International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

# Cyberspace: Mitigating Against Cyber Security Threats and Attacks

Joshua J. Tom (Ph.D)
(Information Security & Cryptology)
Department of Cyber Security,
Admirality University of Nigeria, Nigeria

Abasiama G. Akpan (Ph.D)
(Cyber Physical Systems Group)
Department of Computer Science
Evangel University, Nigeria.

***Abstract*:- The rapid growth of the internet has led to increase in Cyber security threats and attacks that most exploit weaknesses in existing hardware, software, and network technologies. The desire of a novel and effective defense services, mechanisms and techniques have been considered as pressing requisites for the cyberspace. This paper investigates status of cyber security threats and attacks and clarifies what security measures are currently in place to minimize existential security risk. This study is exploratory and uses a survey conducted with questionnaires distributed to 635 students, lecturers and ICT experts. Findings revealed that the educated community not only lacks cyber security awareness but also knowledge of what is happening in the arena of the cyberspace. In this research paper, we proposed several recommendations including the fact that the National Orientation Agency should focus on the national re – orientation and awakening of the consciousness of the citizens particularly the youths and parents, towards raising citizens with strong moral training and ethical background through the integration of Cyber Ethics in our school curriculum.**

***Keywords: Cyber Security, Cyber Attacks, Cyber Threats, Malware, Counter measures, Vulnerabilities.***

## I. INTRODUCTION

Our society, economy, and critical infrastructures have become largely dependent on ICT solutions. The internet is used to exchange goods and services via various e-commerce transactions. Cyber attacks become attractive and devastating as the dependence on these technologies increases. Thus, a secure cyberspace is important to the health of the Nigerian economy and to the security of the global economy [1]. Cyber criminals have improved their tactics, techniques and procedures for exploiting the vulnerabilities of different web technologies, servers, browsers, etc. to the point where these vulnerabilities have become difficult to detect and challenging to investigate and remediate [2]. According to Symantec [2], a cyber attack is any kind of offensive act that targets cyber physical infrastructures using various methods to steal, alter or destroy data or information systems. Cyber attacks become lucrative business because attacks and threats are cheaper, convenient and less risky [3]. As discussed by Tatum [4], Cyber Attack is an attempt to weaken the functioning of a computerized system, or an attempt to track the online movements of individuals without their permission. Attacks of this kind may be unknown to the end user or lead to total disruption of the network infrastructures to the extent that none of the users can perform any tasks [5].

Cyber criminals are not limited by location and distance; they so elusive that they are difficult to identity and prosecute due to unsigned nature of the cyberspace. Given that attacks against cyber physical infrastructures are very eye-catching, it is expected that the number and the complexity of cyber attacks will be on the increase. Hence, cyber security threats are malicious act that destroy data, steal data, and disrupt digital life in general.

Cyber security involves defense strategies to curb cyber criminality in the cyberspace. It takes into consideration the understanding of various attacks and defense strategies that protect confidentiality, integrity and availability of any digital technologies and assets [7].

- *Confidentiality:* It means to prevent the disclosure of information to unauthorized individuals or systems.
- *Integrity:* It is means to prevent any modification or deletion of data in an unauthorized manner.
- *Availability:* It means to guarantee that the systems are responsible for delivering, storing and processing information accessible when needed and by those who need them. In the words of Kosutic [8], Cyber security is the technologies, practice, actions, designed to defend networks, computers, systems, application programs and data from an attack, damage or unauthorized access. In Cyber Security, emerging threats are categorized as malicious attacks, network attacks, or network abuse. Malicious attack is any effort to exploit another digital system and infect the system resources through Viruses, Trojan horses, Spywares etc. Network attacks are intended actions meant to cause damage to or disturb the flow of data of a digital system on a network, which causes effects such as Denial of Service (Dos), Session Hijacking, Email Spoofing, etc.[7]. Network abuse is fundamentally an exploit to the point of interaction of a network, and it could be utilized by actions such as spam, phishing, pharming, etc [8]. Cyber attacks are widely viewed as criminal action perpetrated through the Internet and web by means of the Web. These exploits can be directed against an organization's intellectual property, hijacking online bank transactions, designing and circulating Viruses on different digital systems, hosting secret Business Data on the Web and even destroying national critical network. Internet threats are the highest source of failure to businesses and revenue loses of most organization [9].

Experts consider malicious codes as the key alternative to carry out malicious intentions to breach cyber security efforts on the net [10]. Malicious codes or Malware refers to any attacks on the system, without the knowledge of the legitimate user to compromise the system to the benefit of an adversary. A typical example of malicious codes includes viruses, worms, Trojan horses, spyware, and bot executables [11]. They infect digital systems in many ways;

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

- Propagation from infected machines
- Tricking user to open tainted files,
- Alluring users to visit malware propagating websites.

A typical example of malicious codes infection is that it may load itself onto a USB drive inserted into an infected system, and then infect every other system into which that system is inserted. It may spread from devices and equipments that contain embedded systems and computational logic.

## II NATURE OF CRIME IN THE CYBER SPACE

Cyberspace is the interdependent network of information and communication technologies. This component is a crucial entity of Nigeria's and economy in particular, global economy and critical infrastructure in general. We use cyber space to transmit data, exchange information, and enable e-commerce transactions across a number of domains or sectors. The main targets of cybercriminals are data, network, and access [5, 13]. Cyber crimes under data crimes consist of *data interception*, *data modification*, *and data theft*. Data interception is the interception of data on transmission. Data modification is the change or destruction of data on transmission [14]. Data theft is the taking or copying of data, no matter whether it is protected by any laws or not. Access crimes include unauthorized access and virus dissemination can be considered as an example of such attack. Unauthorized access is the hacking or destruction of a network of system [14].

### *A. Demography and characteristics of Cyber Criminals*

In the study of ChiChao *et al.* [15], the population of cybercriminals is informative as well as alarming and calls for resolute effort by all to avoid an impending tragedy. The report findings indicates that 81.1% were male; 45.5% had some senior high school; 63.1% acted independently; 23.7% were currently enrolled students; and 29.1% were in the 18-23 age bracket, which was the majority group. For those enrolled student cybercrime suspects, the findings show that the percentage of junior high school and senior high school student suspects constituted 69.0% (2002), 76.1% (2003) and 62.7% (2004) of cybercrime suspects in their respective years. The high rate of cybercrimes shows that the number of currently enrolled students suspected of involvement in cybercrime is a cause for concern. The following groups of people easily fall prey or perpetrate cyber-criminalities are:

- Disgruntled employees
- Teenagers
- Political hacktivist
- Professional hackers
- Business rivals
- Ex-boy or Girl friend
- Divorced husbands or wives
- Political enemies

The victims are gullible, desperados and greedy people, unskilled and inexperienced and perhaps unlucky people too can fall victim [16].

### *B. Top 20 Countries with the highest rate of Cybercrime*

Symantec [2] listed and ranked 20 countries that cause the most cyber threats and attacks. In compiling such list, Symantec was able to put a figure on software code that interferes with a computer's normal functions, rank zombie systems, and observe the number of websites that host phishing sites, which are designed to trick computer users into disclosing personal data or banking account information [17]. Symantec was also able to obtain data including the number of bot-infected systems which are those controlled by cybercriminals, rank countries where cyber attacks initiated and factor in a higher rate of cybercrime in countries that have more access to broadband connections. The highest rate of cybercrime was found to be in the United States, which contributes to the broad range of available broadband connections, which are those that allow uninterrupted internet connectivity [18].

### *C. Top list of countries with lowest malware infection rates in computers*

Sweden-19.88%, Finland-20.65%, Norway-21.63%, Japan-22.24%, Belgium-22.78%, United Kingdom-23.38%, Switzerland-23.94%, Germany-24.12%, Denmark-24.34%, Netherlands-24.86% [18].

### *D. Corporate security Concerns*

Denis [19] reported top three computer security concerns. See figure 2.

(a) Embezzlement 30% (92), (b) intrusion or breach of computer systems 22% (67), and (c) computer viruses and denial of service attack 11% (33). These top three computer security concerns reflect the thinking of 63% of the organizations reporting.

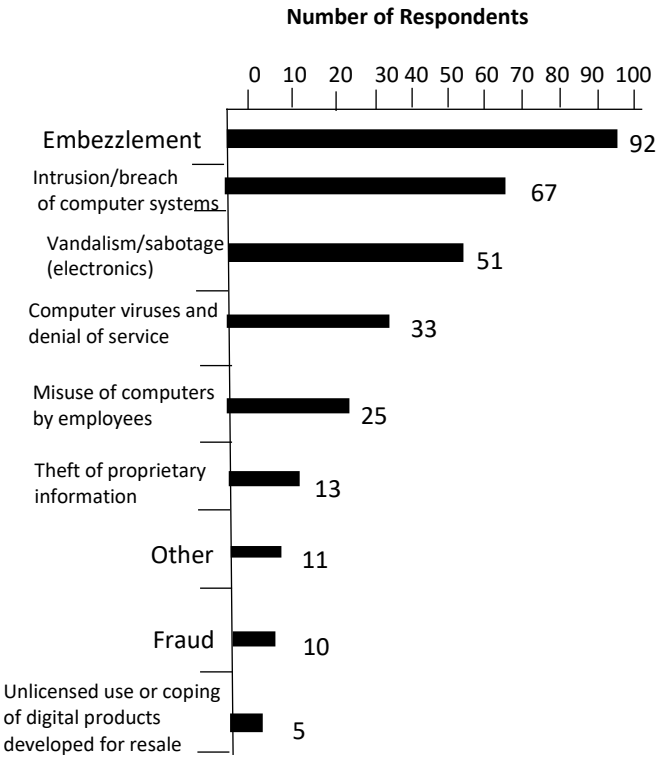


Figure 2: Ranking of computer security concerns by organizations [1].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

*E. Malware as attack tool*

Malware is used mainly to steal sensitive personal, financial, or business information and to target government or corporate websites to gather information or to disrupt their operations. In any case, malware is also used against individuals to gain personal information such as social security numbers or credit card numbers. For example, the greater part of prevalent malware have been designed to take control of user's computers for black market exploitation such as sending email spam or monitoring user's web browsing behaviors and displaying unsolicited advertisements [21].

## III. RESEARCH METHODOLOGY

The data for this research were mainly from secondary sources.

- Documents and Records: Thorough review of documents on crime analysis and mapping were done for the purpose of updating knowledge. This is crucial as it gives directions and enhances result.
- Scholarly Articles: The internet was the major method used during the collection of data. This helps greatly in providing the necessary information needed in the analysis. The information about cyber threats and attacks were gotten. The data collected, greatly enriched the analysis of this study.

## IV. EMERGING CYBER SECURITY THREATS AND ATTACKS

In this study, we seek to further discussions on some of the emerging cyber threats and attacks as follows;

- **Deepfakes:** It occurs when artificial intelligence technology creates fake images and sounds that appear real. Typical examples of deepfakes include creating a video in which words are manipulated, making it appear as if the person said something he never said.
  To reduce the risk, have strict verification procedures enforced.

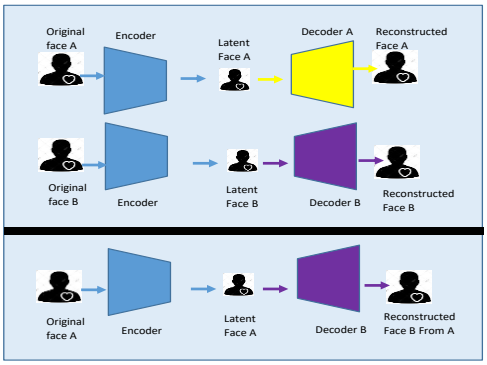


Figure 3: Deepfakes attack

- **Synthetic identities:** They are kinds of identity fraud in which scammers use a mix of real and fictitious identification to create false impression of a real person. Example, a criminal might create a identity that includes a legitimate physical address but social security number and birth date associated with that address might not be legitimate.
  To reduce the risks, ensure that your social security number, both physical and digital, is safe from thieves. Shred old documents that contain personal information.

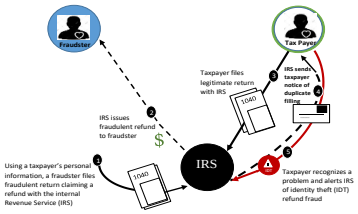


Figure 4: Synthetic identities

- **AI -Powered Cyber attacks:** In AI – Powered Cyber attacks, hackers are able to create programs that emulate known human behaviors. This can be use to trick people into giving up their personal or financial information.
  To reduce the risk, machine learning algorithms is use to learn from historical data and detect errors to enable firms to guide against such cyber threats and attacks effectively and efficiently.

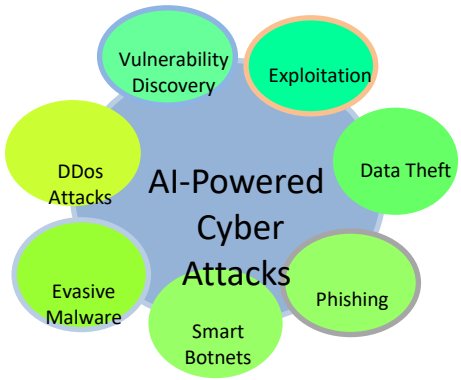


Figure 5: AI - Powered Cyber attacks

- **Poisoning attacks:** Artificial intelligence evolves. In these attacks known as poisoning attacks, cybercriminals can inject bad information into AI program. This bad information can cause the AI system not to function appropriately. Example, getting around spam detectors. To minimize the risk, DNS servers are subject to vulnerabilities. Staying on top of the latest patches can safeguard against attackers looking to exploit these well-known vulnerabilities.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

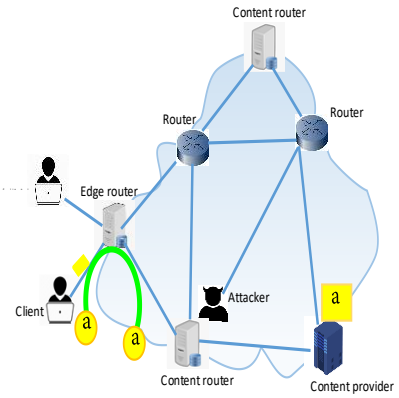


Figure 6: Content poisoning attacks

**Disinformation in Social Media:** This is the intentional spreading information that is inaccurate and designed to persuade electorate to take certain actions or hold specific views. Examples, social disinformation spread through social media such as Facebook, twitter, and even Whatsup App.
To reduce the risk, minimize profile information shared.

- **Advances in quantum computers pose a threat to cryptographic systems:** Quantum technology can decipher cryptographic codes that would take traditional system far longer to crack if they ever could.
To reduce the risk, apply strong cryptosystems with encipherment and implement long key spaces.

- **Autonomous Vehicle Cyberattacks:** Vehicular ad – hoc network allows cars to be connected to the internet, the threat of vehicle-based cyber attacks rises. Cybercriminals are able to access vehicles via this network to steal personal data, track the location or driving history of these vehicles, or even disable or take over safely functions.
- To reduce the risk, a risk-based prioritized identification and protection process for safety-critical vehicle control systems should be put in place.

- **Cloud Jacking:** Is a kind of cyber attack in which cybercriminals penetrate programs and system, stored in the cloud, and use these resources to mine for crypto currency.
To reduce the risk, restrict the IP addresses allowed to access cloud applications.

- **Ransomaware attacks:** The attacker infecting a victim's systems with a piece of malware that encrypts all of the data. The victim is then presented with an option of either paying the ransom or loses their data.
To reduce the risk, strong perimeter security, such as firewalls to prevent malware from uploaded to your systems.

- **IoT – Based Attack**s: It leverages on a victim's use of internet – connected smart devices to slip malware onto a network. To reduce the risk, keep the firmware for these devices up – to – date, as this can help resolve vulnerabilities that have been patched by the developers.

- **Denial-of-Service (DOS) and Distributed denial-of-service(DDOS) attacks:** A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. Examples are, TCP, SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and bonets.
To reduce the risk, IP addresses that are identified as being part of a DDoS attack are blacklisted.

- **Man-in-the-middle (MitM) Attack:** A MitM attack occurs when a hacker positions itself in between the communications of a client and a server. Examples are session hijacking, IP Spoofing and Replay attacks.
To reduce the risk, do not allow employees to use public networks for any confidential work, or Implement virtual private networks (VPNs) to secure connections from your business to online applications and enable employees to securely connect to your internal private network from remote locations.

- **Phishing and Spear phishing attacks:** It is the methods of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering trickery.

- **Spear phishing:** This is a targeted type of phishing activity where attackers' takes the time to conduct research into targets and create messages that are personal and relevant. To reduce the risk, a security policy must be develop that includes, but not limited to password expiration and complexity and deploy a web filter to block malicious websites.

- **Drive-by Attack:** Drive by download attacks are common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. To reduce the risk, one additional security control for preventing a drive-by virus infection is using different Web browsers, and only using vulnerable versions of IE on the specific applications that require it.

- **SQL Injection attack:** SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

the data base via the input data from the client to server SQL commands are inserted into data-plane input (for example, stead of the login or password) in order to run predefined SQL commands.
To reduce the risk, input validation, parameterized queries, stored procedures, escaping and web application firewall should be apply.

- **Cross-site scripting (XSS) Attack:** XSS attacks use third-party web resources to run scripts in the victims' web browser or scriptable application. Specifically, the attacker injects a play load with malicious JavaScript into a website's database. When victim requests a page from the websites, the web site transmits the page, with the website transmits the page, with the attacker's play load as part of the HTML body, to the victim's browser, which executes the malicious script.
To reduce the risk, an effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures filter input on arrival, encode data on output, content security policy and using appropriate response headers.

- **Eavesdropping Attack:** Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network.
To reduce the risk, Eavesdropping attacks can be prevented by using a personal firewall, keeping antivirus software updated, and using a virtual private network (VPN)

- **Birthday Attack:** Birthday attacks are made against hash algorithms that are used to verify the integrity of a message software or digital signature. It also refers to the probability of finding two random messages that generate the same MD when processed by a hash function.
To reduce the risk, the output length of the hash function used for a signature scheme can be chosen large enough so that the birthday attack becomes computationally infeasible, i.e. about twice as many bits as are needed to prevent an ordinary brute-force attack.

- **Malware Attack**-: Malicious software can be described as unwanted software that is installed in a system without the owner's consent. It can attach itself to legitimate code and propagate itself; it can lurk in useful applications or replicate itself across the internet. Examples are macro viruses, file infectors, system or boot record infectors, polymorphic viruses, stealth viruses, Trojans, logic bombs, worms, droppers, ransomware, adware, spyware.

To reduce the risk, Malware attacks can be prevented by using personal firewall and keeping antivirus software updated.

### *A. Security measures in place: Industry security initiatives for the cyber space:*

The followings are some of the Security measures in Place:
Firewalls, Antivirus, Anti-Malware, Pass-Wording, Encryption, Biometric Authentication Systems, Intrusion Detection and prevention Systems.

### *B. Some Tested Palliative solutions in place:*

If correctly installed, the following solutions can help to reduce cyber threats and attacks.

- **Firewalls:** Firewalls are hardware or software devices that block certain network traffic according to their security policy.
- **Software solutions:** Software exist to identify and remove malware and to help manage spam email. Many of them must be paid for but free versions are also available.
- **Authentication:** It involves determining that a particular user is authorized to use a particular computer. This can include simple mechanisms such as passwords, to more complex methods using biometric technology.
- **Hardware cryptography:** It uses computer chips with cryptographic capabilities intended to protect against arrange of security threats.
- **Patches:** They are programs designed by software manufacturers to fix software security flaws. Patched software are often installed automatically. This reduces end-user participation and increases ease of use

## VI. CONCLUSION

Cyber crime is real! The internet is the nervous system of world economy. Cybercrime is conducted remotely and anonymously to take advantage of flaws in software code. Cyber crime has created major problems and has continued to increase at institutions of higher learning. The academia is emerging as a particularly vulnerable for internet crime. Organizations and individuals have suffered losses at the hands of cyber-criminals with only nine percent of such incidents reported to the security operatives. There is need for consistent training of the Nigerian Police in Cyber Crime Prevention and Forensic science for cyber crime policy and control. There is urgent need to develop a single national database to gather and compile cybercrime data. The National Assembly should consider enacting legislations that encourages incident reporting while reducing the risks associated with reporting and provide policies that provide stronger consequences for those found guilty of committing cybercrimes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

## REFERENCES

[1] Akpan, A. G., Mmeah S. and Baah Barida (2018). Cybercrime and Cyber security: A painted scenario of a new type of war. *Journal of Scientific and Engineering Research*, 5(10):185-197.
[2] Watkins K.F. M – Trends 2017: A View from the front lines, Vol. 4, Premier Outlook 2017.
[3] Internet security Threats Report. Symantec, http://symantec.com/threatreprot/,last accessed: August, 2020.http://www.maawg.org/ last accessed: August, 2020.
[4] Goodman, S. E. and Lin, h. S. (2007). Toward a safer and more secure Cyberspace.TheNational AcademicsPress.Anti-phishing group tech report,http://www.antiphlishing.org/phishreportsAcrhive.html, last accessed: September, 2020.
[5] Tatum, Malcolm (2010). "What Is a Cyber-attack?" Available on-line from: http://www.wisegeek.com/what-isa-cyberattack.htm (Accessed 29th September, 2020).
[6] Alhaji Idi Babate, Maryam Abdullahi Musa, Aliyu Musa Kida, Musa Kalla Saidu (2015). State of Cyber Security: Emerging Threats Landscape. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, Vol. 3, Issue 1, pp. 113 – 119.
[7] Julian jang – Jaccard and Surya Nepal (2014). A survey of emerging threats in Cyber security. *Journal of Computer and System Sciences*. Volume 80, Issue 5, pp. 973 – 993.
[8] Whitney, S. (2004). Trend turns more purchase coverage for cybercrime. Best's review, 105(8): 90. Oldwick, NJ: AM. Best Co. Inc.
[9] Kosutic, D 2007, what is Cyber security and how can ISO 271001 help? Blog. Accessed 5 September,2020 <http://blog. iso27001standard.com/2011/10/25/what-is- cyber securityand- how-can-iso- 27001- help/#
[10] Williams, P. (2002). Organized crime and cyber crime: implications for business. Retrieved electronically on September, 2020.
[11] Canty, D. (2012). Digital Danger Zone: tackling cyber security. Arabian Oil and Gas, http://www.arabianoilandgas.com/article- 9868- digitaldanger-zone-tackling-cyber security/ last accessed September, 2020.
*[12]* Justin, M. Rao (2011).The economics of spam email metric MAAWG report Microsoft research.Available at:http://www.maawg.org/system/_les/news/ MAAWG 2013
[13] Ponemon, (2012) Cost of Cyber Crime Study: United Kingdom benchmark Study of UK Organizations, Ponemon Institute Research Report October.
[14] Australian Parliament the report of the inquiry into Cyber Crime http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf
[15] DHSS & TRoadmap for cyber security research, Jan. 2009 http://www.cyber.st.dhs.gov/docs/DHS - Cybersecurity-Roadmap.pdf(Accessed: September, 2020).
[16] ChiChao Li, Wen Yuan Jen & Weiping Chang, Shihchieh Chou (2006*), Journal of Computers*, Vol. 1, No. 6, Sept. 2006, Academicy Publisher, USA.
[17] Osuagwu O.E., Anyanwu E. (2003) Management of Information Technology at Periods of Technological Discontinuity, OIPH, Owerri, Nigeria, p. 23.
[18] Top 20 Countries found to have the most Cybercrime: https://www.enigmasoftware.com/top-20- countries-the-most-cybercrime/(Accessed September 10th, 2020)
[19] List of countries with lowest malware infection rates in computers: https://www.cybersecurity-insiders.com/list-of-countries-which-are- most-vulnerable-to-cyber-attacks/ (Accessed September 16th, 2020)
[20] Denise Marcia Chatam (2007). The Study on Cybercrime's Impact in the Workplace, Campus Technology, USA.
[21] McConnel, B. W. (2001). Hearing on Cybercrime, Committee on legal affairs and Human nights, parliamentary assembly of the Council of Europe, Paris, France: McConnelInternational.
[22] E.E. Schultz (2006). Where have the worms and viruses gone? New trends in malware Computer. Fraud Secure (7) (2006), pp. 4- 8
[23] Anti-phishing group tech reports: http://www.antiphishing.org/phishReports Archive.html (Accessed August 13th, 2013)