AKU: AN AFRICAN JOURNAL OF CONTEMPORARY RESEARCH
ISSN: 26814-0761 (Print) 2814-0753 (e). Vol. 2 No. 1. 2021
A Publication of the Association for the Promotion of African Studies

CYBERCRIMES IN CONTEMPORARY NIGERIA: THE WAY FORWARD

Ejikemeuwa J. O. NDUBISI, PhD
Department of Philosophy & Religious Studies
Tansian University, Umunya, Anambra State, Nigeria
ejikon4u@yahoo.com; ejo.ndubisi@tansianuniversity.edu.ng
ORCID ID: https://orcid.org/0000-0002-2132-4309

Anthony Uzochukwu UFEAROH, PhD
Department of Philosophy,
Nnamdi Azikiwe University, Awka
tonito2006@yahoo.co.uk; au.ufearoh@unizik.edu.ng
ORCID: 0000-0003-2617-6808

Godspower Ifeanyi AKAWUKU
Department of Computer Science,
Nnamdi Azikiwe University, Awka
gi.akawuku@unizik.edu.ng

Abstract

Though the advent of modern technology has made human living quite appealing and literarily turned the world into a small village, it no doubt, comes with some negative effects especially in the area of Information Communication Technology (ICT). One of these adverse effects is the rising phenomenon of Cybercrime which has become a significant issue both in Nigeria and in other parts of the world. Cybercrime can take many forms, including online fraud, identity theft, cyber bullying, and the spread of malware. The lack of strong cyber security infrastructure in many African countries makes them more vulnerable to cyber-attacks, and the financial and social impacts of these crimes can be significant. The emergence of the modern technology, has raised dusts of controversies asking if we can cope without computer technology? How do we effectively control the misuse of computer technologies? Does cybercrime really exist? If it exists, in what forms can they be detected? Studies have proved that proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals restriction of cybercrimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Cybercrime is a threat against various institutions and people who are connected to the internet either through their computers or mobile technologies. The exponential increase of this crime in the society has become a strong issue that should not be overlooked. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation. In this regard, this paper employs the methods of analysis and hermeneutics. It focuses on the prominent cybercrimes carried out in contemporary Nigeria. Finally, it submits, among other things, that if we are to win *this war against cybercrimes in Nigeria, it requires combined efforts of both the government and the individual members of the society as outlined in this study.*

Keywords: Cybercrime, Nigeria, Government, Youth, Criminals

INTRODUCTION

In this contemporary society, the internet has become almost inevitable in our everyday life and activities. Everything we do seems to revolve round the internet and technological innovations such that the world has become a global village; people can now reach out to others in very faraway places without having to encounter much difficulties. One can now have access to information which one desires about virtually everything and everywhere in the world so far as one is connected to the internet. This internet consists of the cyber space. This cyber space is the environment where the communication on the internet takes place.

It is of general knowledge that whatever has an advantage definitely has some disadvantages attached to it and some abuses are bound to occur. These abuses in which people try to go contrary to the main objectives of this technological innovations for selfish interest by breaking their ways into the cyber space in ways that are inappropriate is what is known as cybercrime.

Undoubtedly, ICT, with all its benefits to the contemporary society and in a special way the industrialized world, is without some negative effects. The devastating negative consequences of the use of ICT can be summarized under a single term cybercrime. Cybercrime can be traced back to 1962 when Allen Scherr launched a cyber-attack against the MIT computer networks, stealing passwords from their database via punch cards.[1] Consequently, the thrust of this paper is to lay bare the tenets and issues of cybercrime in Africa and the contemporary world but with special focus on Nigeria. . The paper intends not only to x-ray the nature and causes of

[1] " History of cybercrime", Retrieved from https://arcticwolf.com/resources/blog/decade-of-cybercrime/ (Accessed: 28th December, 2022).

Cybercrime but also proffer possible solutions. But before we go further, it is pertinent that we have an exposé of cybercrime.

WHAT IS CYBER CRIME?

Cybercrime can be seen as any criminal activity which takes place on or over the medium of computer, internet or other technological innovations. Simply put, cybercrime can be seen as any illegal activity carried over on or with the help of internet or computer. Cybercrime, according to Maitanmi, Ogunlere and Ayinde, was defined as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes.[2] It is also defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is often very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. [3]

Cybercrime encompasses a wide range of crimes including stealing people's identity, fraud and financial crimes, pornography, selling contraband items online, creating and downloading illegal files etc.[4] The point here is that any illegal act carried out by the use of a computer and the internet is said to be cybercrime. Debarati Halder and Dr. K. Jaishankar summarized cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks

[2] O. Maitanmi, S. Ogunlere and S. Ayinde, *"Impact of Cyber Crimes on Nigerian Economy"*, The International Journal of Engineering and Science (IJES), Vol. 2, Issue 4 (2013), 46.

[3] Joseph Aghatise, "Cybercrime Definition", Retrieved from http://www.researchgate.net/publication/265350281 (Accessed: 17th December, 2022).

[4] "Computer Crime" Retrieved from http://en.wikipedia.org/wiki/Computer_crime (Accessed: 17th December, 2022).

such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"[5] For the purpose of this study, suffice it to say that cybercrime is a type of crime that involves computer gadget or computer network. It is simply understood as computer crime.

Generally, cybercrime may be divided into two categories: (a) Crimes that affect computer networks and devices directly. Examples are malicious code, computing viruses, malware etc. (b) Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Cyber Stalking, Fraud and identity theft, phishing scams and information warfare.[6] Collectively, the members of this group have come to discover that most cybercrime is an attack on information about individuals, corporations or governments.

CYBERCRIME IN THE CONTEMPORARY WORLD

Today cybercrimes have become so much a problem because there has been a massive improvement in technology. Cyber criminals have also used the contemporary technological developments to have a more advanced way of carrying out their crimes. Most cyber-crimes are committed by criminals whose major aim is to make money but sometimes they aim also to damage computers or networks for reasons other than profit like damaging evidences etc. These criminal acts can be carried out by individuals or organizations. Some are organized and they use advanced techniques and are highly technically skilled. Others are still novices. According to Microsoft's Digital Crimes Unit (DCU), "there are nearly 400 million victims of cybercrime each year. And cybercrime costs consumers 113 billion dollars a year based on statistics. India,

[5] Debarati Halder and K. Jaishankar, "Cyber crime", Retrieved from http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf (Accessed: 1st January, 2023).

[6] Anah Bijik Hassan, Funmi David Lass, Olatunji J. Makinde, "Cybercrime in Nigeria: Causes, Effects and the Way Out", *ARPN Journal of Science and Technology*, Vol. 2, No. 7 (2012), 626 – 631.

followed by Pakistan, Egypt, Brazil, Algeria, and Mexico, has the largest number of infected machines involving malware developed outside Eastern Europe"[7].

In our society today, there have been many ways of committing cybercrimes. We shall take a brief look on some of them below.

PROMINENT GLOBAL CYBERCRIMES

Some of the major cybercrimes in our world today can be summed up as follows:

1. Web Attack: A web attack affects the computer via the internet. These viruses can be downloaded from the internet and end up causing large- scale and irreversible damages to one's system.

2. SQL Injections: SQL injections is a type of cybercrime that effectively employs malicious codes and manipulates backend databases to access information that is not intended to be displayed. These mostly involve private and sensitive data items. SQL can have long- term devastating effects such as deletion of tables.

3. Malware Attacks: A malware attack is where a computer system or network is infected with a computer virus or other types of malware. A computer compromised by malware could be used by cyber criminals for several purposes. They include stealing confidential data, using the computer to carry out other dubious acts.

4. Phishing Attacks: This is the most prominent of them all in our world today. A phishing campaign is when spam emails, or other forms of communication, are sent with the intention of tricking recipients into doing something that undermines their security. Phishing campaign messages may contain infected attachments or links to malicious sites, or they may ask the receiver to respond with confidential information.

5. Spear phishing attacks: This is another type of phishing. This one is a targeted phishing campaign which tries to trick specific individuals into jeopardizing the security of the

[7] "Cybercrime in Africa: Facts and figures - Sub Saharan Africa", Retrieved from https://www.scidev.net/sub-sahara-africa/features/cybercrime-africa-facts-figures/ (Accessed 25th December 2022).

organization they work for.[8] Spear phishing messages are typically crafted to look like messages from a trusted source, etc.

6. Financial Crimes: With the increasing demand of the online banking, the financial crimes have become very alarming. Financial crimes include credit card frauds, stealing money from online banks etc. The criminals of credit card fraud get information from their victims often by impersonating a government official or people from financial organizations asking for their credit information. The victims fall prey to this without proper inquiries and give away their credit card information to these criminals. In these ways, criminals may steal their identity and the consequences are mostly financially damaging.

7. Cyber Pornography: Pornographic websites which allow downloading of pornographic movies, videos and pictures, on-line pornography magazines (photos, writings etc.), all come under this category.[9] The study made by the UK Home Affairs Committee Report on Computer Pornography (House of Commons, 1994) says that "Computer pornography is a new horror". The US Carnegie Mellon University is also one such institute that has made a wide range of study and collected evidences on child and computer pornography.[10]

8. Drug Trafficking: Drug traffickers contribute a major part of cybercrime to sell narcotics using the latest technologies for encrypting mails. They arrange where and how to make the exchange, mostly using couriers. Since there is no personal communication between the buyer

[8] "Various cyber threats", Retrieved from https://www.jigsawacademy.com/blogs/cyber-security/varios-cyber-threats/ (Accessed 29th December, 2022).

[9] Chatterjee Bela, "Last of the Rainmacs: Thinking about pornography in cyber space", In *Crime and the Internet*, ed. Wall David, Retrieved from https://www.research.lancs.ac.uk/portal/en/publicatios/-(d154cb98-427a-4966-bf3a-3078aab5ed75).html (Accessed: 2nd January 2023).

[10] Ibid.

and dealer, these exchanges are more comfortable for intimidated people to buy illegal drugs and even other items.

9. Cyber Terrorism: Terrorism acts which are committed in cyberspace are called cyber terrorism. Cyber terrorism may include a simple broadcast of information on the Internet about bomb attacks which may happen at a particular time in the future.[11] Cyber terrorists are people who threaten and coerce an individual, an organization or even a government by attacking them through computers and networks for their personal, political or social benefits.

10. Online Gambling: Online gambling is offered by thousands of websites that have their servers hosted abroad. These websites are the one of the most important sites for money launderers. This can be in form of trending betting stuffs especially in Nigeria.[12]

11. Cyber Stalking: 'Stalking' as has been defined in Oxford dictionary, means "pursuing stealthily". Cyber stalking is following an individual's or organization's whereabouts on the Internet. These may include sending threatening or nonthreatening messages on the victim's bulletin boards, which may be by social networking sites or even through e-mails. According to David Wall, one of the prevalent forms of Cybercrime is Cyber stalking. This is basically a crime where the individual is constantly harassed by another individual example, sending constant mails to any individual with unsuitable contents and threat messages.[13]

12. E-mail Spoofing and Phishing Scams: Cyber criminals often spoof e-mails of known and unknown individuals. E-mail spoofing basically means sending an e-mail from a source while it appears to have been sent from another e-mail. E-mail spoofing is a very common cause of

[11] David Wall, "Cybercrimes and Internet", *Crime and the Internet,* ed. S. W. David. ISBN 0-203-164504 ISBN 0-203-164504, 1.

[12] Ibid.

[13] Ibid.

monetary damages.[14]The act that attempts to obtain vital information like passwords, details of credit cards by pretending to be a trustworthy entity in an electronic company is called phishing. They are likely to contain hyperlinks to the sites containing malwares.

CYBERCRIMES IN NIGERIA

Africa as a continent is not left out of the menace of cybercrime as it seems many of her youths are actively involved in this illegal 'business'. Some Nigerian youths today seem to believe that 'Yahoo Yahoo' is now the order of the day and a means of livelihood. They have also taken it to social media, where they scam innocent people who are unsuspecting, either through fake online dating, fake company's ownership or other means. During the course of this work, it was discovered that it had gone so worse that some youths now believe that it is a form of payback to the whites who colonized us. Some have gone to the extent of even using diabolic means to make their 'clients' pay.

A study conducted by International Data Group Connect showed that each year, cybercrime cost the South African economy an estimated 573 million dollars. For the Nigerian economy the cost was estimated to be 500 million dollars, and for the Kenyan economy, 36 million dollars.[15] Another study conducted by Deloitte and dating back to 2011 showed that financial institutions in Kenya, Rwanda, Uganda, Tanzania, and Zambia had sustained losses of 245 million dollars, attributable to cyber fraud. Lastly, several Zambian commercial banks were defrauded of over 4 million dollars in the first semester of 2013, as a result of a complex cybercrime scheme involving Zambians as well as foreign nationals.[16]

[14] "Cybercrimes/Effects/Causes/Prevention", Retrieved from en.wikipedia.org/wiki/Phishing (Accessed 19th December, 2022).

[15] "Cybercrime in Africa: Facts and figures - Sub Saharan Africa", Retrieved from https://www.scidev.net/sub-sahara-africa/features/cybercrime-africa-facts-figures/ (Accessed 25th December 2022).

[16] Ibid.

In Nigeria today, there are various names given to cybercrime by our youths. Let's take a brief look at Yahoo, Yahoo plus, Oke-ite and other diabolic practices. The current trends of Yahoo in the whole of Africa and especially Nigeria is now of general knowledge. It has become so common that many of our youths no longer see it as a vice; it has rather been baptized and named 'hustling'. A great percentage of the Nigerian youths are in one way or the other involved in these practices. Our youths (most especially) now defraud people online of their hard earned money just to live up to some standards which they have set for themselves. It is even more worrisome to know that currently, as it seems the wave of 'Yahoo Yahoo' is gradually fading off as people are now more enlightened and these criminals hardly finds people to dupe, they have adopted another means which is generally termed 'Yahoo plus'.

Yahoo plus in the Nigerian parlance according to enquiries came from 'Yahoo Yahoo' which is a Popular name for internet scammers, most of whom operated with laptops and sometimes phones. When people became alert about internet scams, young boys started engaging native doctors to make charms for them to hypnotize and defraud victims, so as to be able to sponsor their extravagant life style. Some even recline to crypto currency as a backup but behind are fraudsters.

On the issue of *'Oke-ite'*, personal investigations indicate that '*Oke-ite'* is made by witch doctors with aims of accelerating accomplishments in life. '*Oke-ite*' makes one's accomplishments sudden and quicker. It is a charm used to manipulate nature to one's benefit but it is not without severe implications. As *'Oke-ite'* accelerates riches and accomplishments, it equally accelerates self- ruin, death, doom, pains, anguish and agony.[17] Though, this negative side of '*oke-ite*' is most at times not clearly explained to

[17] Nnatuanya Chinedu Emmanuel, "The rise of oke-ite ritual among the contemporary Igbo youths: The socio-religious implications," *AKU: An African Journal of Contemporary Research* Vol 3 No 2 (2022): 49, accessed January 2nd, 2023, doi: 10.13140/RG.2.2.14922.03528.

the proponents, but at other times, they are aware and usually get their motivation from the funny assertion "It is better to die young and rich than to die old and broke".

CAUSES OF CYBERCRIMES

The following are some of the identified causes of cybercrime

1. Unemployment: This is one of the major causes of Cybercrimes especially in Africa. It is a known fact that over 20 million graduates in Nigeria do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities as a means of survival and hence a drastic increase in the rate of yahoo yahoo.

2. Get rich quick syndrome: Another cause of cybercrime among Nigerian youths is get-rich-quick-syndrome. Youths of nowadays are generally very greedy; they are not ready to start small hence they strive to level up with their rich counterparts by engaging in cybercrimes.

3. Lack of functional Cyber Crime Laws: This also encourages the perpetrators to commit more crime knowing that they can always go unpunished or not even caught at all. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.

4. Incompetent security on personal computers: Some personal computers do not have proper or competent security controls; it is prone to criminal activities hence the information on it can be stolen.

5. Moral decadence also accounts for the high rate of cybercrime as people without strong moral principles give in easily to peer pressure as they believe that they can do whatever they want to without being questioned. This can also be seen mainly among the youths as the culture of due process keeps dying off daily.

POSSIBLE SOLUTIONS TO CYBERCRIMES IN NIGERIA

Cybercrimes have severe effects on the contemporary society, ranging from its ability to aid corruption, money laundering, undermining technological and socio-economic development of the country and on the overall, making youths to grow lazy by relying solely on cybercrimes. It is also interesting to note that a nation with high incidence of crime cannot grow or develop; hence cybercrime leaves negative social and economic repercussions. Using Nigeria as a case study, the prevalence of cybercrime has created a bad image for Nigeria among the committee of nations as one of the most corrupt nations in the world. This has gone a long way in tarnishing the image of Nigerians as well when it comes to the way and manner a Nigerian is treated abroad with suspicion and caution as Nigerians are stereotyped to be *419ers* and hence not to be trusted.

One fact we must not run away from is that cybercrime cannot be easily and completely eradicated, but can be reduced and managed. Hence, it requires collaborative efforts of individuals alongside with government intervention. In proffering solution to cybercrime, it requires a variety of aspects like protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

a. **Government's intervention:** Although the country has found herself in a great mess by the inability of the government to provide basic necessary amenities such as jobs, security and the likes for her citizens which indirectly has led to high rate in cybercrime, there is still need for the nation to come up with adequate laws to tackle this issue. These laws should be formulated by the government and should strictly be adhered to. However, it is worthy to note that a bill was passed in year 2015 that would combat and punish electronic fraud and other cyber related crimes. The full implementation of this bill will hopefully bring a strategic approach to fight against cybercrime. Some of the bills are highlighted below:

- There will be seven years jail term for offenders of different types of computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cybersquatting.[18]
- Defines the liability of service providers and ensures that the use of electronic communications does not compromise national interest. It provides a legal framework to punish cyber criminals thereby improving electronic communication.
- It specifies all criminal acts and provides guidelines for the investigation of such offences. If these laws are effectively enforced, cybercriminals will be deterred and penalized. This will

[18] Robert. Rowlingston, "Towards a Strategy for E-Crime Prevention", (ICGeS Global e Security, Proceedings of the 3rd Annual International Conference, London, England, April 2007), 3-4

indirectly reduce the incident of cybercrimes, increase customer's confidence while transacting business online and also correct the negative impression about Nigeria and the citizens.

b. **Individual knowledge**: on their part should ensure proper security controls and make sure they install the latest security updates on their computer systems. In addition, they should observe the following:[19]

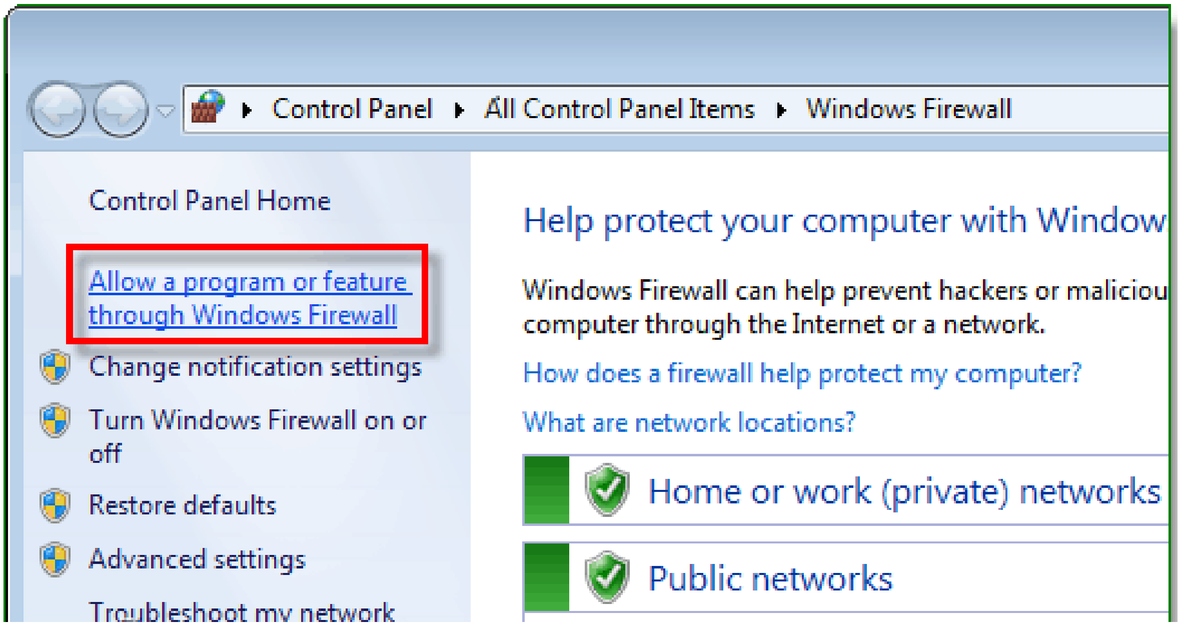
- Avoid pirated software and never disclose one's Personal Identification Number (PIN), bank account and email access code to unknown persons.
- Always ignore any e-mail requiring your financial information. Do not send sensitive information in an email since its security cannot be guaranteed.
- Use strong passwords that are difficult to guess and employ a combination of characters (upper case and lowercase letters), numbers and symbols.
- Avoid inputting your information in a pop-up. If you have interest in any offer you see on a pop up, it is always safer to go directly to the website of the retailer.[20]
- Avoid or never open (click on), any text message will unknown sender, mostly titled **sender**. They contain scripts capable of extracting your bank details when executed by clicking on it.
- WhatsApp's disappearing messages feature ensures that exchanged messages are automatically deleted for everyone after a specific period. To activate Disappearing messages in a given chat, tap the contact's name at the top and select Disappearing messages. Next, choose a period after which a message will be deleted.
- Since 2017, WhatsApp has offered two-step verification to all of its users. Once enabled, two-step verification makes it more difficult for someone to hack into your WhatsApp account. To enable two-step verification on WhatsApp just go to Settings > Account > Two-step verification > Enable. You'll then be asked to create a six-digit PIN which you'll be required to input every

[19] P. Lakshmi and M. Ishwarya, "Cyber Crime: Prevention & Detection", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 4, Issue 3 (2018), 112.

[20] J.R. Early, "Cyber-Bullying on Increase", Retrieved from http://www.tmcnet.com/usubmit/ 2010/02/07/4609017.htm (Accessed 30th December, 2022).

time you need to verify your phone number. You will also be prompted to enter your PIN periodically to help you remember it. [21]

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. To setup firewall for computer. From the Control panel, click System and Security. Click Check firewall status under Windows Firewall.


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
How does a firewall help protect my computer?
What are network locations?
Home or work (private) networks
Public networks

Help protect your computer with Window

Windows Firewall can help prevent hackers or maliciou computer through the Internet or a network.

Figure 1.0 Configuration of firewall on Windows [22]

c. **Technology:** the software or tech configuration applied is essential to giving an organization and individual the computer security(cybersecurity) needed. Tools needed to protect oneself from cyber-attacks are numerous. Three main entities must be protected: endpoint devices like

[21] Dave Parrack. How to Enable Two-Step Verification on WhatsApp, updated sept 30, 2021 Retrieved from https://www.makeuseof.com/tag/enable-two-step-verification-whatsapp/ (Accessed 22nd December, 2022).

[22] Dave Parrack, "How to Enable Two-Step Verification on WhatsApp", updated sept 30, 2021 Retrieved from https://www.makeuseof.com/tag/enable-two-step-verification-whatsapp/ (Accessed 22nd December, 2022).

computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, Domain Name System filtering, malware protection, antivirus software, and email security solutions.

If we are to win this war against cybercrime on the individual level and so as not to fall prey to cyber criminals, there is need for strict compliance to the above rules or guidelines. Other solutions would include: Re-orientation; Proper and good parenting; and celebration and rewards of good values etc.

CONCLUSION

As a starting point, it is quite important for one to take note of the truth about internet fraud. This fraudulent act is one of the most ever rapidly increasing forms of computer crime. The advent of the 'yahoo-boys' subculture in tertiary institutions has introduced another dimension of youth's involvement in cybercrime. Now, findings indicate that internet fraud in tertiary institutions are socially organized and highly networked. It is increasingly becoming specialized and sustained by informal networks. This involves nefarious networking of fellow fraudsters and bank staffs. The latter leak vital customer details to yahoo-boys and facilitate payment without alerting security agencies; while the former arranges bail-out option in crisis period. The money is paid through domiciliary accounts, cheques, credit cards, Money Gram and Western Union. Cybercrime was reported to yield benefits in paying their school fees, acquire properties (cars, lands etc.), and sustain a certain standard of living. This informal network will continue to circumvent any genuine drive to stop cyber-criminality in Nigeria. The Government must address the fear of unemployment and check unbridled corruption, and integrate moral values into the body polity. In our tertiary institutions, seeing the lecturers and others who have done so well for themselves academically not being able to live well and comfortably pay their bills will only but encourage young students to shun education with their regular slang of 'school na scam' and rather embrace cybercrime.

The wave of *Yahoo* is a glaring reflection of institutional anomie in Nigerian society. Parents have abdicated their surveillance and nurturing roles of their children and wards in pursuit of money. Institutional corruption among government officials; award of honorary degrees on perceived corrupt public officials by educational institutions and materialism being preached by religious institutions are negative contributors to the emergence and sustenance of yahoo-boys subculture in Nigerian tertiary institutions.[23] Stealing is a crime, duping people is a crime, deceit is also a crime, Yahoo is a crime and these should not be found among the youths which are the pillars and the future of the nation.[24] There is a clear cut difference between 'Need' and 'Want' and not being able

[23] Benard Hogan-Howe, "Met to Tackle the wave of cybercrime with world-leading unit published in the Evening Standard, 21st November 2013", Retrieved from http://www.standard.co.uk/news/crime/commentary-sir-bernardhoganhowe-on-new-cybercrime-push-8954716.html (Accessed 22nd December, 2022).

[24] Cyril Udebunu, Rector's conference, Pope JohnPaul II Major Seminary, Okpuno, 4th January 2022.

to differentiate between these has led to an increase in the rate of cybercrime just to fit in to the unrealistic standards.

Finally, with a young population that is rapidly adopting new technologies, Nigeria is on the verge of an Internet boom. These advances also bring with them new risks. To keep pace, initiatives by Nigerian leaders should seek to combat cybercrimes and improve Nigeria’s overall cyber security posture. It will take a concerted effort from international governments, industry, and civil society to reduce cybercrime and improve cyber protection and resilience so that Nigeria can reach its full potential in the global economy. As we wind down this paper, we wish to reecho the fact that the energy invested by the youths in cybercrime can be better channeled to technological development which will yield better output.