Towards Determining Cybercrime Technology Evolution in Nigeria

S. O Aneke, E.O Nweke, C.N Udanor, I.A Ogbodo , A.O Ezugwu , C.H Uguwishiwu , M.E Ezema
Department of Computer Science, University of Nigeria Nsukka, Nigeria

***Abstract*--- With a generation that is highly mobile, there is the desire to quickly access information on the go. These may include logging into the office system to retrieve a file, check bank account status or make one form of payment or the other, or even monitor what the children are doing at home while at work, using IP cameras, etc. Technological advancement in the 21st century while trying to make life easier and better for the global citizens comes accompanied with its associated risks. One of the unknown risks is the situation of not knowing that one is taking a risk by putting one's information on the cyber space through the Internet. It is a known fact that the only assumption that can be made regarding the Internet is that it offers no security whatsoever. With the advent of the mobile phones, accessing the Internet is just a click away. This accessibility has become a necessary evil, as one is 'compelled' to fill one kind of form or the other with every click of the button, divulging personal information, not knowing who will intercept it for one reason or the other. This research through online survey and analysis tries to find out if cybercrime is a myth or a reality, especially in developing countries. If a reality, how do the cybercriminals extract information that may lead them to stealing vital information or money from their victims? Results suggest that cybercriminals of recent times seem to target individuals through SMS, E-mails and phone calls.**

***Keywords*--- Cybercrime, Scam, Cybercriminals, Cyber security, Information.**

I. INTRODUCTION

The world has witnessed technological advancements in diverse areas in order to make life simpler, better and easier. In as much as there are numerous undisputed benefits of technology, it does not rule out the fact that it equally has disadvantages. Some individuals perceived that the same technology could assist them to either perpetuate the traditional crimes or commit new and ever-increasing crimes. The computer or internet has become a tool or a target for committing crimes termed 'cybercrimes' in cyberspace. These crimes record high rates in developing countries, which could be due to the desire to live 'big' and be respected in the society. The author [1] describes Cybercrime as a common name for all sorts of different types of crimes which either take place online or utilized technology as means and or target for the attack. The simplest possible definition given is that, Cybercrime is a crime that has some kind of computer or cyber aspect to it. For every 3 seconds someone's identity is stolen as a result of cybercrime [2]. Cybercrimes do not consider any boundaries or territorial barriers. Making the cyber world safer is the major concern of all the stake holders. In this regard, every country will have and enforce its own Cyber law or Internet law to control the cybercrimes in their countries. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being [24]. Cybercrime has been observed as the fastest growing criminal activities across the world mostly perpetrated by young people, and can affect both individuals and businesses [1]. Scam is one of the cybercrimes, and according to [3], a scam can be defined as a fraudulent scheme designed and carried out by a dishonest individual, group, or company in a bid to obtain money or something else of value from unsuspecting persons, group(s) or organization(s). Also in [3], it was also discovered that scams traditionally operate easily in confidence tricks where a person misrepresents himself or herself as someone with skill or authority. According to [4], fraud is generally defined in the law as an intentional misrepresentation of a material's existing fact made by one person to another with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage. Fraud may also be made by an omission or purposeful failure to state material facts, which nondisclosure makes other statements misleading. The introduction of internet technology and its wide acceptance initiated new forms of scams or cybercrimes as can be seen in [3], such as lottery scams; scam baiting, email spoofing, phishing, or request for helps. These are equally considered to be email fraud.

The Nigerian Government did not relent in her fight against cybercrime which has been discovered to be on the increase since the introduction of the Internet technology. As contained in [5], the draft local legislation on electronic crimes, telecommunications and postal offences decree of 1995 define cybercrime to mean "Any person who, inter alia, engages in computer fraud or does anything to fake payments, whether or not the payment is credited to the account of an operator or the account of the subscriber, is guilty of an offence". The significance of cyber legislation and its imperatives in Nigeria, offences and penalties are equally contained in [5].

II. REVIEW OF CYBERCRIME METHODOLOGIES IN NIGERIA

Authors in [6] and [25] examined the 'Yahoo plus' Phenomenon, a new phenomenon in cybercrime which involved mixing spiritual elements with internet surfing to boost cybercrime success rates. In [25] the focus was more on the spiritual dimension of the operation of the 'yahoo boys', while [6] looked at the factors underlying the spiritual dimension to cybercrime, and discussed some of the strategies that were being employed while perpetuating this cybercrime using the Space Transition Theory (STT). The STT was used as a theory of cybercrime because of the fact that criminal behaviour is complex [6] and as a result requires specialized, lower-level theories instead of the generalized explanations of crime to adequately deal with the specific types of human conduct and social situations such as cybercrimes that are said to be characteristic of criminality or deviance. In other words, a theory that is needed should specifically address cybercrime in its entirety. The author [6] also found out three reasons why those involved in cybercrime resorted into using spiritual means to support their activities. First, because of the decline in the number of victims they got due to increased awareness of their techniques and strategies, secondly, the slow response rate from intended victims, and delayed success from their fraudulent transaction due to past experiences, and thirdly, the activity of the Nigeria anticorruption agency, Economic and Financial Crimes Commission (EFCC) and other security agencies.

Omodunbi et al [7] highlighted that the proliferation of the internet in almost all sectors makes cybercrime to be on the increase. The research exposed some sectors in Nigeria where cybercrime are perpetuated the most together with the type of cybercrimes mostly carried out. These include: the Banking Sector with crimes such as Bank Verification Number (BVN) scams, phishing email scams, theft of Automatic Teller Machine (ATM) cards for either 'ATM skimming' or internet order fraud, and cyber banking fraud by hacking into bank computer systems to steal small money from many bank customers; Electronic Business Sector having crimes such as intellectual property theft or software piracy, sale of forged or fraudulent goods or products, and theft of data and airtime from internet service providers; Educational Sector with crimes like cyber plagiarism and cyber pornography; Social Media Sector experiencing crimes like cyber stalking, with beneficiary or Nigerian Prince scam, charity-seeking funds scam, hijacking of social media pages or accounts. Further, the research conducted a survey in order to find out the extent to which university students are into cybercrimes and how exposed they were to such crimes. The authors discovered that majority of the students with their mobile phones were involved in data and airtime theft from service providers, because they consider it to be relatively safe while most of the students agree that internet phishing was the prevalent cybercrime used to swindle money or access personal information from victims. Authors in [8] looked at the economic impact of cybercrime on the banking sector of Nigeria and recognized phishing scam as one of the ever-increasing cybercrimes on the cyberspace since cyber criminals use that technique to fool unsuspecting 'netizens' (frequent internet users) and get them to disclose sensitive personal information such as their bank account details or part with their money after having gained their victim's trust and spoofed an authentic organization that they claimed to send emails from. Further [8] highlighted that the cybercriminals often mimic the emails of a real company while the link in the email redirects the victims to a fraudulent website. Also, cyber terrorism which could cause great damage both financially and physically involves laundering money to finance conventional terrorism using computer infrastructure. They operate by developing alliances with criminal organizations and mainly use credit card fraud to fund their activities. Authors in [9] reported on the surge of phishing activities on big industrial companies because they operate on large scales, overseeing large businesses and possessing large funds more than ordinary individuals. These cybercriminals first create convincing phishing messages normally accompanied with an infectious malwares as file attachments, which when opened infects the company's computer and begins to inspect and send snapshots of transactions. These are mainly sent on week days (and appear as original as the ones these companies receive from their real business dealers) to the company's employees. The article identified Alibaba as the email resources that the phishers use since their goal is to target companies that buy and sell products. Okeshola and Adeta [10] surveyed and analyzed cybercrimes in Nigeria. The survey was to discover the nature of cybercrime by finding out the category of people, the particular time, the places, how often, and the techniques used to commit the cybercrimes. It observed that young people, mostly males engage in cybercrimes and that majority of the people questioned in their survey agreed that the crime could be carried out at any time of the day, though some believed that it is committed at night. Again, it was revealed in the research that cybercrimes are mainly perpetuated at homes. Further, the techniques used to commit cybercrimes were highlighted as follows: SQL injection, mathematical model, man-in-the-middle, password crackers, honey-pot, key loggers, creation of illegitimate websites, and kernel level root kits. Finally, the predominant cybercrimes were identified as credit card fraud, hacking, software piracy, phishing, and the use of social media network. Unemployment, poverty, corruption and peer influence were identified as the key causes of the cybercrime, according to the study. The various cyber-attack techniques used by cybercriminals were identified in [11], to include the following: Botnets which are bots used to send malwares automatically, Fast Flux used to quickly transfer information to computers that send malwares such that it is hard to track the originating source of the malware being spread or the phishing websites, Zombie Computer which is a computer

already hacked into and being used to distribute malicious malwares or is made to be one of the botnets, Denial of Service attacks which involves overfilling a computer network or server with lots of data or messages so as to hinder legitimate users from using the network by making it unavailable. Another technique is Skimmers, which uses smart computer device to steal from unsuspecting owners their personal credit card information in places like ATM stands, stores, restaurants when the owners swipe their cards through those devices. Social Engineering which is a manipulative way of playing tricks in the minds of the target individuals in order to make them give out their sensitive and personal information is another tactics. Examples of social engineering crimes include phishing emails and websites, sending convincing email attachments containing malicious malwares that come in the form of games, or anti-malware software, demanding for passwords from their prospective victims while hiding under the guise of a network administrator for network maintenance for those people. It was highlighted moreover, in [12] that because of the strict security measures put in place on computers, the cybercriminals went beyond wasting efforts to break into and hack computers, to manipulating the trust or loyalty of employees of companies. They identified two major ways of doing that which are through CEO fraud and fraudulent invoice. The former involves the cybercriminal posing as an auditor or a highly placed individual in the company and using email or telephone to find out from among the employees, the person that is authorized to sign large amount of money during transactions. The criminal, still under pretense, contacts and demands from the employee in question to execute a secret transaction involving large sum into a foreign account for either a tax audit or something else that seems convincing. In a situation where the employee expresses doubt about the transaction, the criminal mounts pressure on him/her either by using rank to intimidate or by flattery or by calling names of influential people. The cybercrime is perpetuated successfully if the employee succumbs to the pressure and carries out the transaction. Again, in the case of Invoice fraud, the cybercriminal gains unauthorized access as 'man in the middle' to legitimate invoices posted or sent through email by seller companies or customers. They attempt to modify the bank account details in the original invoice to a different account owned by the scammer, thereby hijacking the transaction. A survey carried out by [13] emphasized that some of the factors that made cybercrime to be on the rise include the following: upsurge in the use of mobile phones, increase in the use of social networking sites, the security issues involved in the use of cloud computing, the tendency to take into consideration only the security of the computer systems instead of ensuring also that computer information is secured as well, the introduction of new computer devices and new platforms, and the desire to digitalize everything. Among the numerous cybercrimes perpetuated, [14] identified the prevalent ones in Nigeria and their methods of operation. These include: the CEO email fraud which is a phishing scam that spoofs the email addresses of the CEO of firms and finds out subtly employees that have control over large finances. Then social engineering technique is employed to ask the employee to send some large funds to an account belonging to the cybercriminal posing as the CEO. Again, Cyber terrorism uses the internet to add new recruits to a terrorist group such as Boko Haram in Nigeria and also for strategizing on the launching of attacks on their targeted countries. Moreover, Internet-Assisted Kidnapping uses the Geolocation data of devices like smart phones or Geotagging information of a person's social media account to track the location of their targeted victim and trace them. Further, Identity theft fraud involves the cloning or design of fake bank application web pages by scammers so that they could get personal account information of their targets. They may even create online forms in web pages that demand the unsuspecting people to fill in their personal details such as passwords and then use that information to perpetuate criminal activities on the cyber space. Finally, Hacking which could be achieved by having a background program installed on their target's computer unknown to them and then use those applications to steal sensitive information like passwords or information pertaining to a private data of a company.

A. Investigating the Impact of Cybercrimes

Using Qatar as a case study, [15] investigates the impact of cybercrime and the level of damage carried out, noting that financial gain may not be the only motivation for cyber related crimes. Their study is geared towards improving national security and creating awareness, while suggesting a global solution to cybercrime. It has also been reported that students may not have the knowledge of adequately reporting cybercrime and hence may be at the verge of loss when targeted or eventually become a victim of such acts. In their work, [16] explores the impact of cybercrime on undergraduate students in order to understand their awareness of cybercrime. This study was conducted through the use of interview and surveys, it was discovered that half of the subjects of the study had experienced one or more forms of cybercrime as a student; this includes phishing, hacking and malware. [17], explores the major causes and the various forms of cybercrime in Nigeria, they also explore the rate of victimization and economic cost to the country, proposing alternative strategies of reducing the dangers of these crimes.

B. Cybercrime Awareness and Prevention

A study among university students in Saudi Arabia carried out by [18] shows the security risks and awareness level of cybercrime in the area. Their study shows some of the reasons for cybercrime which includes financial, political, and cultural, also shows social networks as the greatest access for the penetration of cybercrime. Authors in [19] tested their

assumptions of users' avoidance of internet services being as a result of perceived fear of cybercrime. Using a structural equation modeling analysis they were able to test and disprove their assumption. On the contrary their result shows more determined users who are confident in using services such as online banking, online shopping and online social networking with little or no perception of the risk of cybercrime. In their work, [20] investigates individual's awareness of cybercrime in Nigeria and also the impact of these crimes on the economy of the country. In the work of [21], they explored and analyzed the nature of groups that were engaged in cybercrime. They equally outlined the definition and scope of cybercrime, theoretical and empirical challenges in fighting what has been known about cyber offenders, and the likely role of organized crime groups in escalating the activities of cyber criminals. In trying to prove the involvement of well organized groups in cybercrimes and related offences, the study has shown that the challenge facing this is the absence of well researched evidences to that effect nonetheless; it cannot be proved equally that organized groups do not engage in cybercrimes. Considering the growth of cybercrime in India, [22] makes an attempt to investigate into various cybercrimes committed in India, the author also reports on the government's response in countering these crimes in the country. Bhatti and Sami [23] uses real time data mining to complement the security of systems which will normally be unable to update themselves giving the fast rise in cybercrime. Because of the ever changing nature of the perpetrated cybercrime conventional systems find themselves lagging behind in catching up with the pace of these crimes in order to solve them. Their solution is targeted at some number of cybercrime.

III. MATERIAL AND METHODS

In an attempt to investigate the prevalence and methods of cybercrime operations, this research conducted an online survey among students between ages 16 years and 25 years, and professionals from ages 26 years and above. The analysis of the result from the respondents is presented below.

A. The Respondents

Out of the 66 respondents from USA, South Africa, Nigeria (93.4%), and Cameroun, 57.8% were between ages 16 and 25 years, while 42.2% were 26 years and above. Fig. 1 shows a pie chart distribution of the respondents. Fig. 2 shows that 66.7% of the respondents are students, while 33.1% are employed, and the rest are unemployed. Among the respondents, 77.3% were male while 22.7% were female.

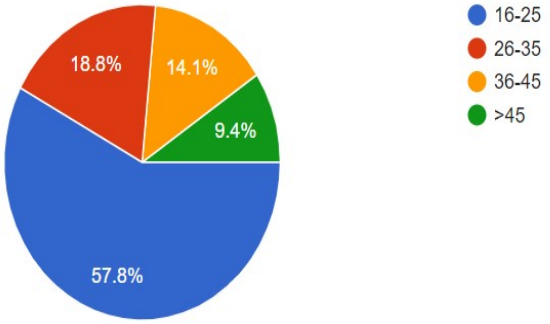

Fig. 1 A distribution of respondents

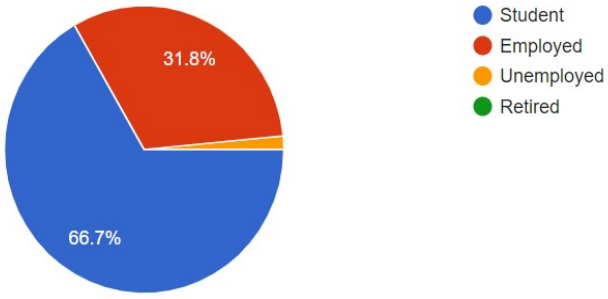

Fig. 2 Professional distribution

B. E-Platforms used by Respondents

Fig. 3 shows the percentage of the e-platforms used by the respondents. Mobile banking platforms come top with 74.2%, followed by social media (65%), and next is e-mail and ATM, each with 60%.

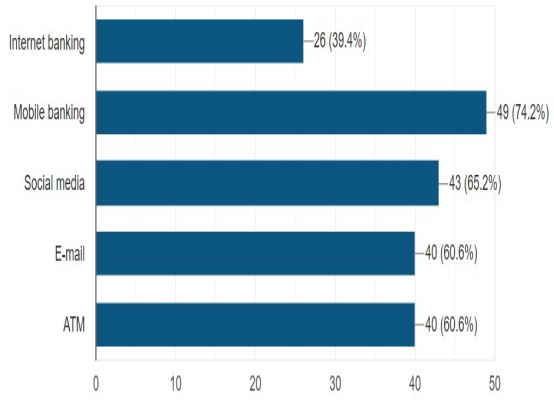

Fig. 3 E-platforms

C. E-Platforms used for Financial Transactions

Fig. 4 shows that Debit/credit is the most popular means of financial transactions with 67.7%, followed by Mobile banking with 58.5%, and Internet banking with 27.7%, etc.

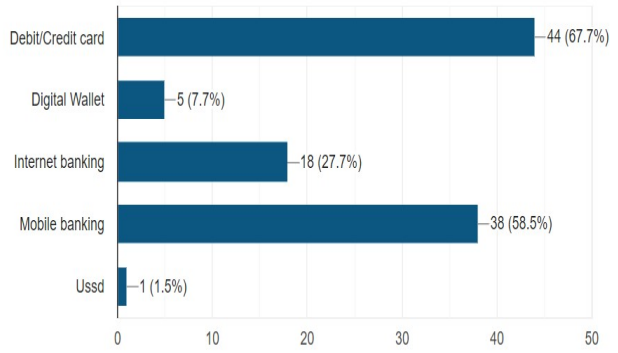

Fig. 4 Methods of financial transactions

D. *Financial crime target*

On whether the respondents have been targets of financial cybercrime, the response is as shown in fig. 5, of which 30.8% agreed to, while 20% are not sure, and rest said they have not been targets.

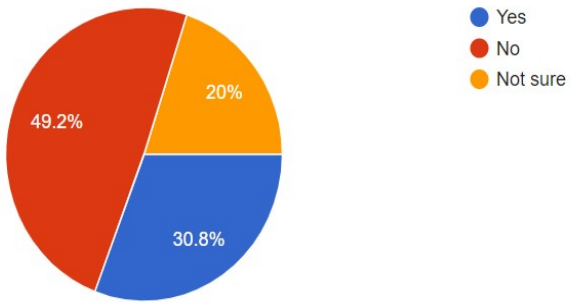

Fig. 5 Respondents' Percentage distribution of target of cybercrime

E. *Means of financial cybercrime*

Out of the 30% of respondents who agreed that they have been targets of financial cybercrime; 57.1% of the cybercrimes were perpetraded using SMS, 47.6% by E-mail, 42.9 through phone calls, while 19% was experienced though ATM, as shown in fig. 6.

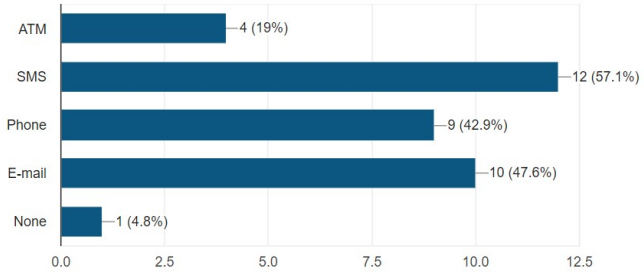

Fig. 6 Methods of financial cybercrimes

F. *Victims of financial Crime*

Eighteen percent (18%) of the respondents agreed to having fallen victims of cybercrime, while 10.8% are not sure if they had at any time been victims. The distribution is shown in fig. 7.

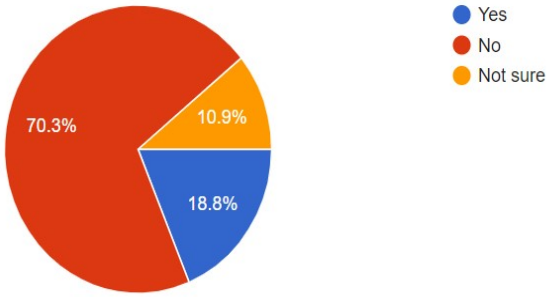

Fig. 7 A distributions financial cybercrime

G. *Means of cybercrime attacks*

Fig. 8 shows that out of the 18% of respondents who accepted being victims of cybercrime, 61.5% were through SMS, and 30.8% through phone calls, 15.4 were through ATM and phone calls, respectively.

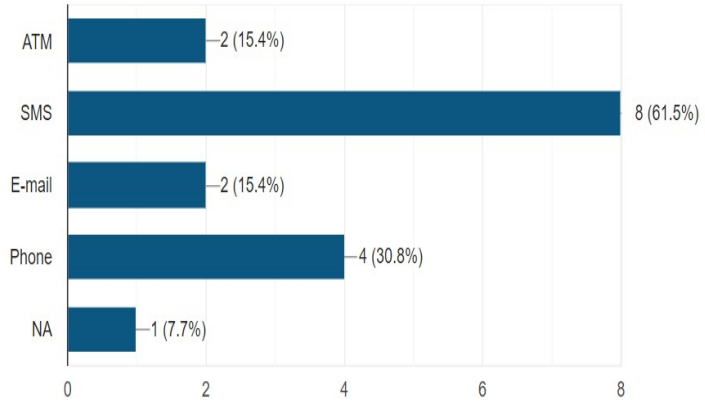

Fig. 8 Means of cybercrime

IV. RESULTS AND DISCUSSION

Findings show that most respondents belong to the youth class, who are usually more technology savvy. It is also discovered that these respondents use multiple platforms for financial transactions. It is significant to find out that 30% of the respondents have been targets of financial cybercrimes. It means that every 3 out of 10 people that use e-platforms are exposed to cyber-attacks. Surprisingly, SMS, E-mail, and phone calls have become the most common targeted avenues through which cyber criminals perpetrate cybercrimes. To corroborate this finding, the 18% of the respondents who have been victims of financial cyber-attacks gave SMS (61.5%),

and phone calls (30.8%) as the top two methods of financial cybercrime attacks.

Could it be that the technologies used by financial institutions are so advanced that the criminals were discouraged from trying to break in through those platforms? Or is it that e-platforms have become more personal than ever before, since the proliferation of mobile devices now make it much easier to reach the targeted victims through phone calls, SMS or E-mail at any time?

Secure4U [12], agrees that because of the strict security measures placed on computers, cyber criminals have moved to manipulating the trust of individuals. The cybercriminal posing as a familiar or a highly placed individual using email, SMS or telephone calls to target victims, convincing them to part with valuable personal information that may give the criminal access to the victim's finance, such as PIN, credit card number, BVN, etc. Ravi [13] thinks that the upsurge in the use of mobile phones, increase in the use of social networking sites, made cybercrime to be on the rise. Dambo [14] identified the CEO email fraud or phishing scam that spoofs the email addresses of the CEO of firms and finds out subtly employees that have control over large finances as the prevalent method of operation of cyber criminals in Nigeria.

V. CONCLUSION

The study through survey has established that cybercrime is a reality now in developing countries due to the adoption of technologies in every area of our daily lives. It is also discovered that the ultimate motive of the cybercriminal is to be able to steal money from victims, either directly or indirectly. An interesting finding is that cybercrimes today are more targeted at stealing vital information or coercing individuals to give out information that will lead the criminal to the victim's money and valuables. Mobile phones have become targets of cybercrimes, as they may contain information such as PINs, e-banking applications, SMS alerts, revealing text messages, etc. that may lead to stealing money from the victim. This study concludes with the takeaway that as technology has evolved, cybercrime methodologies have also evolved. For instance, with the advent of 3G or 4G mobile data networks, cybercrimes can be committed on the go. Gone are those days when perpetrators patronized cyber cafes with VSAT services. All that is needed now is either a mobile phone with data connectivity or a laptop with WiFi or a modem.

REFERENCES

[1] "Cyber crime and online safety". [Online]. Available: https://www.bedfordshire.police.uk/information-and-services/Crime/Cyber-crime-and-online-safety/Cyber-crime-and-online-safety. [Accessed: 17-Jul.-2019].

[2] Federal Investigation Agency: National Response for Cyber Crime. http://www.nr3c.gov.pk/cybercrime.html . [Accessed: 18-Jul.-2019]

[3] "What is scam? definition and meaning - BusinessDictionary.com". [Online]. Available: http://www.businessdictionary.com/definition/scam.html. [Accessed: 17-Jul.-2019].

[4] "Fraud Law and Legal Definition | USLegal, Inc.". [Online]. Available: https://definitions.uslegal.com/f/fraud/. [Accessed: 17-Jul.-2019].

[5] A Summary Of The Legislation On Cybercrime in Nigeria, The Communicator, Nigerian Communications Commission, NCC (2018) Issue 25, December, 2018. Available: https://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=899:a-summary-of-the-legislation-on-cybercrime-in-nigeria&catid=23&Itemid=179. [Accessed: 16-Jul.-2019].

[6] T. Oludayo (2013, October). "A Spiritual Dimension To Cybercrime In Nigeria: The 'Yahoo Plus' Phenomenon." *Institute for Research in Social Communication, Slovak Academy of Sciences, Human Affairs* [Online]. Vol. 23, pp. 689–705, DOI: 10.2478/s13374-013-0158-9. Available: https://link.springer.com/article/10.2478%2Fs13374-013-0158-9. [Accessed: 16-Jul.-2019].

[7] B. O. Omodunbi, P. O. Odiase, O. M. Olaniyan and A. O. Esan (2016, September). " Cybercrimes in Nigeria: Analysis, Detection and Prevention", *FUOYE Journal of Engineering and Technology* [Online]. Vol. 1, Issue 1. pp. 37-42. Available: http://engineering.fuoye.edu.ng/journal/index.php/engineer/article/download/16/pdf. [Accessed: 16-Jul.-2019].

[8] F. Wada and G. O. Odulaja (2014). " Electronic Banking and Cybercrime in Nigeria- A Theoretical Policy Perspective on Causation", *African Journal of Computing & ICT*[Online]. Vol 4, No 3, Issue 2. Available: https://pdfs.semanticscholar.org/fda3/23b00610705ddc20151480749cf27576da65.pdf. [Accessed: 14-Jul.-2019].

[9] Kaspersky Lab ICS CERT, (2017, June). "Nigerian Phishing: Industrial Companies under Attack", Secure List, June, 2017, Available at https://securelist.com/nigerian-phishing-industrial-companies-under-attack/78565/ [Accessed: 13th July, 2019]

[10] F. B. Okeshola and A.K. Adeta (2013, September). "The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria." *American International Journal of Contemporary Research*[Online]. Vol 3 No 9. Available: http://www.aijcrnet.com/journals/Vol_3_No_9_September_2013/12.pdf. [Accessed: 12-Jul.-2019].

[11] "How Cyber Criminals Operate." *Carnegie Mellon University* (2019) [Online]. Available at: http://www.carnegiecyberacademy.com/facultyPages/cyberCriminals/operate.html. [Accessed 13- July-2019]

[12] "How Cyber Criminals Operate". *KBC Secure4U (2019*) [Online]. Available at: https://www.kbc.be/corporate/en/info/internet-crim.html. [Accessed 12- Jul.- 2019].

[13] S. Ravi (2012, June). "Study of Latest Emerging Trends on Cyber Security and its Challenges to Soceity", *International Journal of Scientific & Engineering Research* [Print].Vol. 3, Issue 6.

[14] I. Dambo, O. A. Ezimora and M. Nwanyanwu (2017, November) "Cyber Space Technology: Cybercrime, Cyber Security and Models of Cyber Solution, A Case Study of Nigeria." *International Journal of Computer Science and Mobile Computing* [Online]. Vol 6, Issue11, pp 94- 113. Available: https://ijcsmc.com/docs/papers/November2017/V6I11201734.pdf. [Accessed: 12-Jul.-2019].

[15] A. Tabassum, M. S. Mustafa and S. A. A. Maadeed (2018, March). "The need for a global response against cybercrime: Qatar as a case study," *6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya. [Online]. pp. 1-6. doi: 10.1109/ISDFS.2018.8355331. Available: https://www.researchgate.net/publication/324031555_The_Need_for_a_Global_Response_Against_Cybercrime_Qatar_as_a_Case_Study. [Accessed: 14-Jul.-2019].

[16] M. Bidgoli, B. P. Knijnenburg and J. Grossklags (2016, June). "When cybercrimes strike undergraduates," *IEEE Computer Society*. Proceedings of the 2016 APWG Symposium on

Electronic Crime Research, eCrime 2016. [Online]. pp. 42-51 doi: 10.1109/ECRIME.2016.7487948. Available: https://pennstate.pure.elsevier.com/en/publications/when-cybercrimes-strike-undergraduates. [Accessed: 16-Jul.-2019].

[17] A.M. Dagaci, M. Sule, Y. M. Damagun (2014). "Cybercrimes and Victimization: An Analysis of Economic – Cost Implications to Nigeria." *Handbook on the Emerging Trends in Scientific Research,* Proceedings Book of ICETSR, 2014, Malaysia. ISBN: 978-969-9347-16-0 777

[18] Elrasheed Ismail Mohommoud Zayid and Nadir Abdelrahman Ahmed Farah, A study on cybercrime awareness test in Saudi Arabia - Alnamas region. DOI: 10.1109/Anti-Cybercrime.2017.7905290 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), March 2017

[19] M. Riek, R. Bohme and T. Moore (2016, March). "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance." *IEEE Transactions on Dependable and Secure Computing* [Online]. vol. 13, Issue 2, pp. 261-27. Available: https://ieeexplore.ieee.org/abstract/document/7056466. [Accessed: 16-Jul.-2019].

[20] O. Maitanmi, S. Ogunlere, S. Ayinde and Y. Adekunle (2013, January). "Impact of Cyber Crimes on Nigerian Economy." *The International Journal Of Engineering And Science (IJES)*[Online]. Volume 2, Issue 4. Pp. 45-51. ISSN(e): 2319 – 1813 ISSN(p). Available: https://www.researchgate.net/publication/309313165_Impact_of_Cyber_Crimes_on_Nigerian_Economy. [Accessed: 17-Jul.-2019].

[21] P. Broadhurst, P. Grabosky, M. Alazab, B. Bouhours and S. Chon (2014, January). "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime", *International Journal of cyber criminology* [Online]. Vol. 8, Issue 1. Available: https://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf. [Accessed: 15-Jul.-2019].

[22] P. N. V. Kumar (2016, March). "Growing cyber crimes in India: A survey," *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*, Ernakulam [Online] pp. 246-251. doi: 10.1109/SAPIENCE.2016.7684146. Available: https://www.researchgate.net/publication/311612941_Growing_cyber_crimes_in_India_A_survey. [Accessed: 14-Jul.-2019].

[23] Baber Majid Bhatti and Nouman Sami. Building adaptive defense against cybercrimes using real-time data mining. DOI: 10.1109/Anti-Cybercrime.2015.7351949. 2015 First International Conference on Anti-Cybercrime (ICACC), November 2015

[24] ITU-D, Understanding cybercrime: Phenomena, challenges and legal response. Available: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[25] S. A. Olubukola (2017). "Cybercrime and Poverty in Nigeria". Canadian Social Science, Vol. 13, No. 4, pp. 23-24.