THE THREATS OF CYBER-CRIME AND ITS EFFECTS AMONG NIGERIAN YOUTHS: THE WAY FORWARD

Orji, Chidi Paul, Ph.D.
University of Agriculture and Environmental Sciences, Umuagwo, Imo State,
E-mail: paul.orji@uaes.edu.ng, hipaulco@gmail.com,
+234 (0)8149412995, ORCID ID: https://orcid.org/0009-0000-2941-5398

Ogunsanya Sunday Omotola,
Tai Solarin Federal University of Education, Ijebu-Ode, Ogun State,
Email: ogunsanyaso@tasued.edu.ng,
+2348054533940, ORCID ID: https://orcid.org/0009-0005-4211-5249

Oluwafunmilayo Omolola Fabiyi, Ph.D.
Federal University of Medicine and Medical Sciences, Abeokuta, Ogun State,
Email: oluwafunmilayo.fabiyi@fummsa.edu.ng,
+2348107202774, ORCID: https://orcid.org/0009-0005-9741-0632

Nwagbara Rufus Godswill, Ph.D.
Babcock University, Ilisan Remo, Ogun State,
Email: nwagbarag@babcock.edu.ng,
+2348069211771, ORCID ID: https://orcid.org/0009-0004-2351-3148

Abstract
Crime has existed for as long as humanity itself. As long as society exists, there will always be a struggle between good and evil, and it is this presence of evil that allows crime to persist. This paper examines the issue of cybercrime and explores strategies to curb its growing influence among Nigerian youth by focusing on the proper implementation of cyber security and the creation of jobs. The study strongly suggests that religious organizations should actively preach against the immorality of cybercrime, as it is currently destabilizing young people and hindering societal progress. Furthermore, it recommends that the government prioritize providing employment opportunities for the youth, giving them the chance to grow personally and contribute meaningfully to the development of society as a whole.
Keywords: Crime, Cyber-Crime, Cyber Security, Youths, Employment Creation.

Introduction
Crime has been a persistent concern for humanity since the dawn of time. In many parts of the world, and particularly in Nigeria, criminality poses a significant barrier to national development. While Nigeria has attempted to combat cybercrime by implementing security measures and focusing on job creation, these efforts have not been entirely successful. Every day, countless individuals lose their hard-earned money and valuables to cybercrime and other forms of fraud, much of which is fueled by high unemployment rates. Technological advancements have turned cyberspace into a fertile ground for criminal activity. While its role in enhancing communication and other digital interactions is clear, it has also been exploited by malicious actors to carry out various cybercrimes—particularly when users lack adequate security safeguards (Chong, 2013; Akinyetun, 2021).

In Nigeria, incidents of cybercrime have risen sharply, driven in part by widespread internet access among the youth. Offenses such as phishing, cyber-stalking, online extortion, cyber-bullying, and similar activities have become increasingly common. These crimes are taking a toll on the nation's socio-economic stability, and without effective intervention, they could undermine national security, public order, and the overall economy (Bhawna, 2016).

Since its introduction to Nigeria in 1996, the Internet has expanded massively, with the country now boasting more than 108 million users (Johnson, 2021). This digital landscape opens up endless possibilities for commerce, social connection, and learning. Indeed, the positive impact on the Nigerian economy is clear, fueling growth in areas like digital banking, insurance, stock markets, and general commercial activity. However, this connectivity comes with a dark side. The rise of the Internet has brought about serious issues such as email scams, identity theft, organized crime, cyber-piracy, and various forms of exploitation like fake lotteries and solicitation. These digital threats pose a genuine risk to the economic, social, and political stability of nations worldwide, including Nigeria. If left unchecked, cybercrime could disrupt vital societal sectors and stall the country's overall development. Nigeria is a young, rapidly growing nation where many people are driven by the sheer necessity of making a living. With such a vast population of young people, cybercrime has the potential to become a widespread menace, making prevention and control absolutely essential. As Sorunke (2011) noted, Nigeria faces significant vulnerabilities in cyberspace, particularly regarding the security of payment systems. Without proactive measures from organizations and businesses to safeguard their data, the rise of hacking and digital theft could lead to devastating financial losses and threaten the very survival of online enterprises. Consequently, there is an urgent need to guide the youth away from the misuse of the internet. Cybercrime acts as a setback to national progress, causing severe economic and social instability within any society.

The Concept of Cybercrime

Cybercrime is generally understood as criminal activity that uses a computer, a network, or a networked device to deceive individuals. These acts are carried out by hackers or cybercriminals seeking to make money through dishonest and illegal means, whether acting alone or as part of an organized group. Ebeleogu, Ojo, Adeh, and Agu (2019) define cybercrime as offenses involving digital technologies, specifically targeting computing and communication systems. Often, this is driven by young people looking for easy ways to make a living, leading them to defraud individuals and organizations alike. Similarly, Ibikunle and Eweniyi (2013) describe cybercrime as a series of organized attacks on both cyberspace and cyber-security. In Nigeria and across the globe, cybercrime has become a complex, tangled issue; many criminals operate from remote locations, making it incredibly difficult for security agencies to track and apprehend them.

The lack of up-to-date laws further complicates the fight against these digital threats. Bosser, Adam, Berenblum, and Tamer (2019) view cybercrime as a computer-oriented offense involving both a computer and a network, where the device serves as either the tool used to commit the crime or the target itself. Aghatise (2006) similarly defined it as a crime committed via the internet, using a computer as a weapon or a victim. He categorized cybercrime victims into four groups: the gullible, the desperate, the inexperienced, and the unlucky.

Ultimately, cybercrime involves various criminal tactics aimed at making money through illegal digital channels. Some attackers are highly skilled, organized, and use advanced strategies to achieve their financial goals. Beyond individual theft, cybercrime can threaten the security of companies and entire nations. It raises massive privacy concerns when sensitive data is intercepted or leaked. On an international scale, both government and non-state actors engage in cyber-related activities like espionage and financial theft. When these crimes cross international borders and involve state actors, they are sometimes referred to as "cyber-warfare."

The economic impact is staggering. A 2014 report by McAfee estimated that cybercrime causes

$445 billion in annual damage to the global economy. In the U.S. alone, roughly $1.5 billion was lost to online credit and debit card fraud in 2012. By 2018, a study by the Center for Strategic and International Studies (CSIS) in partnership with McAfee found that nearly $600 billion—about one percent of the global GDP—is lost to cybercrime every year. Based on these findings, it is clear that cybercrime uses digital devices to defraud people and groups for unlawful financial gain, driven primarily by the desire to make money through deception.

Ranges of Cybercrime

Cybercrime can be classified into several categories, including:

Financial Criminals and Fraudsters: This category includes phishing, scams, and social engineering. Social engineering requires criminals to pose as trustworthy representatives of an organization to trick victims. Phishing, a common method, involves hackers sending malicious emails, attachments, or URLs to gain access to accounts or computers. These often contain links to fake banking sites designed to steal private information. Scams frequently appear as advertisements or spam emails promising rewards or money; these "too good to be true" offers often contain malware that compromises a user's information once clicked. Social engineering relies on manipulation and convincing lies to trick people into revealing sensitive data. According to Ebeleogu, Ojo, Adeh, and Agu (2019), common social engineering tactics include:

I. Sending emails that claim there is an issue with an account and providing a link to a fraudulent website. When the victim enters their credentials, the information is sent directly to the criminal (phishing).

II. Tricking victims into opening email attachments containing malware by claiming they are something the user wants (like a game) or needs (like anti-malware software).

III. Pretending to be a network or account administrator and requesting a victim's password under the guise of performing necessary maintenance.

IV. Claiming a victim has won a prize, but insisting they must provide credit card details to claim it.

V. Asking for an internet service password and then using those same credentials to access other accounts, taking advantage of the fact that many people reuse passwords across different platforms.

VI. Promising the victim they will receive millions of dollars if they simply help the sender by providing money or their bank account information.

2. **Website cloning**: One of the newer methods in cybercrime involves the emergence of "copycat" websites designed to deceive consumers. People who are unfamiliar with the internet or who do not know the official web address of a legitimate company may unwittingly enter their credit card details into a fraudulent database while trying to purchase goods. The fraudster then uses this data for their own gain or sells it to others interested in credit card fraud.

3. **Spamming**: This refers to the mass distribution of emails used to promote and advertise specific products or websites.

4. **Identity theft and credit card theft (phishing):** This involves fraudulent emails where scammers impersonate well-known, legitimate companies. The goal is to trick the user into handing over private information that will be used for identity theft, allowing criminals to assume the victim's persona.

5**. Cyber harassment**: This involves using electronic means to intentionally carry out threatening acts against individuals. This can include directing obscenities or derogatory statements at people based on their race, gender, religion, nationality, or sexual orientation.

In some instances, the use of a computer can lead to an enhanced legal sentence. For example, in the United States, in the case of United States v. Neil Scott Kramer, the defendant received an enhanced sentence under US sentencing guidelines for using a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of a minor to engage in prohibited sexual conduct." Kramer appealed, arguing that he should not be convicted under that specific statute because his charge involved persuasion

via a computer device, and a cell phone is technically not a computer. However, the U.S. sentencing guidelines define a "computer" as any electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical arithmetic or storage functions, including any data storage or communication facility working in conjunction with such a device. In recent years, many countries have enacted similar laws to govern cybercrime.

6. **Cyber laundering**: This refers to the electronic transfer of illegally obtained funds with the intent of hiding both their source and their destination.

7. **Hacking**: In this category, hackers exploit loopholes in operating systems to destroy data or steal sensitive information from a victim's computer. This is often achieved by installing "backdoor" programs. Hackers also use password-cracking software to gain unauthorized access to resources and may install various programs on a user's machine without their knowledge to harvest personal data like credit card numbers and passwords.

8**. Cyber theft**: This type of cybercrime uses computers and communication systems to steal data in electronic formats. Criminals breach banking systems to transfer cash directly into their own accounts. This has become a global crisis due to the massive amounts of money illegally transferred. Interestingly, many defrauded organizations stay quiet about these incidents out of fear of losing customers and shareholder confidence.

These types of cybercrimes are the most common ones reported by individuals and organizations. Criminals often gain these funds with minimal effort, which has had a negative impact on the youth, who may be drawn to the "quick money" syndrome. Other classifications of cybercrime include the spreading of worms and viruses.

Methods and tricks used by cybercriminals to deceive individuals or organizations in Nigeria:

Nigeria is a vast country, which sometimes allows individuals to go into hiding for extended periods, making it difficult for security agencies to apprehend cybercriminals. However, the following tactics are commonly used to manipulate people and steal their assets:

9. **Lottery scams**: This is an advance-fee fraud that typically begins with an unexpected email, mail, or phone call (sometimes accompanied by a large check) claiming the recipient has won a massive sum of money in a lottery. The target is usually told to keep the news a secret due to a "mix-up" in names or numbers and is instructed to contact a "claims agent." Once the victim contacts the agent, they are directed to pay various "processing fees" or "transfer charges" to release the winnings. In reality, the victim never receives any money. Many of these scammers use the names of legitimate lottery organizations or corporations to appear authentic, though the actual emails usually come from free accounts like Outlook, Yahoo, Hotmail, Live, MSN, or Gmail.

10. **Internet service scams:** This is a method that has been particularly developed by young, tech-savvy criminals in Nigeria. They achieve this by connecting cyber cafes to various ISP networks in a way that evades detection, allowing them to operate entirely for free.

- Bogus cashier's checks: In this scenario, victims list items for sale online and are subsequently targeted by scammers.

11. **Internet charity scams**: This is a prevalent form of e-crime in Nigeria, where cybercriminals set up websites for fake charitable organizations to solicit monetary donations and supplies for non-existent causes.

12. **Next of kin scams**: Cybercriminals use this method to siphon money through various banks and transfer fees by tricking victims into believing they are entitled to inherit millions of dollars from a deceased relative in a Nigerian bank.

Causes of Cybercrime in Nigeria:

As a multi-ethnic nation, Nigeria faces numerous challenges that have hindered development. This stagnation negatively impacts citizens, particularly the youth, who make up the bulk of the labor force. Furthermore, the widespread availability of computers has introduced new vulnerabilities,

which, when combined with existing socio-economic issues, fuels the rise in cybercrime.

The primary causes include:
- Alarming poverty rates: Nigeria is globally recognized as a developing nation struggling with an alarming poverty index. This gap continues to widen; while the wealthy accumulate more, the poor struggle to survive. The lack of basic amenities and an unstable power supply have also brought many small and medium-sized enterprises to a standstill.
- Peer pressure: In certain social circles, there is an intense pressure to belong to the upper class regardless of one's actual background. This erodes the moral upbringing of many Nigerian youths, who attempt to emulate their peers by defrauding individuals and organizations. Driven by the "ends justify the means" mentality, they seek a luxurious lifestyle without regard for the consequences.
- Negative role models and parental influence: Some parents inadvertently encourage criminal behavior by constantly comparing their children to others and emphasizing that wealth is the only measure of success. This "money talks" mindset lures children into a life of crime.
- Collusion between security personnel and fraudsters: Instead of apprehending cybercriminals, some security officers act as bodyguards, covering up illicit activities in exchange for bribes. Some even go as far as advising criminals on how to launder illegally acquired wealth to avoid detection by government agencies, which emboldens these individuals to continue their crimes.
- Corruption: Until the establishment of financial crime monitoring agencies like the EFCC (Economic and Financial Crimes Commission) in 1999, Nigeria was ranked among the most corrupt countries in the world.
According to Ebeleogu, Ojo, Andeh, and Agu (2019), poor economic conditions and a failing educational system also contribute significantly to the spread of cybercrime in Nigeria. Other contributing factors include rapid urban migration, failing infrastructure, weak legal frameworks, and the "quick money" syndrome.
Strategies for Reducing Cybercrime in Nigeria
A problem well-defined is a problem half-solved. Given that the root causes include corruption, the desire for easy money, and high unemployment, several remedies can be proposed:
- Public enlightenment and education: The Nigerian government should organize regular seminars for school leavers, teaching them how to build sustainable livelihoods. Additionally, citizens need to be educated on internet security protocols to protect their privacy from hackers.
- Strengthening cyber laws: It is essential to enact robust cybersecurity legislation and ensure consistent follow-up to monitor and apprehend criminals.
- Job creation: The government must generate more employment opportunities and support small-scale industries by reducing tax rates and providing grants and loans.
- Implementation of firewalls: To protect computer systems from unauthorized access, there should be greater use of hardware and software firewalls.
- Address Verification Systems (AVS): This can help prevent fraud by ensuring that the shipping address provided for international orders matches the billing address on the cardholder's statement.
- Establishing skill acquisition centers: The government should establish at least one skill acquisition center in every local government area. Providing the youth with tangible skills will offer them legitimate paths to success and reduce the temptation of cybercrime.
- Effective enforcement of cyber security laws: Cyber security involves protecting networks and systems from data theft, hardware damage, and service disruptions. To implement this effectively, the government must employ genuine experts in the field to close existing loopholes in the digital landscape.

Conclusion and Recommendations

Nigeria's international reputation has suffered due to high rates of corruption, with cybercrime being a prominent example. These activities lead to massive financial losses, decreased productivity, and a damaged national image—consequences that are increasingly visible across the country. Based on these findings, the paper offers the following recommendations:

Governments at all levels—from federal and state to local authorities—must properly enforce cyber-security laws to more effectively track and stop fraudsters and their accomplices.

The government should establish seminars and skill acquisition centers to help lower the unemployment rate.

Individuals need to do their part by staying vigilant against suspicious activities, such as fake bank alerts, and by keeping their online passwords strictly private.

Providing grants and loans to individuals and small businesses could redirect people's focus toward legitimate work and earning a decent living, rather than turning to cybercrime.

Religious leaders—including Christian pastors, Muslim imams, and practitioners of African Traditional Religion—should actively preach against illegal ways of making money to their followers.

References

Adebusuyi , A (2008). The Interest And Emergence of Yahoo Boys Sub-Cultures In Nigeria, *International Journal of Cyber Criminology* O794-2891, Vol 2 (2).

Aghatise, E.J (2008). Cybercrime Definition. Computer Research Center. Http://Www.Crime –Research .Org/ Article Joseph 06/2

Aghatise, E.J (2006). *Level of Awareness of Internet Intermediaries Liability.*

Ajibike, T (2019). *"Youth and Cybercrime in Nigeria, Punch News*. March 15.

Bossler Adem, Berenblum, Tamar New Directions in *Cybercrimes Research Journal of CrimeAnd Justice* 42 (5), 495-499: Doi:10:1080/0735 648x. 2019.1692426. Issn 0735-648x

Ebeleogu, C.U, Ojo, S.D. Andeh, C.P And Agu, E.O (2019). Cybercrimes, Its Adherent Negative Effects On Nigerians Youth And The Costly at Large, Possible Solution. *International Journals of Advances in Scientific Research and Engineering (Ijasre).* E-Issn: 2454-8006, Volume 5, Issue 12.

Ibikunle , F. And Eweniyi .O (2013). Approach to Cyber Security Issues in Nigeria, Challenges And Solutions (Iycrsee) *International Journal of Cognitive Research in Science, Engineering And Education* Vol.1no.1.2013

International Telecommunication Union. Http:// Www. Itu,Int/En//Pages/Default .Aspx.

Longe, O.B, Chiemeka .S (2008). Cyber Crime and Criminality In Nigeria- What Roles Are Internet Access Points In *Playing European Journal Of Social Science* – Volume 6, Number 4

Nkenga, E. (2008). *Combating Cyber Crime Menace in Nigeria* .www. allafrica.com

Olumide, O.O. and Victor, F.B (2010). Crime in Nigeria. Trends, Tricks and Treatment. *ThePacific Journal of Science and Technology* Volume ii. Number 1 2010 (Spring) Stassman. P.A. (2009). Cyber Security for the Department of Defense. Http://Www-Strassman.Com/Pubs/Dod/Cybersecuirty-Draft -Vipdf.