BOOK CHAPTER | Cyberspace Security Exposition

An Exposition on Cybercrimes and Cybersecurity

[1]Konyeha S., [2]John-Otumu A.M, [3]Osa E. & [4]Oshioiribhor E.O.
[1]Department of Computer Science, University of Benin, Benin City, Nigeria
[2] Federal University of Technology, Owerri, Nigeria
[3] Dept of Electrical/Electronic Engineering, University of Benin, Benin City, Nigeria
[4]Department of Computer Science, Ambrose Alli University, Ekpoma. Nigeria
E-mail: [1]susan.konyeha@uniben.edu
Phone: +2348060826547

Abstract

The menace of cybercrime is increasing at an exponential rate owing to the ever increasing reliance of modern institutions on the internet. Today, people no longer have to move physically when attending to everyday life activities like shopping, business and communication. Even organizations now conduct meetings virtually and store all their data online undermining the risk of cybercrime. We are living in a digital world virtually everything has a footprint on the internet. Be it data storage or access, the assistance of the internet is highly sought. This continuous reliance on the internet which is the cyber world therefore makes us prone to cyber threats. This report is an exposition on the causes of cybercrime and the importance of cybersecurity to forestall cybercriminals.

Keywords: Cybercrime, cybercriminals, internet, cybersecurity

Introduction

Cybercrimes could be defined as crimes committed on the internet using the computer as an instrument to further illegal ends. It refers to the use of a computer to commit a crime. Criminal offenses committed via the Internet or otherwise aided by various forms of computer technology, such as committing fraud, human trafficking, child pornography, theft of intellectual property, stealing identities, violating privacy and so on. Cybercrime or computer-related crime is also a crime that involves the computer and the network (Igba et al, 2018) such as the use of online social networks to bully others or transmitting obscene sexual content through digital means.

Cybercrime began as a criminal activity when, cybercriminals known as hackers started accessing high-level computer networks illegally. Some examples of cybercrime activities are credit card theft, identity theft and network intrusions. Some of the most renowned organizations in the world have found themselves having to incur huge recovery costs after falling prey to cybercrime. Many institutions of higher learning have been compromised due to the huge databases of personal and research information they harbor.

Citation; Konyeha S., John-Otumu A.M, Osa E. & Oshioiribhor E.O. (2022): An Exposition on Cybercrimes and Cybersecurity. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series Book Chapter on Web of Deceit - African Multistakeholders' Perspective on Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical and Design Approaches. Pp 203 -206. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P34

Types of Cybercrimes

Some types of cybercrime are listed below.

- Cryptojacking
- Identity theft:
- Software piracy
- Cyberstalking
- Cyberterrorism

Types of Cyber Criminals

Cyber criminals, loosely known as hackers, employ computer systems to gain illegal access to business records and personal information for malicious use. They are extremely difficult to identify on both an individual and group level due to the various measures by which they hide their identities online such as obscuring their computer addresses, impersonating other personalities and so on. Various types of cybercriminals exist who carry out attacks for various reasons. Some are described below:

i. **Hackers:** The term hacker could refer to anyone with technical skills, however, it typically refers to an individual who uses his or her skills to achieve unauthorized access to systems or networks so as to commit crimes.
ii. **Organized Hackers:** These are hackers who carry out sophisticated attacks in an organized format. They may span large geographical boundaries and often have a wide range of resources.
iii. **Internet stalkers:** These are cybercriminals who monitor others online without their consent often for illicit purposes.
iv. **Disgruntled Employees:** These refers to employees who may not be satisfied with conditions in their place of work and react by malicious use of the network facilities of the organization.
v. **Hacktivists:** These are political actors who carry out their agitations or protests online by hacking systems and networks.

Causes of cybercrime in Nigeria

Cyber security and information technology security refer to a collection of measures for preventing unwanted access to computers, programs, networks, and data, as well as exploitative attacks. Cybersecurity is a system for defending against cyber-attacks. It is distinct from information security, which is a mechanism for safeguarding data against any type of threat, whether analog or digital. Cybersecurity mainly involves the cyber arm of law enforcement authorities and deals with cybercrime and cyberfraud.

Youth and Cybercrime

Nigeria has a generation of young individuals that are engrossed in the realm of cybercrime, presumably inspired by Hushpuppi (a recently arraigned Nigerian for cybercrime). Youths can be found in several Nigerian cities, including Lagos, Benin, and Owerri, as well as Accra, Johannesburg, Dubai, and Kuala Lumpur. These youthful opportunists attempt to initiate phishing and ransomware attacks, as well as malicious spams, all over the world from faraway locations. When they try to elude criminal punishment, they often stand out due to their distinctive clothing and brazen lifestyles. Some of these cyber offenders are high school grads or even undergraduate students who have not completed their schooling.

In Nigeria, these criminals refer to themselves as 'yahoo boys,' implying that they are unconcerned with their actions. Accra residents frequently refer to their work as 'pressing computer.' They also go to great lengths to enlist the help of spiritualists, ostensibly to telepathically command their victims to comply with their hot and deceptive demands.

The Federal Bureau of Investigation (FBI) has ranked Nigeria as the 16th most vulnerable country to cybercrime, and the rising number of fraudsters in the country is a relatively new problem (Igwe, 2021). The cause of this in Nigeria is sometimes attributed to a deterioration of society values, which is a result of the growing negative impact of politicians who become wealthy overnight by diverting public resources for personal gain. The belief is that because no special qualifications are required to engage in politics, one can become wealthy overnight if elected to public office. This get-rich-quick mentality has a significant negative impact on the younger generation, as they strive to succeed at all costs, including illegal activity. Other factors, such as poverty, unemployment, and economic disparities, do exist, though. Many people are drawn to cybercrime because the chances of being caught are slim, and many of these criminals have the physical and technological means to carry out their crimes.

Cybercrime motive and Operations

Ransomware attacks, IoT attacks, Cloud attacks, Phishing attacks, Blockchain and cryptocurrency attacks, Software vulnerabilities, Machine learning and AI attacks, BYOD policies, and so on are all examples of cyber attacks. Phishing scams, Internet fraud, online intellectual property infringements, identity theft, online harassment, and cyberstalking are the most common types of cybercrime reported by victims. Because most hackers solely care about their own financial gain, they frequently use ransomware or other phishing techniques to blackmail victims into making a fake financial transaction. Money is the most typical motivation for criminal hackers. They are frequently linked to established criminal gangs, making them part of a business with sophisticated tools and techniques.

Cyber criminals can use a wide range of intrusion methods and campaigns with such resources. They engage in large-scale phishing scams and ransomware attacks, among other things. Such tactics are frequently used to target as many victims as possible indiscriminately in order to maximize prospective earnings. Other techniques are more focused; many assaults involve finding affluent businesses and committing fraud, theft, or blackmail through spearphishing or direct network entry attempts. Attacks on private sector organizations are more common than attacks on public sector bodies and individuals because private sector organizations and individuals are typically more cash-rich.

Table 1 presents a compendium of some sources of cyber threats and cyber attacks that are carried out.

Table 1: Sources of cyber threat and major types of attack (Yuchong and Qinghui, 2021).

Sources of cyber threat	Major types of cyber Attack
Foreign countries	Logic bomb
Sabotage groups	Denial of service
Hackers	Spyware
Internal dissatisfied factors	Abuse tools
Organized hackers	Trojan horse
Terrorists	Sniffer and Virus

Cybersecurity

Cyber security and information technology security refer to a collection of measures for preventing unwanted access to computers, programs, networks, and data, as well as exploitative attacks. Cybersecurity is a system for defending against cyber-attacks. It is distinct from information security, which is a mechanism for safeguarding data against any type of threat, whether analog or digital. Cybersecurity mainly involves the cyber arm of law enforcement authorities and deals with cybercrime and cyberfraud. Nowadays cyber attacks are perpetuated using sophisticated technologies.in Konyeha, (2020) we Cybersecurity Threats in Digital Marketing was explored and in Akpon-Ebiyonare and S. Konyeha. (2019), a survey was carried out for Cyber Insecurity: End User Vulnerability Awareness and Perception Assessment.

Importance of Cybersecurity

The importance of cyber security bothers on human desire to keep digital information and their containers private and safe. Companies also need cyber security systems to keep their operations data, financial records and intellectual property safe. Konyeha, 2019 study recommends that cybersecurity policies should incorporate technical government measures and institutional measures to compliment government effort in securing and protecting ICT infrastructures.

Cybersecurity Tools

Every cybersecurity expert carries a different set of tools, depending on their mission and skill set be they penetration testers, digital forensics professionals, etc. Some cybersecurity tools are listed below:

1. Aircrack-ng
2. Burp Suite
3. Gophish
4. Have I Been Pwned
5. Kali Linux
6. Metasploit Framework
7. Nmap
8. Nikto
9. OpenVAS
10. OSSEC
11. Password managers
12. PfSense
13. P0f
14. REMnux
15. Security Onion
16. Snort
17. Wire shark

Recommendation

This exposition has introduced certain concepts in relation to cybercrime and cybersecurity. As can be seen, cybercrime is a dangerous canker worm eating deep into the fabric of modern day society. Owing to the huge negative effects of cybercrimes on institutions of various types, it is highly recommended that cybersecurity schemes and professions should therefore be encouraged at various levels of academia, industry and government so as to assist in making a safer cyberspace.

References

1. Hassan A. B., Lass F. D. and Makinde J. (2012): Cyber crime in Nigeria: Causes, Effects and the Way Out, ARPN Journal of Science and Technology, vol. 2(7), 626 – 631.
2. Igba D.I., Igba, E.C, Nwambam, A.S., Nnamani, S.C., Egbe, E.U. and Ogodo, J. V. (2018). Cybercrime among University Undergraduates: Implications on their Academic Achievement. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 2. pp. 1144-1154.
3. Igwe, U. (2021). Nigeria's growing cybercrime threat needs urgent government action. Available at: https://blogs.lse.ac.uk/africaatlse.
4. Konyeha S. (2019) Evaluating Hacking and Cyber-Security issues in Nigeria. Benin Journal of Advances in Computer Science. Vol. 4 No. 2 Pp 15-24. www.bjacs.org.ng.
5. Konyeha S. (2020) Exploring Cybersecurity Threats in Digital Marketing. NIPES Journal of Science and Technology Research 2(3) 2020 pp. 12-20
6. Akpon-Ebiyonare, D.E. and S. Konyeha. 2019. "Cyber Insecurity: End User Vulnerability Awareness and Perception Assessment". Pacific Journal of Science and Technology. 20(2):88-94.
7. Yuchong Li, Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021, Pages 8176-8186, ISSN:2352-4847,https://doi.org/10.1016/j.egyr.2021.08.126.