IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 11, Issue 4 (July. – August. 2024), PP 10-16
www.iosrjournals.org

Cybercrime And Its Negative Effects In Developing Countries

Ugah John Otozi[1], Bernard Ephraim[2], Afolabi Idris Yinka[3], Mamah Chukwurah Hyginus[1]

[1](Department Of Computer Science, Ebonyi State University, Abakaliki - Nigeria)
[2](Department Of Computing Sciences, Admiralty University Of Nigeria, Ibusa, Delta State, Nigeria)
[3](Department Of Computer Science/Informatics, Alex Ekwueme Federal University, Ebonyi State, Nigeria)

Abstract:
Background*: This paper investigates the prevalence and the negative impacts of cybercrime in developing countries. It also attempts to proffer solution to the problem of cybercrime focusing on identity theft, phishing, and other cybercriminal activities that are common in 21st century. This research is imperative because cybercrime has become a teething problem to most developing countries where monitoring and tracking of cybercrime offenders is still a big challenge. In Nigeria for example, cybercrime comes in different forms and affects almost all aspect of human endeavor in our day due to the rapid expansion of internet access and digital technologies.*
Materials and Methods*: The research employs a mixed-method approach. First, it took a tour on different established cases of cybercrimes in recent time. It then carried out real life survey using a sample of about 68 students studying computing science in some universities in the southern part of Nigeria.*
Results*: Findings reveal a high level of concern about cybercrime among respondents, with many reporting personal experiences such as phishing attempts and identity theft via social media platforms like Facebook and Instagram. The discussion emphasizes the importance of cybersecurity education and robust government regulations to combat cyber threats effectively.*
Conclusion: *Recommendations include addressing youth unemployment, promoting ethical wealth generation, and strengthening cyber security laws to mitigate the socioeconomic and moral impacts of cybercrime in developing countries. This study contributes to understanding the multifaceted challenges posed by cybercrime in developing nations and underscores the necessity for comprehensive strategies encompassing policy reforms, educational initiatives, and socioeconomic interventions.*
Key Word*: Cybercrime, Security challenges, Developing countries, cyber threats, Impacts on society, policy.*

Date of Submission: 14-07-2024 Date of Acceptance: 24-07-2024

I. Introduction

Cybercrime is a criminal activity involving the use of computers and digital technology to commit illegal acts such as identity theft, hacking, cyberbullying, cyberterrorism, and phishing[1]. This has become a significant concern globally due to the advancement in technology and the widespread use of the internet. With the emergence of the Internet and communication technology, cybercrime began to take a frontal stage as its devastating negative impact became severe, especially in developing countries with poor infrastructure, little or no policy on Internet fraud, and weak legal framework[2]. Communication technology like the Internet serves useful purposes and helps in real-time communication, thereby enhancing businesses, education, and medical opportunities[3]. Unfortunately, the positive impact of the Internet has been significantly reduced by cybercrimes.

Developing countries remain particularly vulnerable due to poor policies and infrastructure to combat criminal activities in cyberspace. Nigeria, accounting for about 39.6% of African internet users, faces high vulnerability to cybercrime[4]. This vulnerability has adverse effects on the economy both small and large-scale businesses[1].

The effects of cybercrimes in developing countries like Nigeria can be excruciating, as individuals, businesses, and governments may experience negative impacts in several ways. Governments battle attacks on their websites and fake news, while individuals suffer identity theft, financial loss, and psychological harm. Businesses face reputational damage, intellectual property theft, and financial setbacks[3]. Therefore, it is crucial to explore the problems of cybercrime and its negative effects in developing countries using Nigeria as a case study. Understanding the prevalence of cybercrime, contributing factors to vulnerability, and its negative effects is essential for policymakers and practitioners to develop effective strategies to combat cybercrime[4]. Hence, this

paper is to provide an analysis of the problem of cybercrime and its negative effects in Nigeria by examining the frequent occurrence of cybercrime, identifying the factors that contribute to vulnerability, and verifying the negative effects of cybercrime on individuals, businesses, and the economy.

II. Review Of Related Literature

Several literatures were reviewed in the course of this research. According to [5] cybercrime is a criminal activity perpetuated using computer networks or the internet. [6] sees cybercrime as a series of organized criminal attacks on cyberspace and cyber security. This implies that". Cybercrime is closely connected to the term hacking which was first conceived at the Massachusetts Institute of Technology (MIT) in 1960 as a fancy way of describing the manipulation of computers. Hacking has, however, evolved to infer causing damage to information systems and computers[7]. The first occurrence of a major cyber attack which attracted legal sanction was by Robert Tappan Morris in 1988 in which he released a computer program that exploited a backdoor in the electronic mail system and a bug in a program that identified network users[8]. This program known as worm propagated across an estimated 6000 out of approximately 60,000 computers connected to the Internet in just 24 hours causing damages estimated to exceed $100,000[8]. Since then, cyberspace exploitation has been increasing and cybercrime has become recognised as a major international problem[9, 10]. [11] attributes the increase in security threats to the fast-paced growth and wide acceptance of the Internet; an increase in popularity infers an increase in opportunity for cybercriminals says [12].

Moreover, [12] holds that the Internet was originally built for research rather than commercial use and to this end, security was not considered in the design. Also, [13] using the term "digital optimism" explains that countries perceived cybersecurity as mainly a technical issue rather than a strategic challenge, hence decisive government actions were missing early enough. Cybercrimes can be in the form of email scams or phishing, online harassment (cyberbullying), malware attacks, identity theft, denial of service, child pornography, soliciting and producing child pornography, spreading hate and inflammatory terrorism, grooming, violating copyright, and selling illegal items[14], forgery such as fake documents, certificates, malvertising, ransomware, spamming, botnets, fake bank alert messages (SMS), and unsolicited SMS requesting you to provide bank details as Bank Verification Number (BVN)[15]. According to [13], the emergency of cryptocurrencies, though not bad, has introduced novel ways cybercrimes are perpetrated due to their pseudonymization and decentralized nature. In Nigeria, cybercrime is popularly referred to as "Yahoo Yahoo"[16, 17] and the individuals involved are collectively called "Yahoo boys"[17] and majorly carried out by youth[11]. The so-called Yahoo boys either scam single women by luring them into fake relationships online or present themselves as being in a very pathetic hardship hence endearing the victim to send money to them to help overcome the hardship[17]. They exploit psychological factors like instant gratification, willingness to help, and emotional connection of their victims who most times find it difficult to resist[18]. Usually, emails associated with this type of cybercrime have subjects like 'Re', 'Good day', 'Greetings', 'Dear friend', 'Confirm', 'Attention', and 'Hello dear'[18]. As [19] explain this causes a reduction in user trust in devices with Internet capabilities and a decline of trust in the use of these devices and the Internet which negatively affects customers' trust in e-commerce sellers[20] and leading to non-completion of purchase through e-commerce[10]. [16] cited that the potential for a gain greater than the risk, managers dissociating themselves from operations, lax computer security, inadequate caution in hiring, training and assigning personnel, and complexity of computer programs leading to human errors are among the culprits for cybercrime.

According to [21], the increasing unemployment rate and increased accessibility of internet services at low subscription fees[16] combine to serve as a boon to cybercrime in Africa. As well, [14] listed weak cyber security measures, the emergence and use of new technology by cybercriminals, and cybercrimes with business schemes are reasons for cyberattacks. In Nigeria, [11] and [15] outline unemployment, the quest for wealth, the lack of strong cyber laws, and incompetent security on personal computers as major motivators for cybercrimes. On a larger scale[22] attributes 39% of cyber fraud to be from external perpetrators (which included by percentage customers 26%, hackers 24%, vendors/suppliers or third parties 19%), 39% from internal perpetrators (where middle management takes 34%, operational staff 31% and senior management 26%), and 20% is attributed to collusion between external and internal perpetrators. In recent times, these cybercrimes have targeted private companies and government organizations as well since economic, commercial, cultural, social and governmental activities and interactions of countries at all levels take place in cyberspace[23]. [10] and [16] group the targets of cyber attacks as individuals, property, society and organisations. The financial sector is most vulnerable to cyber attacks[24]. Cyber attacks are either carried out to harm companies, individuals or groups financially or motivated by military or political intentions[23].

The effects of cybercrime are far-reaching, as put by [16] pornography and online prostitution undermine morality in society leading to the risk of a breakdown in moral values and norms, sudden accumulation of wealth through cybercrime negatively affects the socioeconomic well-being of a country with reduced levels of productivity, lack of trust in performing transactions within cybercrime prone countries is inevitable. [24] report that about 42% of companies and businesses initially affected by cybercrime are either in good shape or

experienced an increase in revenue as a direct consequence of management's decision to manage the crisis. As a solution to cybercrime and to improve trust and acceptance of new technologies, [13] advocates for a shift from "digital optimism" to "digital pragmatism" in which new technologies are "secured by design.

III. Material And Methods

In this research both qualitative and quantitative methods were adopted with a review of existing literature, surveys, and data analysis. The literature reviewed was on past and recent researches sourced from Google Scholar, Taylor and Francis, and Research Gate databases. The survey was carried out using questionnaire and it covered a total of about 68 respondents from different university students studying computer science.

Study Design: This study employed action research design. First, an investigative posture was adopted until the understanding of a problem was developed. Based on the understanding gained, interventionary strategy was used and pertinent observations were collected in various forms. The new interventional strategies adopted were carried out, and the cyclic process repeats, continuing until a sufficient understanding of the problem was achieved. The reason for using action study design is because an action search study has straight and clear relevance to practice. Action search design focuses on down-to-earth and solution-driven research rather than testing theories only. Again, this study design t conforms to the general design principles

Study Area: The study area for this research included two categories of people: University students and others who uses the Internet for one thing or the other.

Study Population: The population in this study was made up of 68 respondents from different schools and from other fields of life.

Data Collection Method: Two basic methods were used to collect data in this study. The instruments used were questionnaire and survey. The use of questionnaire ensures confirmation and completeness of data as well as increased confidence in the credibility of our findings. Extensive review of relevant articles and related literatures were also carried out to help establish the current status in this domain.

IV. Result

The problem that necessitated this study was the fact that cyber criminals are on the increase and many more persons are becoming a victim of cybercrime in developing countries. To get an insight into the nature and impact of cybercrime in developing countries taking Nigeria as a case study, a survey comprising 68 respondents was carried out with the majority of the participants being university students studying computing science. The research kicked off seeking for answers to some troubling questions. Responses were given on a scale of 1-5 questionnaires.

(i) How concerned are you about the increasing prevalence of cybercrime in today's digital landscape?

The following results were obtained at the end of the study.

(i) Eighty (80) questionnaires were shared out of which 68 responses were collected and analyzed. From the analysis carried out with about 96% of the respondents indicated that the increasing prevalence of cybercrime is a thing of concern. See Fig. 1.

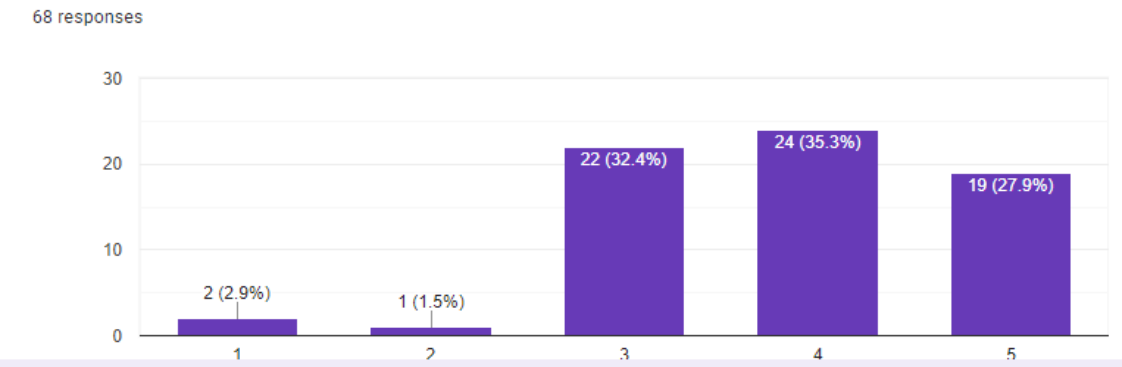

Fig. 1. Prevalence of cybercrime in today's digital landscape.

(ii) Have you or someone you know personally experienced any form of cybercrime, such as identity theft, online fraud, cyberbullying etc in recent times?

The following results were obtained at the end of the study.

(ii) Eighty (80) questionnaires were shared out of which 68 responses were collected and analyzed. From the analysis carried out 76.5% of the respondents reported Yes, suggesting that they or someone they personally know have been affected by cybercrime. See Fig. 2.

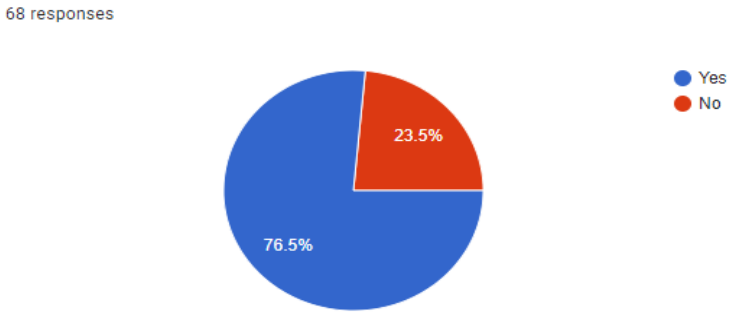

Fig. 2. Personal or close experience of cybercrime

(iii) Have you ever received phishing emails, phone calls from anonymous bank customer care representatives, or messages on social media platforms such as WhatsApp attempting to trick you into disclosing personal information?

The following results were obtained at the end of the study.
(iii) From the analysis of the response to this question, 92.6% of the respondents indicated to have received a one form of phishing emails or social engineered messages.
(iv) If yes in Q3, How often? specify the number of times.
The following results were obtained at the end of the study.
(iv) Out of the Eighty (80) questionnaires distributed, 58 respondents reported to have been targets of at least one to several cases of phishing or social engineered messages.
(v) From your experience which of the following platforms do hackers or "Yahoo Boys" use most to defraud people? Tick all that apply.

The following results were obtained at the end of the study.
(v) From the analysis of the responses to the platform commonly used by hackers, 60.3% mentioned Facebook, 57.4% mentioned Instagram and phone calls from the bank, 51.5% mentioned online adverts, 47.1% mentioned WhatsApp, 22.1% mentioned Twitter(X), 17.6% mentioned Snapchat, 13.2% mentioned Tiktok, and 1.5% mentioned Youtube. See Fig. 3.

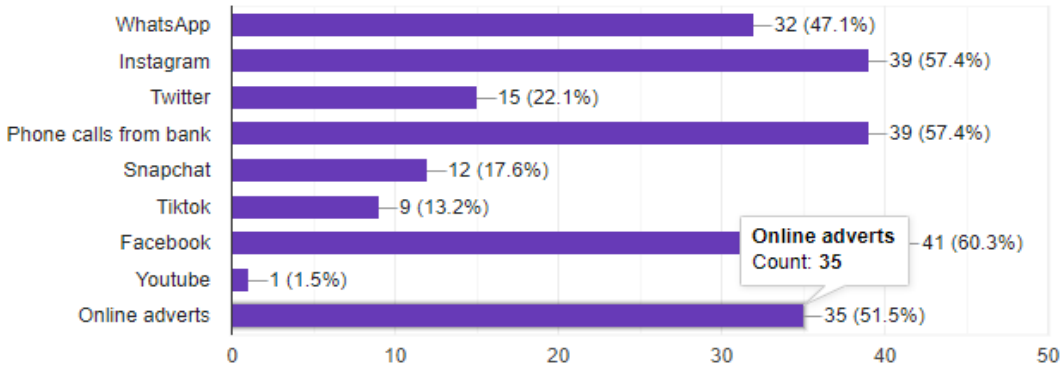

Fig. 3. Platforms used by hackers based on experience.

(vi) Have you ever been a victim of a cyberattack (online 419) that resulted in financial losses?
The following results were obtained at the end of the study.
(vi) The analysis of the response of casualties from cyber-attacks, 60.3% of respondents reported not to have lost financially to cyber-attacks.
(vii) If yes in Q6, What measures have you taken to prevent such incident from reoccurring?
The following results were obtained at the end of the study.
(vii) Analysis of the responses shows that the respondents apply the following measures to prevent the reoccurrence of cyber-attacks: 1) not doing online business with any unrecognized entity, 2) learning from victim experience, 3) not answering strange calls, 4) not listening to anyone they do not know well, 5) exposing the criminals by alerting others through the available social media channels, 6) not clicking on promo or giveaway

links, 7) using the True Caller app, 8) paying more attention to bank regulations, 9) stopping online transactions with unknown persons.

(viii) How familiar are you with the concept of ransomware attacks?

The following results were obtained at the end of the study.

(viii) From the 80 questionnaires distributed, 68 responses were received for this question. An analysis of the responses shows that 38% of the respondents are very familiar with the concept of ransomware attacks, 35% are unfamiliar with the concept of ransomware attacks, and 26% are unsure of their familiarity with the concept. See Fig. 4.

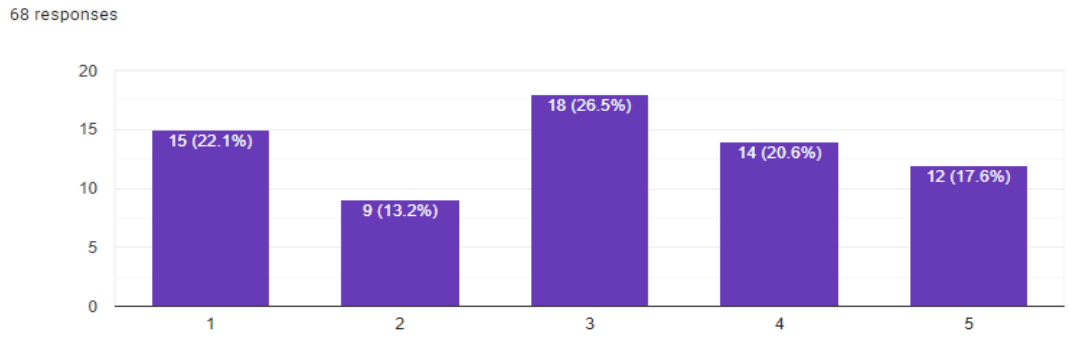

Fig 4. Familiarity with the concept of ransomware

(ix) Do you have the basic knowledge to mitigate such threats as ransomware attacks to your personal or professional data?

The following results were obtained at the end of the study.

(ix) An analysis of the 68 responses to this question shows that 50% of the respondents have basic knowledge of mitigating ransomware attacks on personal or professional data.

(x) On a scale of 1-5, What is the level of confidence you have in the security measures taken by the online platforms you regularly use to protect your personal information.

The following results were obtained at the end of the study.

(x) Analyzing the 68 responses obtained, 39.7% were very confident, 13.2% were confident, and 47.1% showed indifference to the level of confidence in the security measures put in place by online platforms they use on a regular basis. See Fig. 5.

(xi) To what extent do you believe that government regulations are effective in preventing and combating cybercrime?

The following results were obtained at the end of the study.

(xi) Out of the 68 responses received, 49.1% of the respondents do not believe that government regulations are effective in preventing and combating cybercrime, 5.9% believe that government regulations are effective in preventing and combating cybercrime, and 25% are indifferent.

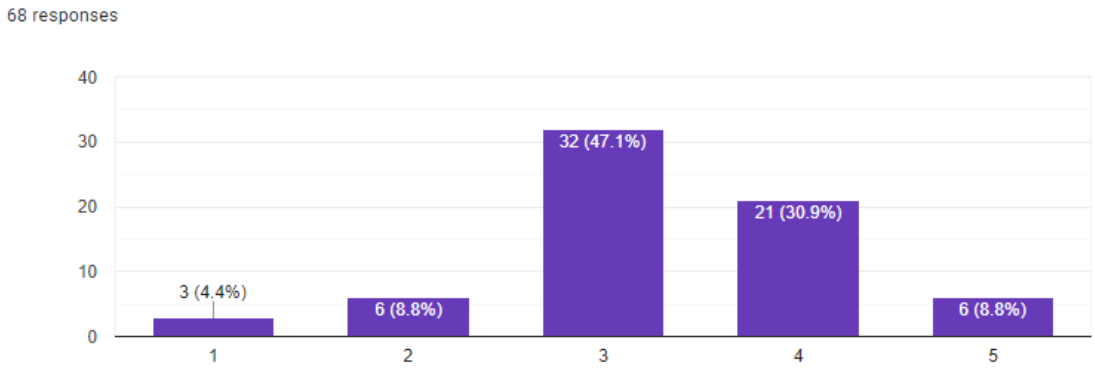

Fig 5. Level of confidence in security measures taken by online platform

(xii) In your Opinion, what role should educational institutions play in educating individuals about cybersecurity best practices to reduce the risk of falling victim to cybercrime?

The following results were obtained at the end of the study.

(xii) An analysis of the responses to the role of educational institutions in mitigating cybersecurity indicates that the respondents are of the opinion that educational institutions can engage in organizing public enlightenment through seminars and talks, teaching cyber security courses in schools, as well as counselling students.

V. Discussion

Based on the result of the analysis done in this research, it appears that cybercrime has become a thing of concern even in developing countries as the results of the survey show that the majority of the respondents indicated this as such. Most respondents reported having received at least one kind of malicious email, call, online advertisement, and message on social media channels or other attempt to trick them into disclosing personal information. The survey results show that Facebook, Instagram, phone calls from banks, online adverts, and WhatsApp are among the most targeted channels by cybercriminals. While Twitter(X), Snapchat, and TikTok were among the less targeted channels, YouTube was reported least.

However, it appears that the majority of the respondents who had been cybercrime targets were not involved in resultant financial losses, this could be that they are likely aware of the tactics of the cybercriminals or they were just lucky to decode the malicious conversation early enough. It is also, good to know that most of the respondents have countermeasures for cybercrimes which can be viewed as the ABCs of countering cybercrimes. The measures include using the True Caller app to reveal the identity of an unknown caller and even get the general sentiment of other True Caller users about the caller, not answering strange calls, not sustaining conversations with anyone you do not know well, being compliant with banking regulations, and not clicking on promo or giveaway links.

On the issue of ransomware, only a few are fully aware of ransomware with only 50% knowing how to protect themselves against it and this can pose a threat to the organizations that they may be working for. The survey shows that the respondents have more confidence in the effectiveness of the security measures put in place by online platforms to combat cybercrimes than in the government regulations drafted for the same purpose. The respondents suggested organizing symposiums, seminars and talks to enlighten the public on cybercrime and cybersecurity, counseling students probably involved as actors in cybercrime, and introducing cybersecurity courses into the school curriculum.

VI. Recommendation

From the outcomes of the survey and the reviewed literature, it is obvious that cybercrime has negative impact on the society in both the economic and moral fronts. The major contributing factor to the spread of cybercrime in developing countries is idleness of youth resulting from lack of or under employment. The government must do all in her powers to ensure that the youth are meaningfully and gainfully employed by making the ecosystem friendly to small and medium scale businesses and entrepreneurs. Another factor is inordinate quest for wealth. Success in most developing countries is measured by the amount of money (wealth) one has (not considering the legitimacy of the source), this mindset must be worked upon by the government (using its appropriate agencies) through counseling, public enlightenment, and rewarding individuals for good performance or behavior and prosecuting those who flaunt ill-gotten wealth. Furthermore, weak cyber laws and incompetent cyber security professionals is another causative factor. Developing countries have weak cyber laws regulating the use of personally identifying data, banking and credit card data and so on by agencies, businesses and institutions who employ less stringent security considerations while building public-facing software. An, effective cyber laws must be developed and implemented to force compliance by parties involved in building public facing software systems.

VII. Conclusion

This research has looked at the negative effect of cybercrime to youths, children, adults and to all aspect of human endeavors particularly in developing countries. It also attempted to recommend solutions to the problem of cybercrime in 21st century. The research focused on identity theft, phishing, and other cybercriminal activities that are common in our age. The truth is that the fight against cybercrime is an unending one but we must start somewhere to tackle it. It should be noted that cybercrime has the power to consume individuals, businesses and even governments that fall into its trap. It is therefore needful that all hands must be on deck to ensure that cybercrime and cyber criminal are totally eliminated or at least reduced to the minimum in our present time. We must therefore arise to contend with fox eating deep into the economy of countries. There should be establishment of cyber attack proof systems and laws. This will help provide desirable monitoring and also sustain user trust in performing transactions online. Fixing the issues of unemployment, underemployment, inordinate quest for wealth, legal and cyber practitioner competence would go a long way in this regard.

References

[1]. R. W. Taylor And E. J. Fritsch, Digital Crime And Digital Terrorism, 2016.
[2]. T. J. Holt And A. M. Bossler, "Cybercrime In Progress: Theory And Prevention Of Technology-Enabled Offenses," 2016.
[3]. D. S. Wall, "Cybercrime: The Transformation Of Crime In The Information Age," 2007.
[4]. K. Jaishankar, "Global Criminology: Crime And Victimization In A Globalized Era," 2018.
[5]. Merriam-Webster, "Cyber," 19 January 2024. [Online]. Available: Https://Www.Merriam-Webster.Com/Dictionary/Cyber. [Accessed 24 January 2024].
[6]. S. C. Pawar, R. S. Mente And B. D. Chendage, "Cyber Crime, Cyber Space And Effects Of Cyber Crime," International Journal Of Scientific Research In Computer Science, Engineering And Information Technology, Vol. 7, No. 1, Pp. 210-214, 2021.
[7]. R. Sabillon, J. Cano, V. Cavaller And J. Serra, "Cybercrime And Cybercriminals: A Comprehensive Study," International Journal Of Computer Networks And Communications Security, Vol. 4, No. 6, P. 165–176, June 2016.
[8]. Fbi, "Morris Worm," [Online]. Available: Https://Www.Fbi.Gov/History/Famous-Cases/Morris-Worm. [Accessed 24 January 2024].
[9]. S. M. Furnell, "Categorising Cybercrime And Cybercriminals," Journal Of Information Warfare, Vol. 1, No. 2, Pp. 35-44, 2001.
[10]. H. Saleh, A. Rezk And S. Barakat, "The Impact Of Cyber Crime On E-Commerce," International Journal Of Intelligent Computing And Information Science, Vol. 17, No. 3, Pp. 85-96, 7 2017.
[11]. O. Bolaji, P. O. Odiase, O. Olaniyan And A. Esan, "Cybercrimes In Nigeria: Analysis, Detection And Prevention," Fuoye Journal Of Engineering And Technology, Vol. 1, No. 1, Pp. 37-42, 2016.
[12]. L. Y. C. Chang And N. Coppel, "Building Cyber Security Awareness In A Developing Country: Lessons From Myanmar," Computers & Security, Vol. 97, 2020.
[13]. J. Świątkowska, "Tackling Cybercrime To Unleash Developing Countries' Digital Potential," Pathways For Prosperity Commission Background Paper Series, 2020.
[14]. D. Chudasama And R. S. Deora, "Brief Study Of Cybercrime On An Internet," Journal Of Communication Engineering & Systems, Vol. 11, No. 1, Pp. 1-6, 2021.
[15]. A. A. Muhammad, W. D. Daniel And I. Samson, "An Empirical Analysis Of Cybercrime Trends And Its Impact On Moral Decadence Among Secondary School Level Students In Nigeria," Ieee Computer Society - Nigeria - Technical Paper Series, Pp. 73-85, 2020.
[16]. J. T. Jackson And E. W. Robert, "Cybercrime And The Challenges Of Socio-Economic Development In Nigeria," Jorind, Vol. 14, No. 2, Pp. 42-49, 12 2016.
[17]. E. Moga, G. A. Salihu And R. Abdulkarim, "A Historical Assessment Of Cybercrime In Nigeria: Implication For Schools And National Development," Journal Of Research In Humanities And Social Science, Vol. 9, No. 9, Pp. 84-94, 2021.
[18]. V. P. Falade, "Trend And Emerging Types Of "419" Scams," Proceedings Of The Cyber Secure Nigeria Conference, Pp. 105-114, 11-12 7 2023.
[19]. R. Yoro, F. Obukohwoaghware, M. I. Akazue, A. E. Ibor And A. Ojugo, "Evidence Of Personality Traits On Phishing Attack Menace Among Selected University Undergraduates In Nigerian," International Journal Of Electrical And Computer Engineering (Ijece), 2023.
[20]. R. Apau, F. N. Koranteng And S. A. Gyamfi, "Cyber-Crime And Its Effects On E-Commerce Technologies," Journal Of Information, Vol. 5, No. 1, Pp. 39-59, 2019.
[21]. D. Olowu, "Cyber-Crimes And The Boundaries Of Domestic Legal Responses: Case For An Inclusionary Framework For Africa," Journal Of Information, Law & Technology (Jilt), Vol. 1, 28 5 2009.
[22]. Pwc, Pwc's Global Economic Crime And Fraud Survey, 2020.
[23]. Y. Li And Q. Liu, "A Comprehensive Review Study Of Cyber-Attacks And Cyber Security; Emerging Trends And Recent Developments," Energy Reports, Vol. 7, Pp. 8176-8186, 2021.
[24]. O. V. Sviatun, O. V. Goncharuk, C. Roman, O. Kuzmenko And I. V. Kozych, "Combating Cybercrime: Economic And Legal Aspects," Wseas Transactions On Business And Economics, Vol. 18, Pp. 751-762, 21 4 2021.