherence to cyber security. Anonymity strengthens these elements by allowing offenders to mask their identity, location, and digital traces, making it harder for law enforcement or other guardians to intervene. This creates an environment in which the convergence of offender, target, and lack of guardianship is more likely to result in crime. For many youths, anonymity makes cybercrime appear low-risk and high-reward, further incentivizing the fraudulent behaviour over conventional work.

METHODOLOGY

The study adopted a descriptive cross-sectional research design. The setting of the study is Benin Metropolis comprising three local government area, Oredo, Egor and Ikpoba Okha. The study population consist of youth from 18 to 35 years within the study area. A sample size of 500 respondents were sampled using Taro Yamane sample size formula. The study adopted multi-stage sampling technique. Data was collected using questionnaire. Questionnaire were structured using open and close ended format. The choice of this technique of data collection was to enable the researcher to obtain a wide range of responses from the respondents. Quantitative data was presented in nominal distribution tables and analysed using frequencies and percentages.

RESULTS

Data for this study was collected from respondents with different socio economic background. The findings have been presented in the table below.

Table 1: Socio-Economic Characteristics of the Respondents

	Variable	Frequency	Percentage
Sex	Male	370	74.0
	Female	130	26.0
	Total	500	100
Age	18-26 years	216	43.2
	27-30 years	164	32.8
	31-35 years	120	24.0
	Total	500	100
Marital Status	Single	315	63
	Married	185	37
	Total	500	100
Religion	Christian	378	75.6
	Muslim	29	5.8
	African Tradition	74	14.8
	Others	19	3.8
	Total	500	100
Educational Qualification	Primary Education	166	33.2
	SSCE	213	43.6
	HND/BSc	91	18.2
	Total	500	100

Source: field survey 2026

Table 1 is concerned with the demographic characteristics of respondents and it revealed that 370 respondents which constitute 74.0% were male while 130 respondents which constitute 26.0% were female. The result on age revealed that 216 respondents which represents 43.2% are between the ages of 18-26; 164 respondents representing 32.8% are between 27-30 years, while 120 respondents representing 24.0% are between ages 31-35 years. The result on marital status shows that majority of the respondents 315 which accounted for 63% were single while 185 which accounted for 37% were married. Furthermore, the table shows that 378 respondents representing 75.6% were Christians, 29 respondents representing 5.8% were Muslims, 74 respondents representing 14.8% were worshippers of African Traditions while 19 respondents representing 3.8% worship other religion. The result on the educational level of respondents shows that the 166 respondents which constitute 33.2% had primary education, 213 respondents representing 43.6% had SSCE, 91 respondents which represents 18.2% possess HND and B.Sc. degree respectively.

Table 2: Various Cybercrimes committed by Youth in Benin Metropolis

Variable	Response	Frequency	Percentage %
Which of the following cybercrime do you believe is the most prevalent among youth in Benin Metropolis	Romance/Dating scam	146	29.2%
	Business Email Compromise	32	10.4%
	Phishing/Hacking	120	24.0%
	Credit Card Fraud	114	22.8%
	Online Investment Scam	68	13.6%
	TOTAL	500	100%
Do cybercriminal use mobile phones or laptops for their work	Mobile Phone	210	42%
	Laptops	181	36.2%
	Both equally	78	15.6%
	Desktop computers	131	6.2%
	Total	500	100
Which age group is most associated with “wire wire” (illicit international bank transfers)	18-20	37	7.4%
	21-25	228	45.6%
	26-30	88	19.6%
	31-35	137	27.4
	Total	500	100
Do you believe that the use of charms or spiritual fortification is an integral part of cybercrime among youth	SA	147	29.4%
	A	133	24.4%
	U	95	19.0%
	D	66	13.2%
	SD	70	14.0
	Total	500	100

Source: Fieldwork, 2026

Data on table 2 above showed the various cybercrime committed by youths in Benin metropolis. 29.2% of the respondents revealed that romance scam is the most prevalent form of cybercrime committed by youths. Also 42% of the respondents revealed that cybercriminals carry out their fraudulent activities with mobile phones. 41.6% of the respondents revealed that the age group mostly associated with "wire wire" are between 21–25 years. While 29.4% of the respondents strongly agreed that the use of charms or spiritual protection is an integral part of cybercrime among youths.

Table 3: Effect of Access to Internet technology on cybercrime among youths in Benin Metropolis

Variable	Response	Frequency	Percentage %
How many cyber-enabled devices (smartphones, laptops, tablets) do you personally own?	None	52	10.4%
	One	186	37.2%
	Two	196	39.2%
	Three or more	66	13.2%
	Total	500	100
Do you agree that the widespread availability of cheap smartphones has made it easier for youth to start cybercrime	SA	153	30.6%
	A	142	28.4%
	U	85	17.0%
	D	66	13.2%
	SD	54	10.8%
	Total	100	100%
How easy is it for a youth to acquire a high-end laptop for cybercrime	Very easy	24	14.8%
	Easy	146	29.2%
	Difficult	235	47%
	Very difficult	45	9.0%
	Total	500	100
Do you agree that the presence of 24/7 power supply in certain areas encourages cybercrime	SA	98	19.6%
	A	387	77.4%
	U	69	13.8%
	D	68	13.6%
	SD	82	16.4%
	Total	500	100

Source: Fieldwork, 2026

Data on table 3 above revealed that 38.2% of the respondents stated that they own more than one cyber-enabled devices. Also 30.6% of the respondents stated that the availability of cheap smartphones have made it easier for youths to start cybercrime. 47% of the respondents stated that it is difficult for youths to acquire high-end laptop for cybercrime. While 77.4% of the respondents stated that the presence of 24/7 power supply in certain areas encourages cybercrime among youths.

Table 4: Control measures of cybercrime among Youths in Benin Metropolis

Variable	Response	Frequency	Percentage %
Do you believe that frequent arrest of cybercriminals by EFCC in Benin Metropolis serves as a deterrent to others?	Yes	130	26.0%
	No	195	39%
	Not Sure	177	20.9%
	Total	500	100
Do you agree that corruption within law enforcement agencies hinders the control of cybercrime	SA	237	47.4%
	A	116	23.2%
	U	73	4.6%
	D	44	8.5%
	SD	30	6.0%
	Total	500	100
Which of these is the most effective way to control cybercrime? (please select one)	Stricter prison sentence	105	21%
	Job creation/empowerment	242	48.4%
	Parental/Moral education	59	11.8%
	Technological monitoring/tracking	94	18.8%
	Total	500	100

Source: fieldwork 2026

Data on table 4 above showed the control measure of cybercrime among youths in Benin metropolis. 39% of the respondents stated that frequent arrest of cybercriminals by EFCC does not serve as a deterrent to others. Also 47.4% of the respondents strongly agreed that corruption within law enforcement agencies hinders the control of cybercrime among youths, while 48.4% of the respondents revealed that job creation and empowerment will go a long way in curbing the menace of cybercrime among youths.

DISCUSSION OF FINDINGS

Examining the various cybercrime committed by youths in Benin metropolis it was observed that romance and dating scams is prevalent among youth in Benin metropolis. This finding aligns with the work of Olurounbi (2023) who documented the evolution of cyber-deception tactics in southern Nigeria and establishes that "billing" through romance scams, which fundamentally relies on identity theft and fake social media profiles, serve as the primary baseline entry point for emerging cyber criminals. Also finding from the study revealed that respondents strongly agreed that the use of charms or spiritual fortification is an integral part of cybercrime among youth in Benin metropolis. The findings agreed with the work of Audu (2011) who examine the hybridisation of traditional African religious practice and modern technology and pointed out that as adapted

security systems make it harder to successfully execute scams, youth offenders increasingly rely on witch doctors, "juju" supernatural rituals, which is driven by a belief that these methods can hypnotise or charm remote victims ("magas") into compliance. The finding further reveals that majority of the respondents opined that cybercriminal often carry out their cybercrime with mobile phones. The finding is in consonance with the work of Tade and Aliyu (2011), and Pehehse (2021) who stated that while early 2000s cybercrime relied heavily on commercial desktop computers in cybercafes, the transition to smartphones represented a major structural shift, coupled with high speed mobile networks and advance smartphones technology that allow modern operators to run encrypted communication channels and spot location seamlessly from private spaces, which drastically lower the barriers to entry for youth participation.

Findings further revealed that the age group of youths mostly associated with "wire wire" (illicit international bank transfers) are those between the ages of (26–30 years). The finding agreed with the report from Sophos/CTU Research (2016) regarding the structural profile of West African cyber-threat groups. The authors draw a sharp distinction between younger cybercriminals aged (15–25) who focus on romance scams and older highly organized networks specializing in "wire wire" or business email compromise, which requires deep corporate insights, access to complex illicit international bank networks, and mature money-laundering systems. Finding revealed that most of the respondents stated that identity theft (impersonating others to solicit funds) is a major cybercrime among youths in Benin metropolis.

Examining the access to internet technology on cybercrime among youths in Benin metropolis, it was discovered that most of the respondents own more than one cyber-enabled devices because of availability of cheap smartphones. Finding from the study further revealed that majority of the respondents were of the opinion that it is difficult for youths to acquire a high-end laptop for cybercrime. This finding agreed with the work of Aduwa-Ogiegbaen (2022) who stated that since high-end laptops remain financially out of reach for lower-income youths, their digital proficiency is redirected towards low-overhead mobile-accessible illicit operations where cheap smartphones suffice to extract fast immediate economic liquid returns. Finding further showed that majority of the respondents opine that the presence of 24/7 power supply in certain area encourages cybercrime among youths.

Examining the control measures of cybercrime among youths in Benin metropolis, it was discovered that most of the respondents stated that they are not sure whether the frequent arrest of cybercriminals serves as a deterrent to others. Finding from the study further showed that majority of the respondents stated that corruption within the law enforcement agencies hinders the control of cybercrime among youths. The finding also revealed that most of the respondents were of the opinion that job creation and empowerment will go a long way in curbing the menace of cybercrime among youths.

CONCLUSION

The study concludes that cybercrime have evolve beyond isolated criminal acts into a socially recognise sub culture among youths as criminal activities such as romance and dating scam, identity theft, and other online fraudulent schemes have become normalised and are increasingly viewed as legitimate means of survival. Therefore addressing cybercrime effectively will require more than punitive measure and law enforcement actions; it will necessitate deliberate effort to tackle the root cause of cybercrime.

RECOMMENDATION

Based on the findings for this study, the following recommendations were made:

- i. Efforts should be made to encourage youth who possesses digital literacy and internet access to channel this skills into legitimate online ventures such as software development, digital marketing, graphic design, content creation, freelancing, cybersecurity services, e-commerce, and other digital economy opportunities.
- ii. Since corruption and information leaks were found to undermine internet crime control efforts, strict monitoring mechanisms should be introduced to ensure accountability among law enforcement personnel, and officers found engaging in bribery, collusion, or leaking operational information should face appropriate disciplinary and legal sanctions.
- iii. Government should formulate and implement policies aimed at creating sustainable employment opportunities for youth. This can be achieved through investment in labour-intensive industries, public works programmes, technology hubs, and private-sector partnerships.

References

- Adejoh S.O. (2019). High rate of unemployment and the prevalence of cybercrime among youth in Lagos State, Nigeria. *International Journal of Cyber criminology*, 13(2), 444-459
- Adeniran A.I. (2020). Cybercrime, campus cultism and the sociology of deviance in Nigerian Universities. *University Press*.
- Adeniran, A. & Johnson, R. (2012). Investigating the level of cybercrime in Nigeria. *International Journal of Cyber Criminology*. 2(2): 368-381
- Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviours and cybercrime awareness among university students. *Crime Science*, 2(3): 21-27.
- Akinyemi, T., & Osunwoko, C. O. (2022). Socio-economic factors as a driving force to youths' involvement in cybercrime. *Journal of Criminology, Law and Social Sciences*, 1(1), 12–25.
- Alemika, E. E., & Chukwuma, I. C. (2020). Policing: A Driver of Change. Analysis of Police and Policing in Nigeria. Lagos: *CLEEN Foundation*.
- Aransola, J.O. (2017) Ritualistic violence and the Psychological Barrier to Crime. *Nigerian Criminology Journal*. 54(4): 201-218
- Audu, M.S. (2011). Intra Ethnic Violence and Conflict in Eboraland Nigeria: An Aspect of Social Movement in Nigeria History. 6(1&2): 49-72
- Bossler, A. M., & Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers? *Journal of Crime and Justice*, 34(2), 83–103.
- Button, M. (2017). *Cyber frauds, scams and their victims*. Routledge.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.
- Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice*, 5(4), 120–131.
- European Union Agency for Law Enforcement Cooperation. (2023). *Internet organised crime threat assessment (IOCTA) 2023*. Publications Office of the European Union
- Holt, T. J. (2020). *Cybercrime through an interdisciplinary lens*. Routledge.
- Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behaviour*, 35(1), 20–40.
- Kpae, G. (2026). Assessing the impact of social media on youth involvement in criminal activities in Nigeria. *Iconic Research and Engineering Journals*, 9(9), 1509–1521.

- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Journal of Criminal Justice*, 44, 1–8.
- National Youth Policy of Nigeria (2009). Published by Federal Ministry of Youth Development.
- Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *Journal of Criminal Justice*, 39(6), 521–528.
- Nwocha, M. E., Iteshi, C. V., & Awada, P. M. (2025). Social media facilitated cybercrimes in Nigeria and the challenges of legal enforcement. *Law and Social Justice Review*, 5(3).
- Nzeakor, O. F., & Nwoke, C. N. (2023). Internet access and cybercrime victimization experience in Abia State, Nigeria. *FUOYE Journal of Criminology and Security Studies*, 2(1): 209-229.
- Obaro, O. A. (2014). Sociological and legal issues in Nigeria's pervasive corruption: The criminalisation of the state and the citizenry in Nigeria. *Mediterranean Journal of Social Sciences*, 5(9), 307–316.
- Obi, F. A., Nyekwere, O. C., & Brisibe, P. (2025). Exploring the role of social media platforms in facilitating cybercrime activities among youths in Rivers State. *Rapid Journals RJIP: Journal for Media and Communication(JMC)*, 2(10): 1216-1224.
- Odoyi, C. D., & Olatunji, R. W. (2025). The imperatives of social media entrepreneurship for employment generation and cybercrime reduction among youths in Nigeria. *Journal of Economic, Business & Accounting Research*, 3(1): 72-78.
- Ojedokun, U. A. (2017). Cybercrime and the Nigerian youth: An analysis of motivation and deterrence. *African Journal of Criminology and Justice Studies*, 10(1), 1–18.
- Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3), 116–125.
- Olofinbiyi, S. A. (2021). Exploring youth awareness of cybercrime and factors engendering its proliferation in Nigeria. *African Renaissance*, 18(4), 319–342.
- Olurounbi, R. (2023). Nigeria's unemployment rate and the global ranking surge. Bloomberg news
- Omokhabi, A. (2024). Cybercrime and the digital economy: emerging trends in Benin metropolis, *Benin Journal of Social Sciences*. 3(1): 55-70
- Oyenuga, A. (2020). Youth employment and informal economy engagement in Nigeria. *International Journal of Social Economics*. 47(11): 1334-1338
- Sani, *et al.* (2024). Cybercrime awareness, digital competence and ethical standards among undergraduate students in Nigeria, *International Journal of Social Economics*. 4(1): 124-131.

- Suleiman, A.A. (2019). Cybercrime and the sociological implication in the Nigeria Tertiary Institution, *FUDMA Journal of Science*, 2(1): 51-62
- Tade, O., & Aliyu, I. (2011). Social organisation of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, 5(2), 860–875.
- United Nations Office on Drugs and Crime. (2021). *Report on the meeting of the expert group to conduct a comprehensive study on cybercrime*. United Nations Office on Drugs and Crime
- Wall, D. S. (2021). *Cybercrime: The transformation of crime in the information age*. Polity Press.