Assessment of the Factors Influencing Cybercrime in Academic Libraries of Tertiary Institutions in Yobe State, Nigeria

By

[1]Kabiru Akande Babatude, [2]Augustine Alhaji Adejo & [3]Ajayi Joushua Eyiolorunshe

[1]University Library, Federal University, Gashua, Yobe State. Kabiruakande@gmail.com
[2]Nigeria French Language Village, Ajara, Badagry, Lagos State,Adejoaugustine123@gmail.com
[3]University Library, Federal University, Dutsin-ma, Katsina State, ajayijoshua788@yahoo.com

Abstract
This study explored cybercrimes in Academic Libraries of Tertiary Institutions in Yobe State. Two (2) objectives set to guide this study were; to identify the types of cybercrimes perpetrated in academic libraries in Yobe State and reveal factors that influence cybercrime in academic libraries in Yobe State. Qualitative research methodology and multiple case study research design were employed. Data was collected using in-depth Semi-interview and document analysis. A sample of 6 participants was used for the study. Moreover, all the narratives from the 6 participants" were used for analysis. The data was analyzed using grounded theory Analysis. The findings revealed that the types of cybercrime perpetrated in Academic Libraries of Tertiary Institutions in Yobe State are cyber phishing, cyber bullying, impersonation, viewing of classified and pornographic materials. The factors that influences cybercrime includes poverty, technical know-how, lack of system security, lack of disciplinary action, lack or poor cyber policy, inappropriate monitoring and user's negligence. Finally, the study recommended The Management of Federal University, Gashua, Federal Polytechnic, Damaturu and Federal College of Education (Technical), Potiskum to establish a quick response website where victims can report cybercrime cases along with digital forensic laboratory that would report cybercrimes related issues to the Management. And The Government and the Management of Federal University, Gashua, Federal Polytechnic, Damaturu and Federal College of Education (Technical), Potiskum should provide student Work-Study Programs to alleviate the financial pressures that drive students toward cyber fraud as a means of survival.

Keyword: Cybercrime, Academic Libraries, Tertiary Institutions, Yobe State, Nigeria

Introduction

The advent and growth of the Internet has not only altered how people interact but has also added a new dimension to criminal activities in the society. Cyber fraud poses a great challenge to the cash-less society. Therefore, the prevalence of fraud on internet contributes to the growing of technophobia as users are apprehensive for the safety of their funds on electronic payment platforms (Lemo, 2013). Moreover, developed countries such like America, Britain, Russia and Western Countries have recoded high rate of crimes perpetrated through the Internet. According to Saulawa and Abubakar (2014), reported that in 2012, an estimated $1 trillion was lost to cyber-related frauds globally. Thus, only $390 billion was reported for obvious reasons. Broadhurst & Chang, (2013) cited AFP, (2010) in their article that the United States Internet Crime Centre received 336,655 complaints reporting a total in direct losses of USD$559.7 million. They stated

that this is an estimate based on complaints to just one Internet crime reporting service in one country.

Saulawa and Abubakar (2014), reveals that a recently report by the South African based Institute of Digital Communication indicated that Nigeria is losing about $80 million dollars yearly to software piracy alone. Similarly, Sesan, Soremi & Oluwafemi (2012) reports that in 2012 alone, an estimated customer loss of ₦2,146,666,345,014.75 ($13,547,910,034.80) was incurred to cybercrime in Nigeria. Indeed, with each passing day, people witness more and more alarming cases of cyber-crimes in Nigeria, each new case more shocking than the one before. It has become a stubborn mouth sore which caused a lot of pain and shame because criminal minded individuals in the country are stealing and committing atrocity through the aid of the internet (Okeshola & Adeta, 2013).

It has however, been observed that a sizeable number of criminals in Nigeria fall within the youthful age. The youths at present have discovered different ways of using the Internet in doing different types of criminal activities and these age bracket are usually found in tertiary institutions in Nigeria (Olaide & Adewole, 2004). A study by Zero Tolerance (2006) indicated that cyber criminals are usually within the ages of 18 and 30 years and they indulge in the crime in order to survive and have a taste of good life. Moreover, these have led to the erosion of confidence in genuine Nigerian commercial credibility, and today many western countries with France taking the lead, have moved to deny Nigerian businessmen and women who are legitimate the rewards of e-commerce. France today requires web camera verification for most online business transactions from Nigeria. This has left the Nigerian Government with no choice than to enforce the security and regulatory agencies such as EFCC, NITDA, NCC etc. to arrest cyber-crime culprits. An attempt to address cyber-crime by various governments and international organizations has not been successful, owing to the fact that the identities remain inadequate.

Statement of the Problem

Even as cybercrime remains a global threat, most studies on cybercrimes focused on online transaction platforms, business, banking, industries and e-commerce institutions etc. And also largely concentrate on situations in the western world, forgetting the nature of cybercrimes in African and educational institutions (Okeshola & Adeta, 2013).

With the present Industrial Revolution four (IR4) in tertiary institution, academic libraries have incorporated the use of ICTs and Internet connectivity to ensure it users has access to wide range information in which these has led the libraries more vulnerable to cybercrimes. However, some library clients are using this privilege to perpetrate crime and criminality acts the in libraries. Therefore, there is need to know what attributes cyber criminals possess and identify others motivating factors since it has been acknowledged that a good taste of life is a major factor (Zero Tolerance, 2006).

In addition, Okeshola & Adeta (2013), studies revealed that most studies focus on cyber-crime largely concentrate on situations in the western world, forgotten the nature of crimes perpetrated in developing nations specifically within higher educational institutions. Similarly, little research that has been conducted on how student perceive cybercrime issues, thereby deficiencies the issue to perceptions and speculations (Barfi, Nyagome & Yeboah, 2018). As a result of this, there is need for more empirical studies to concentrate on the nature of cybercrime in academic libraries.

Therefore, this study in-depth reveals cyber-crimes perpetrated in tertiary institutions library in Yobe State.

Objectives of the Study

The objectives of the study are:

1. To identify the types of cybercrimes perpetrated in academic libraries in Yobe State
2. To determine the factors that influence cybercrime in academic libraries in Yobe State

Literature Review

Cybercrime has severe impacts on the society, ranging from its ability to aid corruption, money laundering, military espionage, terrorism and above all, undermining technological and socio-economic development of any country (Weber, 2006). However, cybercrimes are crimes committed through the use of World Wide Web (www) to steal someone's identity, watching and downloading of pornographic pictures and films, spread of malicious software (virus), botnet (send spam email massages), accessing unwanted sites and hacking into other computer networks or websites (Babatunde, Muhammed and Aduku, 2019).

There are various kinds of cybercrimes perpetrated across the global. Thus, the types of cybercrimes committed in each country or places vary from one another. Ribadu (2007) stated that the prominent forms of cybercrimes in Nigeria are cloning of websites, false representations, internet purchase and other electronic commerce kinds of fraud. Similarly, Olugbodi (2010) has shown that the most prevalent types of cybercrime are website cloning, financial fraud, identity theft, credit card theft, cyber theft, fraudulent electronic mails, cyber laundering and virus or worm/Trojans. According to Abdulhamid, Haruna&Abubakar (2011) hacking, denial of service attack, virus dissemination, software piracy, pornography, Internet Relay Chat (IRC) crime, credit card fraud, cyber extortion, phishing, spoofing, cyber stalking, cyber defamation, threatening, salami attack, cyber plagiarism and yahoo boy attack are among cybercrimes committed in Nigeria. Warner (2011) identified three main forms of cybercrimes prevailing in Ghana namely identity fraud, fake gold dealers and estate fraud. Also, Barfi, Nyagome &Yeboah (2018), study indicated that the four major forms of cybercrimes are hacking, credit card fraud, software piracy and cyber identity theft as forms of cybercrime in senior high school.

Moreover, numerous studies have shown that cybercrimes are carried out by Nigeria youth and there is inner motion that led most youth to perpetrate cybercrimes. Chris & Itodo's (2016) study revealed that Tunji Ogunleye, an ICT security consultant and a member of the Nigerian Cyber Crime Working Group (NCWG) disclosed that the rate of e-crime in Nigeria has outgrown the rate of Internet usage in the country. They further listed the below items as factors that influence cybercrime:

- ✓ **Domestic and international law enforcement:** A hostile party using an Internet connected computer thousands of miles away can attack internet- connected computers in Nigeria as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.

- ✓ **Unemployment:** The spate of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt. The federal government has proposed a mass sack of government workers. Companies are also embarking on mass sacks of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embarked on mass lay-offs of staff based on adhoc decisions.
- ✓ **Poverty Rate:** On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries.
- ✓ **Corruption:** Nigeria was ranked third among the most corrupt countries in the world. Until 1999, corruption was seen as a way of life in Nigeria.
- ✓ **Lack of Standards and National Central Control:** Charles Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulations, standards and computer security and protection act are hampering true e-business. Foreign Direct Investment (FDI) and foreign outsourcing are encouraging computer misuse and abuse.
- ✓ **Lack of Infrastructure:** Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.
- ✓ **Lack of National Functional Databases:** National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.
- ✓ **Proliferation of Cybercafés:** As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.
- ✓ **Porous Nature of the Internet:** The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

Methodology

This study adopted the qualitative research method and multiple case study design. Twenty (20) Staff of e-library/ICT staff and network administrators who frequently monitor clients who access online information from the three (3) tertiary Institutions(Federal Polytechnic Damaturu, Federal College of Education (Technical), Potiskum and Federal University, Gashua) with ICT/e-libraries and internet connectivity were considered as study participants. Six (6) participants used as sample for this study was selected through purposive sampling technique. Semi-structured interview were used for data collection. Tape recorders were used to record the interview which lasted for 30-45 minutes. The interview was analyzed using content analysis and also documented file on cybercrimes related issues was analyzed and thoroughly examined in the Security Department at each institution. This document analysis allowed the researcher to gain better understanding and develop empirical knowledge.

Data Presentation and Result

This section consists of data presentation and analysis in alignment with the objectives of the study;

Types of cybercrimes committed in Academic Libraries in Yobe State

This objective sought to identify the types of cybercrimes committed in academic libraries inYobe State. Two categories emerged from the narratives of the participants of this study, namely; (1) Cybercrime experience (2) Cybercrime in academic libraries. The categories and their individual subcategories are shown in Table 1 below.

Table 1: Types of cybercrimes committed in Academic Libraries

RQ	Categories	Subcategories
1. Types of cybercrimes committed in academic libraries in Yobe State	1. Cybercrime experience	1.1 Using someone else's account 1.2 Gathering information to harm victims 1.3 Illegal access to computer online 1.4 Cyber bullying 1.5 Cyber(social) engineering phishing
	2. Cybercrime perpetrated on online platforms	2.1 Identity theft 2.2 Viewing & downloading of pornographic movies

Sources: Interview Analysis, 2025.

The emergent categories are discussed as follows starting with Cybercrimes experiencedby E-library staff/ICT Units and network administrators.

Categories 1: Cybercrime experienced

Cybercrime experienced describes the narratives related to the types of cybercrimes ever experienced. It consists of five sub categories: using someone else's account, gathering of information to harm victims, illegal access to computer system online, cyber bullying and engineering phishing. These subcategories are explained below

Using someone else's account: This subcategory contains narratives related information derive on the types of cybercrimes ever experienced. "Participant 5 commented that,

"Cybercriminal log into someone else's account and using it to performs several activities without the consent of the account owner".

Gathering of information to harm victims: This sub-category also emerged from the narratives related on types of cybercrimes ever experienced Participant 6 commented that,

"Hackers source for information online with the aim of harming their victims". In the same vein participant 2 said, *"they take the advantages of the newly people coming online every year for the first time who stored their personal sensitive information online. This increases the potential of cybercriminal to always gather information on their victims".*

Illegal access to computer system online: This sub-category emerged as one of the types of cybercrimes ever experienced. The participants 4 stated that

"Some internet users discovered that their computer system was remotely controlled by unidentified user". Participant 1 said that, *"someone will just discover that his/her computer system has been remotely controlled by someone else".*

Cyber bully: This sub category was derived from the following narrative by Participant 4 on the types of cybercrime ever experienced;

"Part of the types of cybercrime I ever experienced is cyber bully, most ladies were been threatened that their private picture will be displayed on air if money was not given to them".

Engineering phishing: This sub category is observed from the following narrative by Participant 1 on the types of cybercrime ever experienced.

"The cybercrime I ever experienced is that of social engineering phishing, they target my email".

Categories 2: Cybercrimes Perpetrated in Academic Libraries

Cybercrime perpetrated on online platforms gives descriptive narration related to cybercrime perpetrated on the online platforms in academic libraries of Yobe State. It encompasses of two sub categories namely; identity theft and viewing and downloading of pornographic movies.

Identity theft: This subcategory depicts narratives on information related to the cybercrime perpetrated in academic libraries of Yobe State. Participant 5 said that,

"The cybercriminal login into someone social platforms such as whatsapp, facebooketcand began to chat with his or her friends to solicit for money". Participant 2 revealed that *"when a hacker successfully login into someone else's account he uses his/her identity to perpetrate crimes such as fabricating of lies to earn money and performing illegal activities".* Participant 7 summed up that *"cybercriminal hack into someone's account to use his/her identity to commit crimes in order to leave no sign of tracing the cyber culprits".*

Downloading of pornographic movies: This sub-category also emerged from the narratives of a participant of this study. Participant 3 stated that, *"The fraudsters use the institutions network to download movies especially pornographic movies."* However, the case file from the schools security offices showed that the cybercrime perpetrated include; *cyber phishing, cyber bullying, using of fellow students account without the consent of the account users, and viewing of classified and pornographic materials.*

Factors that Influence Perpetration of Cybercrime on Online Platforms

This objective sought to reveal the factors that influence the perpetration of cybercrimes in academic libraries in Yobe State. Four categories emerged from the narratives of the participants of this study namely; (1) Factors that influence cybercrimes (2) Time as a factor that influence cybercrime (3) Vulnerable website influence cybercrime (4) Effect of the factors that influence cybercrimes.

Table 2: Factors that influence the perpetration of cybercrime on online platforms

RQ	Categories	Subcategories
1. Factors influence cybercrimes in academic libraries in Yobe State	1. Factors that influence cyber security	1.1 Poverty 1.2 Technical-know-how 1.3 Lack or weak system security 1.4 Lack of disciplinary action 1.5 Poor cyber policy 1.6 Inappropriate monitoring 1.7 Users negligence
	2. Time as factor that influence cybercrime	2.1 Staying too long online 2.2 Mid night
	3. Vulnerable website influences cybercrime	3.1 Website contain information that teaches how to perpetrate crime
	4. Effect of the factors that influence cybercrime	4.1 Enhance continuation of cybercrime

Sources: Interview Analysis, 2025

Categories 1: Factors that influence cybercrime perpetration in Academic Libraries

Factors that influence cybercrimes perpetration in academic libraries in Yobe state category provide narratives information related to the factors that influences cybercrime perpetration in academic libraries in Yobe State. It consists of seven sub categories: poverty, technical know-how, lack or weak of system security, Lack disciplinary action, Poor cyber policy, inappropriate monitoring and Users negligence. The individual subcategories are explained below:

Poverty: This subcategory emerged from narratives related to the factors that influences cybercrime perpetration in academic libraries in Yobe State. Participant 1 stated that, *"What I want you to understand regarding to the factors that influence cybercrime. For example, if someone has been strike with poverty for a long period of time and all various ways he/she tried to survive end up in vain. However, this may lead him to perpetrate different kinds of crime".* Participant 3 said that, *"Poverty was the genesis that leads most youths to become "yahoo guys" that usually perpetrate online crimes".*

Technical-know-how: This sub-category emerged from the narratives of participants of this study. Participant 1 said, *"Is technical-know-how of cause, those cybercriminal are very knowledgeable on IT gadgets".* In a similar way, Participant 4 stated that, *"But you should know that if you are not computer literate and knowledgeable on IT related facilities you cannot perpetrate crime on the Libraries network".*

Lack or weak system security: This sub category is explained by participant 2, *"Lack of proper security or weak password make IT system vulnerable to crime, if someone comes across a system with vital information or items that are useful and the system security can easily be broken. It serves as an opportunity to commit crime".*

Lack of disciplinary action**:** -This sub category is observed from the following narratives by participant 6 that, *"To me, what I feel that influences cybercrime practices are lack of disciplinary action".* Participant 6 stated that, *"sometime crime related issues were overlooked among few people that witness the crime. It usually not forwarded to the management for disciplinary actions to be carried out".* Participant 3 revealed that, "*Even when some cases are forwarded, some of the management members or disciplinary committee members will ensure that the case is dismiss or not treated due to their familiarity with the culprits".*

Poor cyber policy: This sub category is derived from narratives related from staff experience on those factors that influence cybercrime by internet users in Yobe State. Participant 5 revealed that, *"In my own experience, poor cyber policy influences cybercrimes due to the available rules and regulations that guide clients on the uses of the institutional network does not restrict internet users on most activities they will perform online. It only prevents the available ICT system from being damaged".*

Inappropriate monitoring**:** -This sub category is observed from the following narratives by participant 2 that, *"it was due to inappropriate monitoring of internet users in the library. However, most time users use this privilege to perpetrated cyber bullying such as copy, uploading and posting of fellow female colleague private pictures on online social platforms".* Participant 4 stated that, *"I usually experience that most time when there is no staff monitoring the internet users then begin to copy and uploading of some female student's nakedness on social platforms".*

User's negligence: This sub category is derived from narratives related to the challenges that mitigate cybercrime prevention on online platforms. Participant 4 revealed that, *"I usually experience in most cases when students bring report regarding someone else making use of their ID and password, when we investigate the issues we end up discovering that it was as a result of user's negligence that authorized website to save their ID and password on the website of the online platform".* Although, the case file from the security offices indicated that the inner factors that influence some of the students to commit cybercrime: *are poor family background, lack of cyber policy, careless of fellow students to protect their system, staff negligent ID and password.*

Categories 2: Time as factor that influence cybercrimes

Time as a factor that influence cybercrimes category includes narratives related to the view of e-library staff and network administrators that time could be a factor that influences cybercrime on the online platforms. It consists of two sub categories: Staying too long online and mid night/Break period. The individual subcategories are explained below:

Staying too long online**:** -This sub category is observed from the following narratives by participant 2 that, *"Time is also a factor that influence cybercrime, because once student are online for longtime they will start thinking of how to make money".*

Mid night/Break period: This sub category was derived from narratives related on time as a factor that influence cybercrime on the online platforms. Participant 5 stated that, *"Time is a factor that leads to crime because most criminals operate with time. However, mid night and break period*

were the actual time that is more favorable to criminals because there will be less guard or security. This is also applicable to school network, moreover, the network custodian falls asleep at night and also left the network on when closing for the day".

Categories 3: Vulnerable website as a factor that influence cybercrime

Vulnerable website as a factor that influence cybercrimes category include narratives related to the view of e-library staff and network administrators on how vulnerable website influences cybercrime. It consists of sub category: website contains information that teaches cybercrime. The individual subcategory is explained below:

Vulnerable website influences cybercrime: This sub-category emerged as a result from participants' narratives related information that does vulnerable website influences cybercrime. Participant 1 stated that, *"Some websites also contribute to cybercrime, because they provide list of previous users account detail (ID and password) which enable other users that visited the website to use their identity or login into their account to commit crime".* Participant 3 reported that, *"My view about vulnerable website in influencing cybercrime is that it exposes sensitive information of users account on the website. However, through vulnerable website hackers see information that enables them to login into someone else's account to perpetrate crimes and criminalities act because vulnerable website provide an option that make cyber users on the website to save users ID and password".*

Effect of factors that influence cybercrime

Effect of factors that influence cybercrimes category include narratives related to the view of e-library staff and network administrators on effect of the factors that influence cybercrimes academic libraries in Yobe State. It consists of single sub category: enhance continuity of cybercrimes. The individual subcategory is explained below:

Enhance continuity of cybercrimes: This sub-category emerged from the participants on the effect of the factors that influence cybercrime in academic libraries of Yobe State. Participant 5 remarked that, *"these factors would definitely influence cybercrimes when proper measures are not put in place. The moment any cyber culprit succeeded in breaking someone's account and gain a lot of money he/she will always continue to perpetrate cybercrimes".*

Discussion of Findings

Types of cybercrimes committed in Academic Libraries in Yobe State

This study found that five types of cybercrime were experienced by the e-library staff and network administrators. These include that using someone else's account, gathering of information to harm victims, illegal access to computer system online, cyber bullying and engineering phishing

In this study setting, the types of cybercrime experienced by network administrators and e-library staff are using someone else's account, gathering of information to harm victims, illegal access to computer system online, cyber bullying and engineering phishing. These types of cybercrime are similar to the types of cybercrimes revealed by Ribadu (2007). He stated that the prominent forms of cybercrime in Nigeria are cloning of websites, false representations, internet purchase and other electronic commerce kinds of fraud. Similarly, Olugbodi (2010) has shown

that the most prevalent types of cybercrime are website cloning, financial fraud, identity theft, credit card theft, cyber theft, fraudulent electronic mails, cyber laundering and virus or worm/Trojans. Also, a study by Barfi, Nyagome & Yeboah (2018) indicated participants affirmed that cloning of website/cyber phishing as forms of cybercrime in senior high school. The above cyber phishing is different with engineering phishing. As for engineering phishing, some participants stated that it occurs during process maintenance of someone ICT system.

However, this study further revealed that types of cybercrime committed in Academic Libraries in Yobe State are identity theft and viewing and downloading of pornographic movies. This was also in line with Barfi, Nyagome & Yeboah (2018), study that affirmed that cyber identity theft and pornography are among the forms of cybercrime perpetrated in school. This implied that the types cybercrime committed in academic libraries in Yobe State were using someone else's account, gathering of information to harm victims, illegal access to computer system online, cyber bullying, engineering phishing, identity theft and viewing and downloading of pornographies movies. Indeed, these have shown crimes and criminalities have been carried out in academic library, and some library clients are victims of the culprits.

Factors that influence the perpetration of cybercrimes in Academic Libraries

The findings indicates those factors that influences cybercrimes are poverty, technical know-how, lack of system security, lack of disciplinary action, lack or poor cyber policy, inappropriate monitoring and user's negligence. However, accesses to the internet, peer influence, economic, social and psychological were the significant factors affecting youth involvement in cybercrime (Oyenuga, 2019).The finding correlate with the findings of the study of Okeshola & Adeta (2013) that shown the motivating factors that derived individuals into cybercrime are quick luxurious comfort, easy to perpetrate, low chance of cyber criminals being caught and even lower chances of been convicted by law enforcement agencies, vengeance, sabotage, reinforcement of criminal behavior by family members, lack of resources to purchase original software, gain reputation among peer groups and pleasure.

This study showed that time and vulnerable websites served as factors that influence the perpetrated cybercrimes. Cyber criminals spend longtime online and utilize the opportunity when those monitoring the cyber activities were on break/lunch or at the mid night to committed crimes and also phish at vulnerable websites to extract information that aid them to hack into someone else's account. Oyenuga (2019) further revealed youth involved in cybercrime has been encouraged by the complexity and sophistication of internet. Therefore, this study exposed that these factors enhance continuity of cybercrime prevalence's in academic libraries.

Conclusion

Based on the findings, the study concluded that academic libraries in Yobe State have become vulnerable hubs for various cyber activities due to the integration of ICTs and internet connectivity. The research identified two primary categories of cybercrime: general experiences such as engineering phishing, cyber bulling, and illegal system access, and specific acts perpetrated within the library environment, notably identity theft and then downloading of pornographic content. These activities are driven by a complex interplay of socioeconomic and institutional factors. While poverty and a desire for a good life serve as primary external motivators, institutional

weaknesses including weak system security, lack of disciplinary actions, inappropriate monitoring, and poor cyber policies provide the necessary environment for these crimes to persist. Ultimately, the study reveals that without intervention, these factors create a cycle that enhances the continuity of cybercrime within tertiary institutions.

Recommendations

The following recommendations are proffered:

1. The Management of Federal University, Gashua, Federal Polytechnic, Damaturu and Federal College of Education (Technical), Potiskum should establish a quick response website where victims can report cybercrime cases along with digital forensic laboratory that would report cybercrimes related issues to the Management.
2. The Government and the Management of Federal University, Gashua, Federal Polytechnic, Damaturu and Federal College of Education (Technical), Potiskum should provide student Work-Study Programs to alleviate the financial pressures that drive students toward cyber fraud as a means of survival.

References

Abdulhamid, S. M., Haruna, C. & Abubakar, A. (2011). Cybercrimes and the Nigerian Academic Institution Networks. The *IUC Journal of Information Technology*, 7(1), p.47-57.

Adedeji Oyenuga (2019). Lucrative and Hidden: Factors Influencing Cybercrime Involvement Among Youth in Metropolitan lagos. *International Journal of Social Science and Humanities Reviews*, Vol. 1(2), 238-247p.

Babatunde, K. A., Muhammd, Y. A., & Aduku, S. B. (2019). Assessment of cyber and Social Media Crimes in the Library and ICT Unit of the Federal University, Gashua, Nigeria. *Journal of Environment, Technology & Sustainable Agriculture*, 1(1), 45-51.

Barfi, K. A., Nyagorme, P. &Yeboah, N. (2018). The Internet Users and Cybercrime in Ghana: Evidencefrom Senior High School in Brong Ahafo region. *Library Philosophy and Practice (e-journal)*, Retrieved on 12/6/2021, available at; https://digitalcommons.unl.edu/libphilprac

Chris, O. I. & Itodo, S. M. (2016). Cyber-crime and Nigerian business environment. *National Journal of Advanced Research*, 2(2), p. 28-38.

Lemo T (2013). Cyber crime: Nigeria redeems image. *The Punch*. http://www.punchng.com/business/technology/cyber-crime-nigeria-moves-to-redeem image/ Retrieved on 10th January 2013.

Okeshola, F. B. & Adeta, A. K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), p. 98-114.

Olaide and Adewole. (2004). Cyber Crime Embarrassing for Victims. Retrieved September 2014 from http//www.heraldsun.com.au

Olugbodi, K. (2010). Fighting Cyber Crime in Nigeria. Retrieved September 10, 2011 from http//www.guide2nigeria,com/news_articles_About_Nigeria

Ribadu, N. I. (2007). Cybercrime and commercial fraud: A Nigeria perspective. Modern law for global commerce congress to celebrate the fortieth annual session of UNCITRAL

Vienna, 9-12 July, PP1-3. Available online at http://www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf.visited 26th October, 2012

Saulawa, M. A., & Abubakar, M. K., (2014). Cybercrime in Nigeria: An Overview of Cybercrime Art 2013. *Journal of law, Policy and Globalization*, Vol. 32, p. 23-33. Available at: www.iiste.org/Journals/index.php/JLPG/article/view/18571/18708

Sesan G., Soremi B., & Oluwafemi B. (2013): Economic Cost of Cybercrime in Nigeria. Cyber Steward Network Project of the Citizen Lab. University of Toronto.

Yar, M. (2006). Cybercrime and society. London: Sage Publications.

Zero Tolerance. (2006). Retiree ins Trouble over Internet Fraud. Economic and Financial Crime Commission, 1(2)