WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Menace of Rising Incidences of Cybercrimes Among Nigerian Youths

Chapman Eze Nnadozie

Principal Lecturer, Computer Science Department, Abubakar Tatari Ali Polytechnic, Bauchi, Bauchi state, Nigeria
Doi: https://doi.org/10.55248/gengpi.5.0624.1521

A B S T R A C T

Cybercrimes among the Nigerian youths are increasingly becoming a source of worry in our contemporary society. The objectives of this study are to find out the meaning of cybercrime and its effect on the society; investigate the root causes that has led to the increase in cybercrimes among our youths; and to proffer practical ways through which we can protect our devices as well as combat cybercrimes. The methodology adopted is the use of questionnaires which is administered on the educated working class in our society. The findings show that hacking of devices is rampant leading to devastating experiences on the part of their victims with the perceived notion that lack of employment and weakening parental checks on their wards forms the bedrock that has led to the increasing rate of cybercrimes among Nigerian youths. Furthermore, the findings show that regular user education on safe browsing as well as regular updating of ones' devices security software are highly recommended.

Keywords: *cybercrime, devices, security, software, updating, victims.*

1. Introduction

In today's digital age, which is embodied with lots of technological advancements, cybercrimes are bound to happen as criminals infiltrate systems in search of possible victims. The rising exposure of devices to a huge depository of data on the Internet makes cyberattacks even more prevalent. Cybercriminals are increasingly exploring new ways of compromising the confidentiality and integrity of the available data on the cyberspace. The attack can be targeted at anybody, group, or organization.

Cyberattack victims often incur losses of some sorts, which sometimes can be traceable through proper investigation. Regrettably, some can remain untraceable due to the use of some complex technologies such as usage of some sophisticated artificial intelligence tools. The most common attacks involve the stealing of customer's records from the organization's database, and identity theft that normally accrues from the hacking of the victim's phone number [1].

In this study, the author examines the menace that the rising cases of cybercrimes, mostly committed by the Nigerian youths, poses on the image of the country; and some practical ways through which we can protect our devices as well as combating cybercrimes.

2. Problem Definition

Nigerian youths are overwhelmingly seen to be the most populous part of our society. However, due to the rising unemployment rate and downplaying of some basic moral norms due to the biting economic challenges, has resulted to a surge in cybercrimes. This study is undertaken to delve into the menace of the rising incidences of cybercrimes among the Nigerian youths, the possible causes, and some practical ways through which the menace can be addressed.

3. Objectives of the Study

This study intends to –

1. Find out the meaning of cybercrime and its effect on the society.
2. Investigate the root causes that has led to the increase in cybercrimes among our youths.
3. Proffer practical ways through which we can protect our devices as well as combat cybercrimes.

4. Research Questions

The research questions advanced for this study are as follows -

1. What is cybercrime and its effect on the society?
2. What are the root causes that has led to the increase in cybercrimes among our youths?
3. What are the practical ways through which we can protect our devices and combat cybercrimes?

5. Literature Survey

Cybercrime is defined as "any criminal activity that involves a computer network or networked device". Cybercrimes are perpetuated by cybercriminals with the intent of stealing personal data for profit or corrupting the victim's computer. It can be classified as any of these – a lone person, a group of malicious persons, or a state sponsored actor [2].

Oftentimes, people make some unfounded assumptions. They think that their devices are perfectly protected once they have passwords on them. Beyond this assumption, there is need to ensure that extra layers are added to the security of our devices such as the use of two-factor authorization [3]. Furthermore, deleting data from your device is not enough because it is still within the system. You need to go to the recently deleted files folder or recycle bin as the case may be to completely get rid of such deleted data [3]. A recent report as quoted in [4] has it that in 2019 alone, data breaches occurred in the tune of over 7.9 billion across the globe. To this effect, rising breaches calls for increase in spending on cybersecurity. Gartner's prediction on cybersecurity is that its spending will increase to a glaring $250 billion globally by 2026 [4].

Cybersecurity domains come in terms of identification, protection/prevention, deletion, response/mitigation, and recovery [5]. Ransomware poses a high risk to cybersecurity. The threats were experienced more in 2021 globally and since then, it has been on the rise. Any device can fall prey to hacker's attack especially when it is not sufficiently protected [3]. Cybercrimes can be classified into two – inside attack and outside attack. The inside attack is perpetuated by individuals with valid authentication within an organization. Reasons for such attack could be as a sign of dissatisfaction with the management, revenge or possibly greed. It can also be for recognition. Internet Detection System (IDS) can be used to prevent this from happening. On the other hand, the outsider or external attack can be perpetuated by an individual outside the organization or in collaboration with an insider. These attacks could be structured or unstructured if the attacker is an experienced or amateur cybercriminal respectively [6]. Cybercrimes are reportedly growing by 15% annually and are estimated to attain a net worth of $10.5 billion by 2025 [2]. The damages caused by cybercrimes are enormous. These include diminishing of customer's trust on the organization, the running down of company's stock market, the possibility of the company getting sued by any of the customers for damages [2]. History has it that in Nigeria, '419' and 'yahoo-yahoo' were the crimes committed in the 1990s. This increased following the increase of internet usage between 2002 to 2003 by about 5%. In 2015, usage of the internet became over 40% which is now very rapid in subsequent years [7]. It is estimated that annually cybercrimes cost Nigeria 0.08 percent of its GDP. This when translated in naira stands at about 1.29 billion naira annually [7].

There are basically three factors that has led to the increase in cybercrimes. These factors are - online sale of technologies that can be used in hacking, rapid increase in the number of predators on the Internet, and the use of automation. Nowadays, hackers can easily buy the technologies they require to burst their quest. When they apply such technologies, they can easily see individual ports that are online and override their sessions or password and protection. Also, the rapid increase in the number of predators on the Internet has given room to this increment in cybercrimes. This is because people in developing countries are overwhelmed with lots of issues like youth unemployment, and they happen to be the ones that surf the net more seeking for predators to devour. Again, the use of automation technology has advanced cybercrimes in some sorts. This technology makes it possible for one to easily send a large number of spam emails at a time [8].

In Nigeria, the worsening economic woes has made it look as if youths are inefficient in terms of genuine aspirations. This has led to many of them turning to cybercrimes [9]. It is estimated that about 80% of the 978 convictions secured by EFCC as at September 2021 were all cybercrime related cases [10].

The frightening aspect of cybercrimes these days is the growing influence of artificial intelligence. This technology has advanced the attack from mere malware to the application of appropriate AI tools to perpetuate illicit actions. An example is a reported incident that happened in 2019 involving the loss of $243,000 by an energy firm in the United States. The hacker used an AI tool to crone the voice of the chief executive officer of the company directing the management to transfer the stated sum to a fictitious account. Cyberattacks can be either web-based attack or system-based attack. A web-based attack includes session hijacking, phishing, denial of service, etc. System-based attacks include all forms of malware, be it viruses or bots [11].

The increasing quest for materialism among youths has led to their minds been channelled to trying to make it at all cost. This is not healthy for our society. Sometimes, the parents are no longer monitoring their wards as they should, especially in the area of knowing what they do on the Internet. Many school children have their personal android phones. The increasing rate of unemployment is also adding weight to this problem of cybercrimes [9]. Furthermore, some youths see cybercrime as lucrative, and yet little money is needed to start such illicit business [9], [12]. Despite the fact that there is a high rate of unemployment, most youths do not want to learn vocational skills to earn a living. Everyone wants to go to school and work for government. Despite not having jobs, youths prefer to have a phone with internet access. The proliferation of lots of mobile phones has aided the increase of cybercrimes in the society [12], [13].

There are several kinds of cybercrimes. One of these is called cyberstalking. Cyberstalking refers to a form of crime that entails the threatening or harassing of a victim through the use of any form of messaging to force the victim give in to the perpetuator's demands. Another form of cybercrime is child pornography. Children and youths are exposed to child pornography. This is accelerated due to the rising need of the Internet to do their home works. The internet is no longer safe as they see themselves distracted with disgusting malwares and could be tempted to have a look. Forgery and counterfeiting are yet other forms of cybercrimes. Some youths learn how to do these things using the computer [6]. Other forms of cyberattacks include cyberextortion, identity theft, and software piracy. Cyberextortion refers to the launching of an attack and demanding money before you can stop attacking the victim online. It could be that the cybercriminal is in possession of some nude pictures of the victim and will threaten to post same on social network. Identity theft occurs when one's personal information is stolen by another. The perpetuator uses the victim's identity in the form of impersonation to commit crimes. Software piracy refers to the unlawful copying, distribution and use of one's software or work without prior permission from the original owner. All these constitute cybercrimes [2].

The authors in [9], [13], and [14] outline the following motives such as urbanization, unemployment, quest for wealth, negative role models, weak implementation of cybercrime laws and inadequately equipped law enforcement agencies as some of the reasons for the upsurge of cybercrimes in the society. Similarly, in some instances some parents are said to be culpable as they are seen to turn blind eyes when they know that their wards are engaging in training on the internet to learn how to successfully commit cybercrimes [13], [15]. The outcome of cybercrimes has always been devastating. Such outcomes include disruption of businesses, data manipulation or theft, creating a state of confusion through the tempering of basic infrastructure, and incurring financial losses on the victims [16].

6. Possible Ways of Protecting/Combating Cybercrimes

There are several ways through which one can protect one's devices from cyberattacks. To combat cybercrimes, our devices need to be protected from cybercriminals manipulation, and a need to re-orient freed offenders. The key highlights for protecting/combating cybercrimes in Nigeria includes the following – enhancement of user awareness, observing complete end of sessions once done online, avoiding suspicious mails, enhancing the use of BVN on bank accounts, formulating effective policies and legislations on cybercrimes, use of firewalls, creation of more job opportunities for our teeming youths, re-orientation of offenders, and finally youth enlightenment and mindset resetting.

1. Enhancement of user awareness.

All users must be very aware of the dangers associated with cybercrimes, and also understand how they can surf the net safely to avoid becoming a victim to any form of cyberattack [8]. Organizing workshops to create more user awareness on ways of combating cybercrimes can be done regularly [10].

2. Observing complete end of sessions once done online.

Whenever one is surfing the net, there is need to ensure that the session is completely ended when one is through with a particular app. Logging out from your account after the end of your session is a very effective way of ensuring the safety of one's personal data [13].

3. Avoid suspicious mails.

Always critically inspect any mail you receive on your email account to be certain that they are safe and genuine. This will enable you to be safe from phishing attacks. Same advice is applicable to the opening of links [17].

4. Enhance the use of BVN on bank accounts.

The use of BVN on every bank account is essential as it aids in tracing fraudulent activities, and by extension help in curbing cybercrimes [17].

5. Formulate effective policies and legislations on cybercrimes.

Taking collaborated efforts among all stakeholders in ensuring data safety, and formulation of efficient policies by government would help in curbing cybercrimes [9]. Similarly, there should be enacted laws to enforce property rights of individuals and organizations. Individuals need to be observant while surfing the net to ensure that they do not take simple rules on surfing the net for granted to avoid losing personal data or their property rights [7], [12].

6. Use of firewalls.

Firewalls use should be taken seriously. It is based on some rules like packet filtering and state inspection. Packet filtering ensures that the IP address of the packets are clearly stated and seen to be clear from anything malicious so as to know whether to allow or block such address. The stateful inspection, on its part, entails that the key features to watch out for are well defined for all packets. Windows operating system embedded firewall in its software. Therefore, users should be aware of the need to always update their firewalls while surfing the net for data or services [6].

7. Creation of more job opportunities for our teeming youths.

The government as a major stakeholder in every economy should ensure that conscious efforts are made to create more jobs for the teeming youths [9].

8. Re-orientation of offenders.

The EFCC boss stated that cybercriminals under his custody are being re-oriented on the positive means of making money through the use of the Internet. Furthermore, the parents of such wards have a role to play in ensuring that they are re-oriented to disabuse their minds from every form of criminality, after serving their jail terms [15].

9. Youths enlightenment and mindset resetting.

The youths should be enlightened on how best to channel their time for a better and productive task rather than resorting to cybercrimes. As a matter of fact, parents, teachers, and school heads should be actively engaging their students on why they should shun crimes [18].

7. Methodology

The main instrument used in carrying out this research is the use of questionnaire, consisting of nine (9) questions, which were administered on seven-eight (78) willing educated working-class personalities in the society. The author will derive its assertions through the analysis of the responses obtained, and compare same to already existing findings by other authors on the subject matter – Cybercrime. Table 1 shows the questions and their corresponding responses.

Sn.	Question	Yes	No	Uncertain
1.	Was your phone number ever hacked?	71 (91%)	4 (5%)	3 (4%)
2.	What effect did it have on you?	Open-ended	Open-ended	Open-ended
3.	Do you think that the proliferation of mobile devices has a significant effect on the increasing wave of cybercrimes?	69 (88%)	3 (4%)	6 (8%)
4.	Do you agree that lack of employment for the youths in Nigeria is aiding the surge on cybercrimes?	73 (94%)	0 (0%)	5 (6%)
5.	Do you see some parents culpable to their wards resolve for cybercrimes?	68 (87%)	4 (5%)	6 (8%)
6.	Are you an advocate of regular user education as a way of combating cybercrimes?	70 (90%)	3 (4%)	5 (6%)
7.	Do you belief ending your online sessions when done would enhance your device cybersecurity?	71 (91%)	5 (6%)	2 (2%)
8.	Do you regularly update your installed security software?	64 (82%)	10 (13%)	4 (5%)
9.	Do you regularly ensure that your computing device software is always having the latest software update?	67 (86%)	8 (10%)	3 (4%)

Table I: Questions and their respective responses.

8. Results and Discussion

This paper is geared towards investigating the menace of cybercrimes among Nigerian youths. Three (3) research questions were formulated by the author to address the subject matter. Questions 1 to 3 were meant to delve into the meaning of cybercrime and its effect on the society. Question 1 seeks to know whether the respondent's phone was ever hacked. In response, 71 representing 91% of the respondents say that their phone had been hacked at one point or the other. This is based on the fact that the cybercriminals have seen that they can make illicit gains out of them because of their working status. Question 2 is an open-ended question which seeks to know the effect such an act had on its victims. The overwhelming effect was really devasting and tiring on the victims. A vast majority had the hacking of their phones through their WhatsApp accounts as the hacker was in possession of their WhatsApp contact for a period of one (1) to two (2) weeks before the victims were finally able to retrieve their numbers. In addition, most of them kept using the number without knowing that the registration has been swapped in favour of the hawker. They had to approach their respective service providers later to have their numbers retrieved. Question 3 seeks to know the view of the respondents on whether the proliferation of mobile devices has any significant effect on the increasing wave of cybercrimes. An overwhelming majority (88% of the respondents) belief that the proliferation of mobile devices has a significant effect on the increasing wave of cybercrimes. This assertion is in line with the findings of [12] and [13] which say that the proliferation of lots of mobile phones has aided the increase of cybercrimes in the society. Figure 1 shows the responses of the respondents in respect of research question 1.

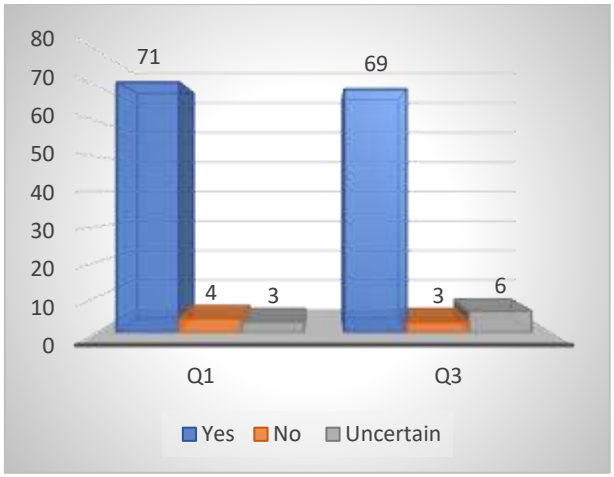

Fig. 1: Responses on cybercrime and its effect on the society.

Questions 4 and 5 seeks to ascertain the root causes that has led to the increase in cybercrime among the youths. Question 4 seeks to know whether the respondents agree that lack of employment for the youths in Nigeria is aiding the surge on cybercrimes. In response, 94% of the respondents assert to this claim. This assertion is in line with the findings of [9], [13], and [14] when they said that motives such as urbanization, unemployment, quest for wealth, and others are some of the reasons for the upsurge in cybercrimes.

Question 5 seeks their views on whether parents should be held culpable for their ward's resolve in cybercrime. In response, 68, 4, and 6 respondents say "yes", "no", and "uncertain" respectively. This implies that the vast majority belief that the parents are culpable, to a reasonable extent, on their child's misconduct. This assertion is in line with the findings of [13] and [15] when they say that some parents are culpable as they are seen to turn blind eyes to their wards activities even when they know that they are having the Internet training to learn how to successfully commit cybercrimes. Figure 2 shows the bar chart representing the responses of the respondents in respect of research question 2.

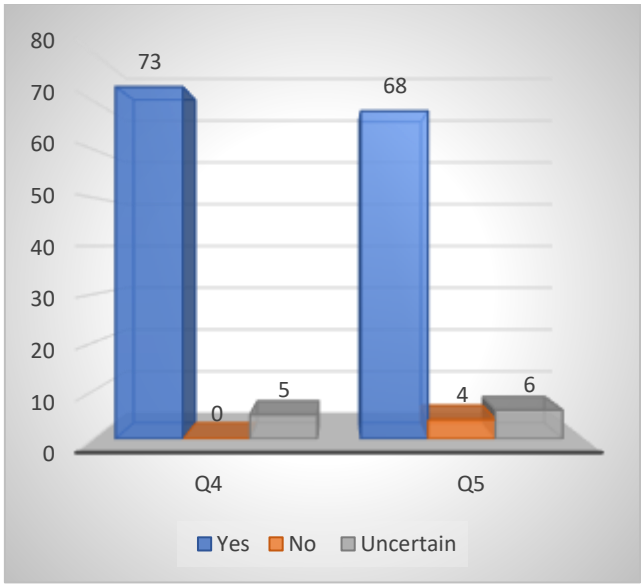

Fig. 2: Responses on the root causes of the rising rate in cybercrimes.

Research question 3 seeks to ascertain the practical ways through which we can protect our devices and combat cybercrimes. Questions 6 to 9 were framed to address it. Question 6 seeks to know their views on regular user education as a way of combating cybercrimes. In response, 70, 3 and 5 of the respondents say "yes", "no", and "uncertain" respectively. This shows that the majority belief that regular user education can be seen as a way of combating cybercrimes. This assertion is in line with the finding of [18] when it says that the youths should be enlightened on how best to channel their time for better and productive tasks rather than resorting to cybercrimes. Similarly, the assertion is in line with the finding of [15] which emphasizes on the need to re-orient the minds of our youths on the positive means of making money.

Question 7 seeks to know whether the respondents know that ending online sessions when done can enhance their devices' security. The responses show that majority of the respondents, which stands at 71 out of the 78 respondents, is aware that ending their online sessions when done with certain apps can enhance their devices' cybersecurity. This assertion is in line with the finding of [13] which emphasises on the need to end sessions completely when done online.

Question 8 seeks to know whether the respondents regularly updates their installed security software. From the responses, majority of the respondents (64 to be precise) are aware of the need for regular updates and they always ensure that they do that regularly. This assertion is a good development as it enhances the safety of their devices.

Question 9 seeks to verify whether the respondents always ensure that their device software is always up-to-date with the device latest software. The responses show that majority of the respondents (that is 67 in number) has their devices software regularly updated, which is a welcomed development as this enhances the security of the devices. Figure 3 shows the bar chart of the responses obtained in respect of research question 3.

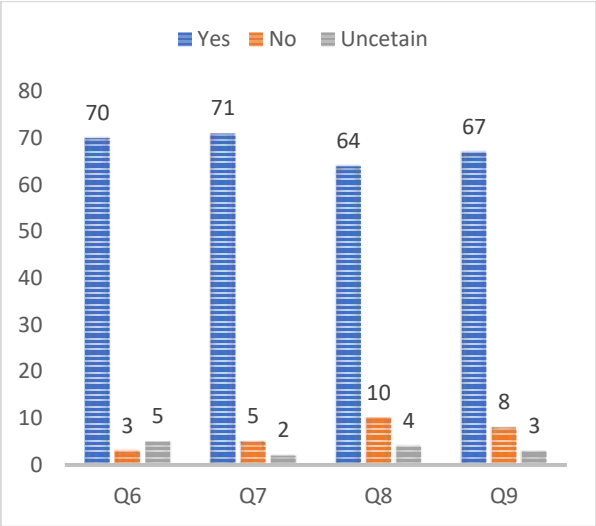

Fig. 3: Responses on the practical ways of protecting and combating cybercrime.

9. Conclusion and Recommendations

Nigeria as a country is blessed with enormous resources, and lots of vibrant youths whose energies need to be channelled towards production rather than their resorting to cybercrimes. The study has shown that the major driver to the rising involvement of youths on cybercrimes is unemployment and perceived lapses on positive proper parenting.

The author strongly recommends that the government should be up and doing in ensuring that they show exemplary leadership through - curbing the high rate of corruption in the society; creating more jobs for the youths; and delivering a more conducive environment for businesses to grow by especially tackling the incessant power supply. It is no longer news that the country had been and is still battling with incessant power cuts on a daily basis which sometimes results to the citizenry painfully enduring lack of electricity for some days. On the part of the parents and teachers, there is need to ensure that the youths are properly guided especially when they are still tender in age in order to inculcate in them the right moral values.

References

[1] Bendovschi, A. (2015). *"Cyber-attacks trends, patterns and security countermeasures"*, 7th International Conference on Financial Criminology, pp. 24 - 31. An open source article published by Elsevier B. V.

[2] Brush, K. & Cobb, M. (2024). "*Cybercrime".* Available at: https://www.techtarget.com/searchsecurity/definition/cybercrime

[3] Kelley, K. (2023). "*What is cybersecurity and why it is important?".* Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

[4] Kaspersky Lab. (2023). "*What is cyber security?".* Available at https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[5] Callejas, J. F., et al. (2021). "*Cybersecurity in the United Nations System Organizations".* Report of the Joint Inspection Unit of the United Nations.

[6] Pande, J. (2017). *"Introduction to cyber security".* Haldwani: Uttarakhand Open University Available at: https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

[7] NCC (2017). *"Effects of cybercrime on foreign direct investment and national development".* A 100pp final report from the NCC Department of New Media and Information Security. Consultant: Newark Security Systems Ltd.

[8] Schreier, F. Weekes, B. & Winkler, T. H. (2015). *"Cyber security: The road ahead".* Available at:

https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

[9] Ajibike, T. (2019). *"Youth and cybercrime in Nigeria".* Punch Newspaper dated 15th March, 2019. Available at: https://thoughtlabgroup.com/cyber-solutions-riskier-world/

[10] Guardian Nigeria (2021). *"80% of EFCC's 978 convictions cybercrime related".* A report in the Guardian Newspaper, 7rh October, 2021. Available at: https://guardian.ng/news/80-of-efccs-978-convictions-cybercrime-related/

[11] Malla Reddy College (2021). *"Digital notes on cyber security (R18A0521)",* A lecture note from the Department of Information Technology, Malta Reddy College of Engineering & Technology, India.

[12] Ejikr, S. (2023). *"EFCC secures conviction of 1,084 cyber criminals, 395 fraud cases".* A report article in Tribune Newspaper, November 8, 2023.

[13] Ebelogu, C. U., et al. (2019). *"Cybercrime, its adherent negative effects on Nigerian youths and the society at large: Positive solutions". In International Journal of Advances in Scientific Research and Engineering (1), vol. 5 (12), December, 2019.*

[14] NCC (2017). *"Effects of cybercrime on foreign direct investment and national development".* A 100pp final report from the NCC Department of New Media and Information Security. Consultant: Newark Security Systems Ltd.

[15] Olukoyode, O. (2023). *"EFCC adopts new strategy to curb cybercrime".* Available at: https://www.efcc.gov.ng/efcc/news-and-information/news-release/9054-efcc-adopts-new-strategy-to-curb-cybercrime

[16] Zope, A. P. & Chaudhari, R. R. (2022). *"A review paper on cyber security".* In International Journal of Engineering & Technology (IRJET), Volume 09, Issue 08, August 2022, pp. 1561- 1566.

[17] Florakis, C. Lovica, C. et al. (2020). "*Cybersecurity risk: A working paper",* No. 2020 – 178. Chicago: Becker Friedman Institute. December 2020. Available at: https://bfi.uchicago.edu/wp content/uploads/2020/12/BFI_WP_2020178.pdf

[18] Olukoyede, O. (2023). *"Youths involvement in cybercrime threat to future leadership – EFCC".* A Punch Newspaper report of 7th December 2023. Available at: https://punchng.com/youths-involvement-in-cybercrime-threat-to-future-leadership-efcc/