NIGERIAN JOURNAL OF EDUCATIONAL PHILOSPHY

EDUCATION, SECURITY, ECONOMY AND VIABILITY OF DIGITAL RESPONSE

VOLUME 33 NO. 2, OCTOBER, 2022

ISSN: 0794-0114
e-ISSN: 2971-5652

Published by:

PHILOSOPHERS OF EDUCATION ASSOCIATION OF NIGERIA (PEAN)
www.peanpapers.com

TIMSMEK GLOBAL PUBLISHERS®, PORT HARCOURT

An imprint of Timsmek Global Ltd
www.timsmek.com | info@timsmek.com | +234-703-455-9895

Education and Cyber Crime: Analysis and Prevention in the 21st Century

Alli Iyabode
Department of Educational Foundations
Philosophy of Education Unit
Nasarawa State University, Keffi
Iyabodealli1@gmail.com
+2348023355789

&

Timothy Isuwa
isuwa97@gmail.com
+2348065343897

Abstract
The paper took a cursory looks on education and cyber crime: analysis and prevention in the 21st century. It is captured in the paper that new technologies create new criminal opportunities as well as new types of crime. With the modernization and availability of technology at affordable prices it has led to wide spread use of technology for development as well as destruction. Cyber crime highlights the centrality of networked computers in our lives and the fragility of such seemingly solid facts as individual identity. The paper also identified the causes of cyber-crime to include unemployment and quest for Wealth among others. It recommends that, government at all levels should ensure that its laws apply at cybercrimes. It is important that Nigeria as a nation takes measures to ensure that its penal and procedural laws are adequate to meet the challenges posed by cybercrimes. In conclusion, the importance of protecting our education system from cyber crime cannot be overstated. Not only do schools, colleges and universities provide vital services to our society and economy, they are rich treasure troves of sensitive data.

Introduction

The Internet is a powerful tool that we use for different purposes including communication, work, education and entertainment amongst others. It is the place where access to online information is so fast that it makes it unprecedented. Information, news whether true or false can spread so quickly and easily that it makes it the perfect target for manipulation. In Nigeria, the three-pronged advent of the Internet, computers and the mobile phones gave rise to massive outbreak of cybercrimes. It is very glaring that criminals and fraudsters leverage the anonymity provided by the Internet to defraud unsuspecting victims. The fraudsters are fond of impersonating others and stealing their identities to perpetrate their acts, and do take undue advantage of a family member in distress to swindle their victims. The prevalence of a high rate of unemployment, harsh economic conditions and poor educational systems also contribute immensely to the proliferation of cybercrimes in Nigeria. The students are no longer facing the

realities of canvassing vocational jobs where they find it difficult to get a white collar job after graduation.

Omodunbi, Odiase, Olaniyan and Esan[1] held that education is seen as a process through which the experiences of generations, comprising knowledge, skills and attitudes are transmitted to individuals, who are members of the community. Concepts change, attitudes and skills undergo alterations, interests and values face revisions and life itself undergoes a continuous modification of experience. In this context, education is the process of assisting the learner to adjust to the ever-changing world.

New technologies create new criminal opportunities as well as new types of crime. With the modernization and availability of technology at affordable prices it has led to wide spread use of technology for development as well as destruction. Cyber crime highlights the centrality of networked computers in our lives and the fragility of such seemingly solid facts as individual identity. For example, Tanner[2] **maintained that** hacking involves attacking the computer's information and other resources. It is a thing of worry, therefore, that the above notwithstanding, the country is not implementing stringent legislation to dissuade the students from partaking in cybercrimes. Weak and fragile laws regarding cybercriminals exist in Nigeria. The most unfortunate is that the nation is not adequately equipped with sophisticated hardware to track down the forensic criminals. Our law enforcement agents are inadequately equipped in terms of personnel, intelligence and infrastructure to tackle the menace of cybercrimes that is adversely affecting the image and corporate identity of the country. How do we combat cybercrimes in Nigerian educational system? It is obvious that cybercrimes cannot be easily eliminated, but they can be minimised.

Types of Cyber Crimes

Cyber crimes simply put are crimes that are committed using the Computers and Networks. There are several types of cyber crimes some of which include:

a. **Cyber Terrorism:** A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. According to Wikipedia[3], a cyber terrorist is someone who intimidates a government or to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them. For instance, a rumor on the Internet about terror acts. In addition, Parker[4] defined Cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. It means that any act intended to instill fear by accessing and distorting any useful information in organizations or Government bodies using Computer and Internet is generally referred to as Cyber Terrorism. Another form of cyber terrorism is cyber extortion which is a form of cyber terrorism in which a website, e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service.

b. **Fraud - Identity Theft:** Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone. For instance, making a false bank webpage to retrieve the account information of someone. The concept is simple; someone gains access to your personal information and uses it for his own benefit. This could range from a black-hat hacker stealing online banking account login and password to getting access to ATM and using such people can make themselves a lot of money with personal information. In Nigeria people design web links forms requesting users to fill in their basic information including, unique details like pin numbers and use that to commit crimes.

c. **Drug Trafficking Deals:** Laura Ani say[5] that another type of Cyber Crime is Drug Trafficking; it is a global trade involving cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition law. Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to make comfortably purchase of illegal drugs. (www.wikipedia.com).

d. **Malware:** to Peters Ifeoma Malware[6] refers to viruses, Trojans, worms and other software that get onto your computer without you being aware it's there. Back in the early part of the century, most such software's primary aim was thrill. The people writing the software found it amusing to write a program that exploited security flaws just to see how far it could spread. Today the incentive for making such software is generally more dangerous. In some cases a piece of malware will pretend to be a legitimate piece of software. When such software is downloaded, it infects the computer system and destroys valuable information. The Trojan horse is also a technique for creating an automated form of computer abuse called the salami attack, which works on financial data. This technique causes small amounts of assets to be removed from a larger pool. The stolen assets are removed one slice at a time.

e. **Spam:** Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. Some of these address harvesting approaches rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site as seen in Saul[6].

   Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are

numerous, and the volume of unsolicited mail has become very high. A person who creates electronic spam is called a spammer.

Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cyber-crime according to Hassan[7]

a) Unemployment is one of the major causes of Cybercrime in Nigeria. It is a known fact that over 20 million graduates in the country do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival.
b) Quest for Wealth is another cause of cybercrime in Nigeria. Youths of nowadays are very greedy, they are not ready to start small hence they strive to level up with their rich counterparts by engaging in cybercrimes.
c) Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught. 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.
d) 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.

Various Cybercrimes in Nigeria

Over the past decade, the internet has experienced an explosive growth with the number of hosts connected to the internet increasing daily at an exponential rate. As the internet grows to become more accessible and more services become reliant on it for their daily operation, so does the threat land scape. In Nigeria, cybercrime has become one of the main avenues for pilfering money and business espionage. According to Check Point[8], a global network cyber security vendor, as of 2016, Nigeria is ranked 16th highest country in cyber-attacks vulnerabilities in Africa. Nigerians are known both home at and abroad to be rampant perpetuators of cybercrimes. The number of Nigerians caught for duplicitous activities carried by broadcasting stations are much more in comparison to other citizens of different countries. The contribution of the internet to the development of Nigeria has had a positive impact on various sectors of the country. However, these sectors such as the banking, e-commerce and educational sector battles with the effect of cybercrimes. More cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its predecessor. Therefore, in this section, prominent specific ways in which cybercrimes are mostly carried out in Nigeria are discussed.

Cybercrimes in the Education Sector

Mbaskei Martin Obono[9] stated that the educational sector in Nigeria suffers greatly from electronic crimes which are perpetuated mostly by students in tertiary institutions. Cyber-Plagiarism: Information housed on the internet has made an effective alteration on the methods in which people educate themselves. The term ‘Copy and Paste’ is the most common phrase used when referring to cyber-plagiarism. Cyber-plagiarism can be defined as copying and pasting online sources into word processing documents without reference to the original writer

/owner. In the educational sector in Nigeria, students, particularly those in the tertiary institutions carry out this crime without enforcing the due penalty.

Cyber Laws in Nigeria
what is a Cybercrime?
Cybercrime is a type of crime that takes place in cyberspace, or in the realm of computers and the Internet. Because our society is evolving towards an information society where communication occurs in cyberspace, cybercrime is now a global phenomenon. Cybercrime has the potential to significantly influence our lives, society, and economy.\

What is Cyber Law?

Halder & Jaishanka[10] opined that any law that deals with the internet and similar technology is known as cyber law. Cyber Law is frequently referred to as "Law of the Internet" or "IT Law." It's a legal framework for dealing with issues relating to the Internet, computing, Cyberspace, and other associated matters. One of the newest aspects of the legal system is cyber law. This is due to the rapid advancement of internet technology. People who use the internet have legal safeguards under cyber law. This applies to both business and common citizens. Anyone who uses the internet should be familiar with cyber laws.

Intellectual property, contract, jurisdiction, data protection laws, privacy, and freedom of expression are all covered by cyber law. It oversees the distribution of software, information, online security, and e-commerce via the internet. E-documents are given legal validity in the field of Cyber Law. It also establishes a framework for e-commerce and e-filling. To put it another way, Cyber law is a legal framework for dealing with cybercrime. Due to the increased use of E-commerce, it is critical that suitable regulatory practices are in place to ensure that no malpractices occur.

Cyber security laws vary a lot from country to country and jurisdiction to jurisdiction. Penalties depend on the nature of offence, and will range from a fine to imprisonment. It is critical for citizens to understand their particular countries' cyber laws in order to ensure that they are fully informed about all cyber security issues.

Cybercrimes (Prohibition and Prevention) Act, 2015

According to Saul Hansell[11], the Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.

Cybercrimes highlighted under this ACT include:

- Offences against critical national information infrastructure
- Hacking Computer Systems and Data Alteration
- Unauthorized Access of Protected Systems
- Illegal Registration of Cybercafé or Usage of Unregistered Cybercafé
- System Interference

- Interception of electronic messages, email, electronic money transfers
- Tampering with critical infrastructure
- Willful misdirection of electronic messages
- Unlawful interceptions
- Computer related forgery
- Computer related fraud
- Theft of Electronic Devices
- Unauthorised modification of computer systems, network data & system interference
- Publishing False Digital Signature and Certificates
- Cyber terrorism
- Exceptions to financial institutions posting and authorised options
- Fraudulent issuance of e-instructions
- Tampering with Computer Source Documents
- Identity theft and impersonation
- Child pornography and related offences
- Cyberstalking
- Cybersquatting
- Racist and xenophobic offences
- Attempt, conspiracy, aiding and abetting
- Importation and fabrication of e-tools
- Breach of Confidentiality and Privacy
- Manipulation of ATM/POS Terminals
- Phishing, spamming, spreading of computer virus
- Electronic cards related fraud
- Use of fraudulent device or attached e-mails and websites

Administration and Enforcement Cyber Law in Nigeria

Under the 2015 Cybercrime Act as cited in Ekeji Chidozie Christopher[12], the National Security Adviser's office serves as the coordinating body for the security and enforcement authorities. The Attorney-General of the Federation reinforces and improves Nigeria's existing legal frameworks regarding cybercrime. All law enforcement, security, and intelligence agencies develop the institutional capacity necessary for the effective implementation of the provisions of the 2015 Cybercrime Act, and in collaboration with the Office of the National Security Adviser, initiate, develop, or organize training programs for officers charged with cybercrime on a national or international level.

Establishment of the Cybercrime Advisory Council

To Coordinate Cybercrime Act[13] 2015, there was established a Cybercrime Advisory Council (in this Act referred to as "the Council") as cited www.efccnigeria.org/efcc_homepage.../establishment_act_2004.pdf(2004) in charge of handling issues relating to the prevention and combating of cybercrimes, cyber threat, computer-related cases and the promotion of cyber security in Nigeria. Furthermore, Meke Eze Stanley[14], observed that the Cybercrime Advisory Council comprises of a representative each of the following Ministries, Departments and Agencies are:

(a) Federal Ministry of Justice;
(b) Federal Ministry of Finance;
(c) Ministry of Foreign Affairs;
(d) Federal Ministry of Trade and Investment;
(e) Central Bank of Nigeria;
(f) Office of the National Security Adviser;
(g) Department of State Services;
(h) Nigeria Police Force;
(i) Economic and Financial Crimes Commission;
(j) Independent Corrupt Practices Commission;
(k) National Intelligence Agency;
(l) Nigeria Security and Civil Defence Corps;
(m) Defence intelligence Agency;
(n) Defence Headquarters;
(o) National Agency for the Prohibition of Traffic in Persons;
(p) Nigeria Customs Service;
(q) Nigeria Immigration Service;
(r) National Space Management Agency;
(s) Nigerian Information Technology Development Agency;
(t) Nigerian Communications Commission;
(u) Galaxy backbone;
(v) National Identity Management Commission;
(w) Nigeria Prisons Service;
(x) One representative each from the following:
(i) Association of Telecommunications Companies of Nigeria;
(ii) Internet Service Providers Association of Nigeria;
(iii) Nigeria Bankers Committee;
(iv) Nigeria Insurance Association;
(v) Nigerian Stock Exchange;
(vi) Non-Governmental Organization with Focus on Cyber Security.

What is the Importance of Cyber Laws in Nigeria?

Cyber law is important for organizations that are exposed to risk as a result of an inefficient cyber security system. These laws apply to all forms of corporate organizations and digital systems that do business on a daily basis. Each organization adheres to unique cyber security guidelines, cyber security legislation, cyber security policies, and legal issues regulations.

The following points demonstrate the significant importance of cyber law in Nigeria as quote in Thisday Newspaper[15]:

- It establishes the parameters for all acts and reactions in Cyberspace.
- All online transactions are guaranteed to be safe and protected.
- Cyber law enforcement officials monitor all internet activity.
- Protection for all data and property of individuals, organizations, and Government
- Contributes to the elimination of unlawful cyber activity through due diligence

- All activities and reactions carried out in any cyberspace have a legal component.
- Maintains a database of all electronic records
- Contributes to the establishment of electronic governance

Challenges

Turf battles (supremacy disagreements) among law enforcement, intelligence and security agencies;

- Lack of understanding of the dire consequences of not criminalising conduct that amounts to cybercrime or the serious dangers, economic loss and national security vulnerability that flows from the lack of adequate cyber security framework, on the part of our lawmakers;
- The absence of a knowledgeable and committed champion at the highest policy levels to sustain the drive for the passage of the Bill, while emphasising the peril of not doing so.
- Lack of integration of public – private sector stakeholders in the process, due largely to distrust of government by the private sector, as well as sectored infighting;
- Insufficient sustained lobbying of the lawmakers by the sponsors of the various previous pending Bills.

How Does Cybercrime Affect Education?

Ewepu[16] maintained that the education sector is seriously under threat in 2018 and the first half of 2019. Threats ranged from nuisance adware to serious malware like trojans, backdoors and, of course, ransomware a malicious file that encrypts system files and information on endpoints and servers of schools are hit by ransomware attacks. Apart from the direct financial damage caused by the inability to access computer systems paralyses the academic institution. The cost of the damage only accelerates the longer the school is unable to send emails, record working hours or allocate classrooms and study resources, including school computers and Internet access necessary for many learning activities. The now-infamous Emotet malware has also been striking schools, with attackers using spearphishing to infect systems with the malware trojan. As many services are now entirely computerized, this can even affect infrastructure like heating and cooling, cafeteria services and security systems. Cyber Incidents map provides a graphic overview of just how widespread the problem is.

It's not only schools that are being targeted either. Higher education institutions are also vulnerable to cyber attacks. A number of universities and colleges have suffered from ransom ware attacks, information leaks, and email hacking in the past year. Unlike schools, universities and academic institutes are also being targeted by more sophisticated attackers interested in stealing the intellectual property (IP) and research data produced there.

Rebecca & Jeanne stated that[17] the situation in other parts of the world is as bad. In Australia the head of the local intelligence agency was recruited to inform universities about cyber threats and ways of prevention. This was one of the initiatives put in place after an extremely sophisticated threat actor compromised ANU and persisted within the university's network for months at a time. They further observed that n the UK in April (2021) penetration testing

conducted by JISC, the government agency that provides many computerized services to UK academic bodies, tested the defenses of over 50 British universities. The results were unflattering: the pen testers scored 100% success rate, gaining access to every single system they tested. Defense systems were bypassed in as little as an hour in some cases; with the ethical hackers easily able to gain access to information such as research data, financial systems as well as staff and student personal information.

Why Are Schools, Colleges Targeted by Cyber Criminals?

It is no coincidence that schools are among the most attacked. Schools manage substantial sums of money, store personal information for students and teachers and connect with a large number of external bodies and providers and, of course, parents, who primarily communicate with the school via email. This means that the school has a very large attack surface.

Coupled with enticing rewards is the fact that students make for easy victims of phishing scams. Students' lack of experience combined with a tendency to use simple passwords across multiple services makes them prone to credential harvesting and password-spraying attacks. In addition, the awareness of parents, teachers and faculty regarding cyber risks is often much lower in education than in other sectors. Further exacerbating the security situation is that educational establishments typically have a limited number of staff dedicated to security. Unlike banks, schools typically do not have dedicated information security personnel who are engaged in 24/7 protection.

The way forward

1. It calls for the collaborative efforts of all the stakeholders like individual corporate organisations and government to nip the scourge in the bud.
2. Government at all levels should also ensure that its laws apply at cybercrimes. It is important that Nigeria as a nation takes measures to ensure that its penal and procedural laws are adequate to meet the challenges posed by cybercrimes.
3. Government should ensure that policies are formulated and strictly adhered to irrespective of the status and personality of the people involved.
4. It is believe that creation of job opportunities for the teeming unemployed youth will minimise the menace drastically.
5. In the case of ransomware, the source of the attack is most likely to be contained in an infected file sent via email. In such cases, the End Point Dictation and Response (EDR) protection system must identify the file as soon as it tries to install itself on the endpoint, disable it and delete it from this and all other endpoints across the organization. This will prevent the attack at the infection phase and prevent the loss of services in the educational institution.
6. Similarly, a solution that can rollback a device to a healthful state, including decrypting encrypted files, should be high on the institution's security shopping list.

Conclusion

The importance of protecting our education system from cyber crime cannot be overstated. Not only do schools, colleges and universities provide vital services to our society and economy, they are rich treasure troves of sensitive data. From personal information like birth records, educational history, social security numbers and financial data to intellectual property and

cutting-edge research, the data held by these organizations is among the most useful to cyber criminals and advanced threat actors. And yet, these storehouses of precious data are perhaps among the least well-defended and under-funded in terms of cyber security.

References

B. A. Omodunbi, P. O. Odiase, O. M Olaniyan and A. O. Esan. Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology, Volume 1, Issue 1, September 2016 ISSN: 2579-0625 (Online)

Tanner, R.E.S. Social Impact of Cyber Crimes. New Delhi. Concept Publishing Company. 2007

Thisday Newspaper (2012): Growing menace of Cyber crime, 20th September, 2012. Http:// www.wikipedia.com

Laura Ani (2011): "Cyber Crime and National Security: The Role of the Penal and Procedural Law.

Peters Ifeoma. Cybercrimes and Cyber Laws in Nigeria: All You Need To know. July 6. 2021

Saul Hansell,(2007): Social network launches worldwide spam campaign, New York Times.

Hassan. Saul. Social network launches worldwide spam campaign New York Times (2007)

Advanced free fraud available at http://www.nigeria law.org/Advance%20Fee%20Fraud%20and%20other%20Fraud%20Related%20Offe nces%20Act%202006.htm (2006).

Mbaskei Martin Obono (2008): Cyber crimes: Effect on Youth Development http://www.igenius.org accessed 27 February, 2013

Halder, D., & Jaishankar, K. (2011): Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA:IGI Global. ISBN 978-1-60960-830-9.

Padhy, P. Crime and Criminology, Principles of Criminology. New Delhi: Mehra Press Ltd. 2006

Ekeji Chidozie Christopher. Cyber Crime in Nigeria. 2020

Cybercrime in Nigeria: Causes and Effects. https://www.proshareng.com/news/Security---Support/Cybercrime-in-Nigeria--Causes-and-Effect/49035

Meke Eze Stanley, N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".

Thisday Newspaper (2012): Growing menace of Cyber crime, 20th September, 2012. Http:// www.wikipedia.com

Ewepu G, (2016) Nigeria loses N127bn annually to cyber-crime — NSA available at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/Retrieved Jun. 9, 2021

Rebecca & Jeanne, M. Criminology. Encyclopedia of the Social and Cultural Foundation of Education. New Delhi: SAGE Publications. 2011