The Impact of Cyber Security on Nigerian Digital Economy

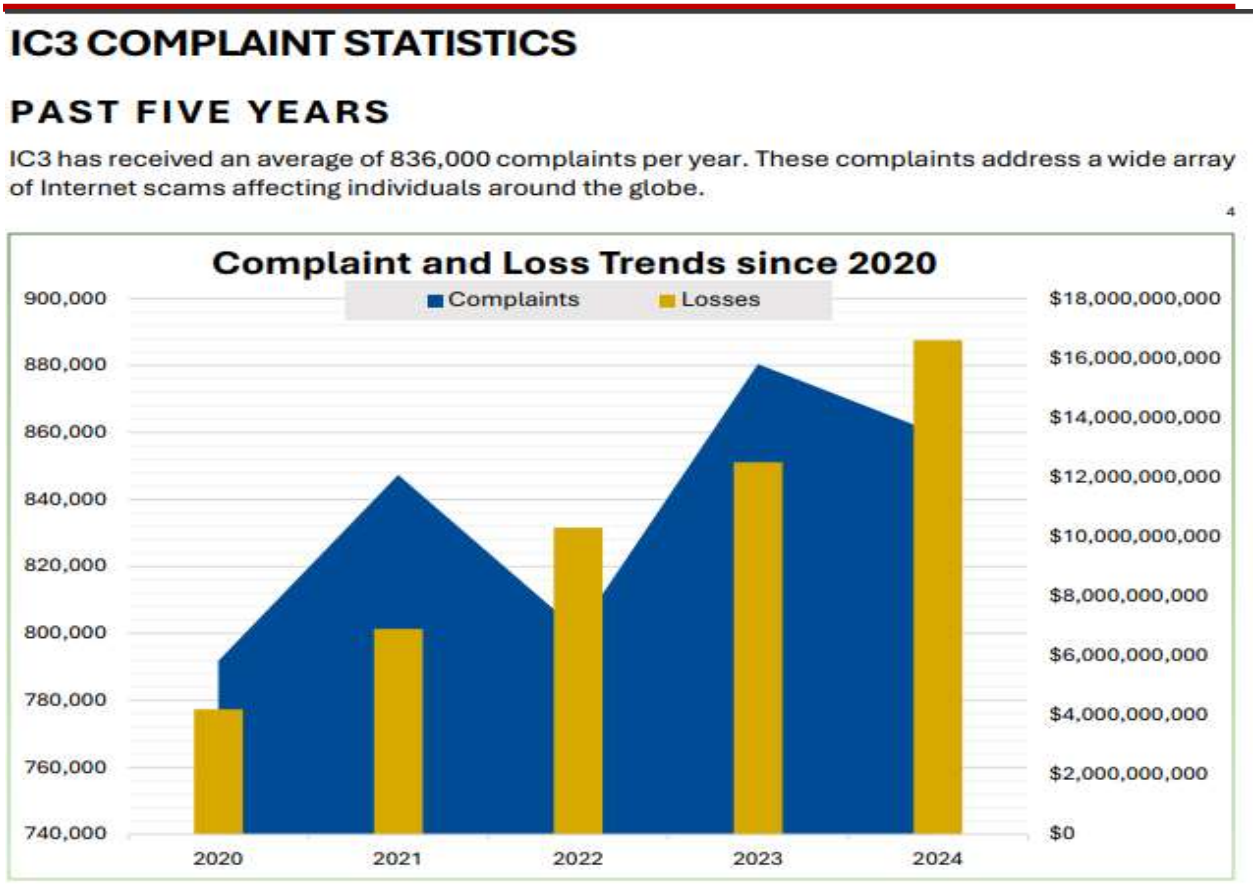
Nwosu John Nwachukwu PhD
Department of Computer Science, Federal Polytechnic, Oko, Anambra State
Phone number: 08035902385 Email: drnwosu2023@gmail.com
DOI: 10.56201/ijcsmt.vol.11.no10.2025.pg1.11

Abstract
The purpose of the research is to examine the impact of cybercrime on Nigeria Digital Economy. Literature study was used to collect data from various materials that include libraries, the internet, books, journals, magazine, and historical stories. Data were also collected from Federal Bureau of Information (FBI), United Nations Conference on Trade and Development (UNCTAD), Economic and Financial Commission (EFCC) site, Nigeria Information Technology Development Agency (NITDA) site, The Economist Intelligence Unit report, Federal Ministry of Communications and Digital Economy report, and World Bank report. Survey method that included questionnaire was used to find out the factors that were responsible for cybercrime in Nigeria. The analysis and discussion shows that digital economy will lead to new jobs, new forms of digital work, new opportunities in digital ecosystem, increased competition from local and foreign digital firms, enhanced productivity from data driven business models, greater control of value chains using platforms-based business models, more tax revenue resulting from increased economic activities. However, cybercrime poses a significant threat to Nigeria's digital economy with far-reaching consequences for businesses, individuals and the nation as a whole. The rise of digital technologies has created new opportunities for cybercriminals to exploit vulnerabilities resulting in substantial financial losses, decline in investor confidence, damage to Small and Medium-sized Enterprises (SMEs), inhibited digital participation and damage to business reputation.

1.0 Introduction

The emergence of the Internet along with new technologies has defined new ways of doing business, research, handle entertainment, carrying out government functions, etc. These benefits that are made possible by the use of the Internet, however, opened frontier for criminal activities called cybercrime (Saban, McGiven, Saykievicz, & Napolean, 2002).
Cybercrime is a crime that involves computer and networks. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet network (Okeshola & Adeta, 2013). The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s (Maitanmi, 2013). In cybercrime, computer may be target of the crime or used to commit the crime (Kruse & Heiser, 2002). Computer is a major source of evidence in cyberspace because either that it is used to commit a crime, a target of crime, or it is used to keep record of criminal log file.

Cybercrime has been on the increase for the immediate past years. A report from Federal Bureau of Information (FBI) that covered the period 2020 to 2024 shows that cybercrimes such as phishing, non-payment/non delivery, extortion, personal data breach and identity theft has been on the increase in the years surveyed.



(Source: FBI Internet Crime Report 2024)

Within the period surveyed, a total of 4.2 million complaints were received, 50.5 billion in losses and an average of 836,000. The period which has many people working remotely led to the emergence of different forms of cybercrime.

1.1 Purpose of the study

The purpose of this research is to examine the impact of cybercrime on Nigeria Digital Economy. The following specific objectives are required:

i. To find out the different types of cybercrime that is prevalent in Nigeria
ii. To find out the factors responsible for cybercrime in Nigeria, and
iii. To find out the impact of cybercrime in Nigeria Digital Economy.

1.2 Methodology

Literature study was used to collect information and data from various materials that include libraries, the internet, books, journals, magazine, and historical stories. Data were also collected from Federal Bureau of Information (FBI), United Nations Conference on Trade and Development (UNCTAD), Economic and Financial Commission (EFCC) site, Nigeria Information Technology Development Agency (NITDA) site, The Economist Intelligence Unit report, Federal Ministry of Communications and Digital Economy report, and World Bank report. Survey method that included questionnaire was used to find out the factors that were responsible for cybercrime in Nigeria. Two campuses of Federal Polytechnic, Oko (Atani Campus and Oko Campus) were used to represents youths, 10 members of the entertainment industry (5musicians and 5 actors), and 25

companies selected from Onitsha and Nnewi were used for data collection. Data obtained from 100 students from each of the campus, 10 members of the entertainment industry and 5 members each of management of each company make a total of 250 as sample size of the study. Out of 250 people 200 responded which is 80%. The survey respondents were small but informative and accurate because the instrument was reviewed before its use. Content analysis technique was used to obtain valid inference for the study.

1.3 Research Questions

The relevant research questions related to this study include the following:

1. What are the different types of cybercrimes in Nigeria?
2. What are the factors responsible for cybercrimes in Nigeria?
3. What are the impacts of cybercrimes to Nigeria Digital Economy?

2.0 Literature review

2.1 Cybercrime

A computer crime is any criminal activity that uses a computer system or computer network as an instrument or target of crime. Cybercrime encompasses a wide range of criminal activities that are carried out using digital devices and/or networks. Cybercriminals may exploit vulnerabilities in computer systems and networks to gain unauthorized access, steal sensitive information, disrupt services, and cause financial or reputational harm to individuals, organizations, and governments (Sukhai, 2004).

The World Economic Forum's 2023 Global Risks Report ranked cybercrime as one of the top 10 risks facing the world today and for the next 10 years (Heading & Zahidi, 2023). If viewed as a nation state, cybercrime would count as the third largest economy in the world. In numbers, cybercrime is predicted to cause over 9 trillion US dollars in damages worldwide in 2024 (Freeze, 2023).

2.2 Types of Cybercrime

EFFC alert site enumerated some of the cybercrimes to include, romance scam, e-commerce/card, employment scam, wonder bank/ponzi scheme, identity theft/phishing, contract scam/fund transfer, inheritance scam, charity scam, juju scam, crude oil/mineral, resources sales scam, scholarship scam, auction/product scam, emergency scam, immigration/visa scam, and local purchase order scam. (EFCC, 2023).

National Cyber Security Policy and Strategy (2021) however, enumerated contents of cybercrime to include phishing, Business Email Compromise (BEC), ransomware and malware, intellectual theft, and international property rights. Other emerging threats include machine learning poisoning, deep fakes, cloud hijacking, artificial intelligence fussing and crypto currency.

In 2000, the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders classified cyber crimes into five categories: unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorized interception of data within a system or network, and computer espionage (Sukhai, 2004).

Some examples of computer crime are hacking, phishing, ransomware, malware distribution, cyber bullying and cyber infrastructure disruption, cyber espionage and cyber vandalism.

Hacking

Hacking in cyber security refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity (Fortinet, 2025).

Hackers use a combination of different techniques to gain unauthorized access to a system. These include social engineering (exploiting human error to gain access to personal information using a fake identity and various psychological tricks), phishing scams, spam emails, instant messages, or even fake websites. They also use a trial and error method is known as a brute force attack, which involves guessing every possible combination of passwords in order to gain access, use of open wireless networks on routers that are not secured, and using programs to track every keystroke a computer user makes (Kaspersky, 2025).

Phishing

Phishing is a type of cyber attack that uses fraudulent emails, text messages, phone calls or websites to trick people into sharing sensitive data, downloading malware or otherwise exposing themselves to cybercrime. In phishing scam, a hacker pretends to be someone the victim trusts, like a colleague, friend, boss, authority figure or representative of a well-known brand.

Phishing is commonly used in romance scams, employment scam, wonder bank/ponzi Scheme, identity theft, contract scam, fund transfer, inheritance scam, charity scam, juju scam, resources sales scam, scholarship scam, auction/product scam, emergency scam, Immigration/visa scam, and Local Purchase Order (IPO) scam, etc. The mode of operation usually involves a hacker sending a message directing the victim to pay an invoice, open an attachment, click a link or take some other action. That "invoice" might lead directly to a hacker's account. That attachment might install ransomware on the user's device. That link might take the user to a website that steals credit card numbers, bank account numbers, login credentials or other personal data. Phishing exploits people rather than technological vulnerabilities (Kosinki, 2025).

Ransomware

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. The United States Cybersecurity and Infrastructure Security Agency (CISA) observed that in recent years, ransomware incidents have become increasingly prevalent among the Nation’s state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations (CISA, 2025).

Malware distribution

Malware (a portmanteau of malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy (Tahir, 2018)

Malware include computer viruses, worms, Trojan horses, logic bombs, ransomware, spyware, adware, rogue software, wipers and keyloggers

Cyber bullying

Cyber bullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted (UNICEF, 2025). Examples include: spreading lies about or posting embarrassing photos or videos of someone on social media sending hurtful, abusive or threatening messages, images or videos via messaging platforms impersonating someone and sending mean messages to others on their behalf or through fake accounts engaging in sexual harassment or bullying using generative AI tools.

Disrupting critical infrastructure

Public institutions and critical infrastructures are quickly becoming top targets for cybercrime around the world, and this can have detrimental effects on the countries, organizations, and all people that rely on them. Attacks on infrastructures have increased because companies are increasingly more reliant on connectivity and developments like remote work and the IoT revolution have hastened the trend on interconnectedness, opening more doors for cybercriminals to strike (Candan, 2024).

Cyber espionage

This is the act of obtaining secrets and information from the computers or networks without the permission and knowledge of the holder of the information using methods such as cracking techniques and malicious software. It involves access to sensitive, classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons. More recently, cyber spying involves analysis of public activity on social networking sites like Facebook, Whatsapp, X(former Twitter), etc.

The most common targets of cyber espionage include large corporations, government agencies, academic institutions, think tanks or other organizations that possess valuable IP and technical data that can create a competitive advantage for another organization or government. Targeted campaigns can also be waged against individuals, such as prominent political leaders and government officials, business executives and even celebrities.

Cyber spies most commonly attempt to access the following assets: research & development data and activity, academic research data, IP, such as product formulas or blueprints, salaries, bonus structures and other sensitive information regarding organizational finances and expenditures, client or customer lists and payment structures, business goals, strategic plans and marketing tactics, political strategies, affiliations and communications and military intelligence (Baker, 2025).

Cyber espionage attacks most often involves social engineering that triggers activities and are sustained through advanced persistent threat (ATP) where the attacker gained entrance into the system, conceals itself and takes times to identify vulnerabilities before launching an attack.

Cyber vandalism

Cyber vandalism is the deliberate and malicious act of carrying out digital destruction, disruption, or defacement of online assets like websites, data, or systems. Though it targets websites and other tech products, it can also be used to threaten individuals or institutions.

A user who causes cyber vandalism is known as cyber vandals. Cyber vandals use all sorts of tools to deface websites, delete files, take over user accounts, or send spam and viruses. The result of cyber vandalism can have a huge impact ranging from financial loss or compromising of personal or high-level security data (Greekforgreek, 2025).

3.0 Findings

Factors responsible for cybercrime in Nigeria

The researcher collected the data from the respondents through email and direct from the interview after the distribution of questionnaires to respondents. Five-point rating scale was used to record score of all positive statement. The ranged is from 5-1 for different response categories. The response categories are: Strongly Agree (SA), Agree (A), Undecided (U),

Disagree (DA) and Strongly Disagree (SDA). The data was analyzed in terms of percentage in which they occur.

The findings drawn out from the data analysis are as under:

Table 1: Why computers or network are tools target or place for cybercrimes?

S/N	**REASONS**	**SA**	**A**	**U**	**DA**	**SDA**
1	**Availability**	**100 (50)**	**80 (40)**	**10 (5)**	**10 (5)**	**0 (0)**
2	**Easy Access**	**70 (35)**	**100 (50)**	**10 (5)**	**10 (5)**	**10 (5)**
3	**Affordability**	**60 (30)**	**100 (50)**	**20 (10)**	**10 (5)**	**10 (5)**

The researcher again wanted to explore why the computer or network are tools target for cybercrimes. Results of Table 1 indicates that 90% of respondents said it is because computers are available nowadays everywhere. Significant respondents (85%) were of the opinion that it is easy to access computers which are connected to the internet. Similarly, a sufficient number of respondents (80%) supported that nowadays computers or mobile phones are affordable and people may browse cheaply internet.

Table 2: What are the factors contributing to cybercrimes?

S/N	REASONS	SA	A	U	DA	SDA
1	Growth of Technology	90 (45)	70 (35)	0 (0)	20 (10)	20 (0)
2	Economic factor	100 (50)	60 (30)	20 (10)	10 (5)	10 (5)
3	Ignorance	60 (50)	100 (30)	20 (10)	10 (5)	10 (0)

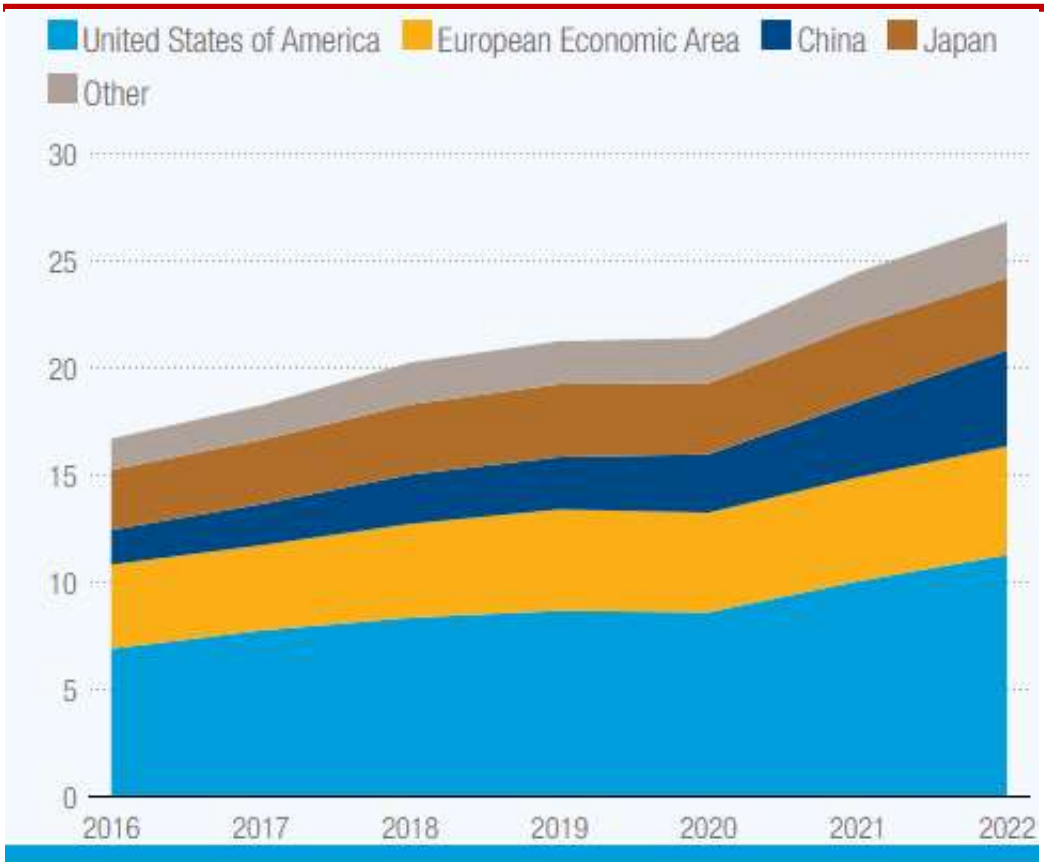
It is evident from table 2 that majority of respondents (80%) said that the growth of technology is one among factors that contribute to the existing of cybercrimes. Similarly, a sufficient majority of respondents (80%) supported that economic is another factor. And another percentage of respondents (90%) supported that ignorance is a factor that contribute to cybercrime.

4.0 Discussion

As it shown in the findings from Table 1, there are almost three reasons as responded by 90% of respondents who said availability, 85% easy access and 80% said computers are affordable. Availability and easy access to computer and internet have contributed much to the cybercrime activities. It is affordable to buy computer and to access internet and therefore many people are using technology in their daily activities whether at home or workplaces. Due to this advancement of using technology, the technology has become the tool target or place of criminal activities. 'As the Internet and computer communications technologies are increasingly inexpensive and available, the opportunities for individuals to engage in harassment via electronic methods, or cyber harassment, have increased significantly' (Chang & Holt, 2010). As the technology grows, the threat to the society increases. This is supported from the findings in Table 2 where by 80% of respondents said that one among factors which contribute to cybercrimes is technology growth. 'A recent survey conducted by Gartner Group of 160 retail companies selling products over the internet reveals that the amount of credit card fraud is 12 times higher online than in the physical retail world (Oates, 2001). Phonographic Industries (Gunter, Higgins and Gealt, 2010) has estimated that a third of all CDs are pirated. As revealed from table 2, ignorance is a major factor that contributes to the rise in cybercrime. Many crimes such as romance scam, card fraud and employment scam result from ignorance rather than economic factor.

5.0 The Impact of cybercrime on Digital Economy.

Digital economy refers to an economy that is based on digital computing technologies. It involved the utilization of information and communication technologies (ICT) across all business sectors to enhance its productivity (OCED, 2014). Measuring the digital economy and related value creation and capture is fraught with difficulties.



(Source: Digital Economy Report of United Nations of Trade and Development, 2024)
The report shows E-commerce sales by companies across 43 economies that represent 75% of global gross domestic product (GDP), trillions of dollars in current prices, 2016–2022.

From the report, business e-commerce sales grew by nearly 60% from 2016 to reach $27 trillion in 2022. The rise in digital economy will lead to new jobs, new forms of digital work, new opportunities in digital ecosystem, increased competition from local and foreign digital firms, enhanced productivity from data driven business models, greater control of value chains using platforms-based business models, more tax revenue resulting from increased economic activities. However, the rise of digital technologies has created new opportunities for cybercriminals to exploit vulnerabilities resulting in substantial financial losses, decline in investor confidence, damage to Small and Medium-sized Enterprises (SMEs), inhibited digital participation and damage to business reputation.

6.0 Preventive measures from cybercrimes

Preventing cyber-criminals' activities is not an easy task because cyber criminals are often difficult to identify since they commit their crimes at the very long distance from their victims. Despite these challenges, Buxton (2025) identified some measures that can be taken to prevent the occurrence of cyber crimes. These measures include use of strong passwords and enable 2FA, keep your software updated, manage your social media settings, strength your home network, keep up to date on major security breaches, monitor your bank statements, protect your personal information online, don't click on suspicious links, take measures to help protect yourself against

identity theft, use of full-service internet security suite, and know what to do if you become a victim.

7.0 Conclusion

Cybercrimes has impacted negatively on the Nigeria digital economy. Digital driven economy is the alternative to the migration from oil driven economy. Modern activities involve many businesses working online, making the cyberspace to become the market place for many businesses. Most digital platforms are designed to simplify activities so that individuals, small medium and large scale businesses, and governments can perform activities smoothly and without hindrance. However, the activities of cyber criminals are driving some multinational companies away from investing in Nigeria. Some individuals and local firms are finding it difficult to trust the Nigeria cyberspace. With the implementation of the stated preventive measures, there is hope of curbing the menace.

8.0 References

Baker, K. (2025, September 23). *Cyber espionage explained.* Crowdstrike. https://www.crordsrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage

Buxton (2025, July 21). How to prevent cyber crime: 11 ways to protect against threats. Norton. https://www.us.norton.com.

Candan, B. (2024, July 24). *Top 5 critical infrastructure cyberattaks.* Anapaya. https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks

Chang, S. & Holt, T. J. (2010). Cyber bullying in Chinese Web Forums- An examination of nature and extent. *International Journal of Cyber Criminology Vol.4*(2), pp 672-684.

The United States Cybersecurity and Infrastructure Security Agency (CISA; 2025).Ransomware. https://www.cisa.gov

Economic and Financial Crime Commission (EFCC; 2022). Types of cyber crime. https://www.efccnigeria.org.

Fortinet (2025, June 7). What is hacking. https://www.fortinet.com

Greekforgreek (2025, July, 15). What is Cyber Vandalism and How to Avoid It? Greekforgreek. https://www.geeksforgeeks.org/computer-networks/what-is-cyber-vandalism-and-how-to-avoid-it/

Gunter, W., Higgins, G. and Gealt, R. (2010). Pirating Youth: Examining the Correlates of Digital Music Piracy among Adolescents. *International Journal of Cyber criminology Vol 4*(2), pp 657-671

Heading, S. & Zahidi, S. (2024, February 3). The Global Risks Report 2023, 18th Edition. World Economic Forum. https://www.weforum.org4.

Kaspersky (2025, June 8). What is hacking? Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-hacking

Kosinki, M. (2025, June 28). What is phishing? Ibm. https://www.ibm.com/think/topics/phishing

Kruse, W. & Heiser, J. (2002). Computer Forensic: Incidents, Response Essentials. Amazon. https:// www.amazon.com.

Maitanmi, O. (2013, January 5, 2025). Cybercrime in Nigeria: Analysis, Detection and Presentation. Researchgate. http/www.researchgate.com.

Moore, R., Tarun, N & Lee, T (2010). Examining factors that influence a Youth's potential to become a Victim of Online Harassment. *International Journal of Cyber criminology Vol 4* (2), p 685-698.

National Cyber Security Policy and Strategy (2021). Meaning of cybercrime. Cert. https://www.cert.gov.ng

Oates, B. (2001). Cybercrime: how technology makes it easy and what to do about it: *Journal of Information Systems Management, Summer2001, Vol. 18* (3). p92.

Okeshola, B. F., & Adeta K. A. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna State, Nigeria. Ijrs. http:/www.ijrs.com

Saban, K. A.; MeGivern, E., Saykiewicz, J. N. (2002); A critical look at the impact of cybercrime on consumer behavior. *Journal of Marketing Theory and Practice, Vol. 10* (2), p2.

Sukhai, N. (2004, October 8). Hacking and cybercrime. *Proceedings of the 1st annual conference on Information security curriculum development. New York, NY, USA: ACM.* pp. 128–132. doi:10.1145/1059524.1059553. ISBN 1-59593-048-5. S2CID 46562809.

Tahir, R. (2018). A study on malware and malware detection techniques. *International Journal Management Engineering, 8*(2), 20 . https://www.cisa.gov/stopransomware

UNICEF (2025). Cyberbullying: What is it and how to stop it. What teens want to know about cyberbullying. https://www.unicef.org/stories/how-to-stop-cyberbullying