THE COLLOQUIUM -A Multi disciplinary Thematic Policy Journal
www.ccsonlinejournals.com
Volume 9 , Number 1 , 2021 Pages 175 – 181
CC-BY-NC-SA 4.0 International **Print ISSN : 2971-6624** **eISSN: 2971-6632**

INTERNET FRAUD IN NIGERIA: THE SECURITY LOOPHOLES EXPLOITED, IT'S DIMENSION AND IMPACT

[1]EGBE, Ola David, [2]EZE, Chimdiya Chiemeka, [3]OLADIMEJI, Biodun S. & [4]AGOHA, Uchechi K.
[1&2]Department of Computer and Robotics ,
Federal College of Education (Tech) Omoku, Rivers,State Nigeria.
[2&4]Department of Computer Science,
Federal Polytechnic Nekede, Owerri, Imo State, Nigeria.
Corresponding Email: david.ola@fcetomoku.edu.ng

Abstract
The digital world with its alluring benefits has brought with it lots of danger; cybercrime. Cybercrime is a threat to various institutions and individuals who are connected to the internet either through their computers or mobile phones technologies. In Nigeria today, several internets assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. This paper provides an overview of Cybercrime and Cyber-security loopholes that are exploited for attacks, its dimension and impact. To achieved the stated objective four research questions were formulated and quantitative data was collected from Nigeria's six geopolitical zones, the collated data was analyzed and the information from the analysis was represented on column and bar charts.

Keywords: *Cybercrime , internet fraud, security loopholes*

Introduction

The popularity of the internet which stems from the efficiencies it offers has forced a lot of processes, transactions and businesses to go online, which in time past has nothing to do with the internet. Making our lives inextricably interwoven with the internet and the trend is the new normal. Every IT solution come with new security challenges and loopholes that hackers can exploit to gain unauthorized access to systems and IT infrastructures with malicious inclination to steal assets, which has become the major opening for all forms of cybercrimes. Cybercrime can be defined according to Maitanmi and Ayinde (2013) "as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy breach, spam mailing and the likes". Computer device is the primary tool while the internet is the medium of connectivity through which these fraudulent breaches are carried out. Vadza (2013) classify cybercrimes into two main groups as: "using the computer to attack other computers. e.g. Hacking, Virus/Worm attacks, Denial of Service (DOS) attack etc." Secondly, "using the computer as a weapon: -using a computer to commit real world crimes. e.g. Cyber Terrorism, ATM and Credit card frauds, EFT frauds, Pornography etc." As new innovative technologies are introduced to the cyberspace, malicious users device new means of exploiting such systems that is why the dimension of attack vectors keep changing from time to time, that is why this research study the trends of cyber-attacks, the method of operations adopted for this nefarious acts with aim of keeping the security of IT systems and infrastructures ahead of the malicious users. Lastly, the factors that influence and motivate cybercrimes in Nigeria.

Cite this article as
Egbe, O. D., Eze, C. C., Oladimeji, B. S., & Agoha, U. K. (2021). Internet Fraud in Nigeria :The Security loopholes exploited, its dimension and impact. *THE COLLOQUIUM*,9(1), 175-181

THE COLLOQUIUM -A Multi disciplinary Thematic Policy Journal
www.ccsonlinejournals.com
Volume 9 , Number 1 , 2021 Pages 175 – 181
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

According to the FBI cybercrime report of 2020 as quoted by the Cable, Nigeria was "ranked 16th among the countries most affected by internet crime in the world in 2020". The report also indicated the amount of money lost from the illicit proceeds of internet crime globally in 2019 was $3.5 billion and increased to $4.2 billion in 2020. In addition to the report above, certain cybercrimes pushed up that index which "include phishing, non-payment/non-delivery, extortion, personal data breach and identity theft (Chinedu, 2021). According to the Guardian, the trend has risen considerably in 2022, with phishing hitting the top index. "The menace of cybercrime in Africa sustained a huge rising profile in the first six months of the year with phishing and scams hitting 438 per cent and 174 per cent in Kenya and Nigeria respectively". There are some literatures that are relevant to the dimension of cybercrimes in Nigeria they are discussed under the categories of cybercrimes below:

i.Hacking and Cracking

Hacking according to Albert (2018) is "any attempt to intrude into a computer or a network without authorization. This involves changing of system or security features in a bid to accomplish a goal that differs from the intended purpose of the system". The aim of hackers is to break the security locks on systems and gain an unauthorized access to systems with the goal of stealing and altering information and having control of such systems. The other side of hacking is the ethical hacking, that study hacking with the aim of being ahead of the malicious hacker, the experts in this area are employed to secure IT systems and infrastructure. Albert (2018) also added by defining a cracker as "someone who breaks into a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The main intention of both hacking and cracking is illegal access to systems and networks for negative manipulation. For instance, several accounts on Facebook and WhatsApp have been taken over by malicious hackers to defraud people this is called "social engineering" or "human hacking". Cracking is used mostly in software piracy; where the intellectual property of software developers is unlawfully duplicated by bypassing the unique installation codes that comes with those software to put a check on unlawful duplication.

ii.Spoofing

This when cybercriminals mimic individuals and organization with the intention of scamming them to divulge private information such as social media login details, bank account credentials like debit or credit card details which are used for fraudulent attacks. CompTIA (n.d.) added that "spoofing can apply to emails, phone calls and websites, or it can be more technical, such as IP spoofing, Address Resolution Protocol (ARP) spoofing or Domain Name System (DNS) server. Oftentimes spoofing is used during a cyberattack to disguise the source of attack traffic". Everything about spoofing is shrouded in deception and disguise to manipulate systems for the extraction of information. "Oftentimes spoofing is used during a cyberattack to disguise the source of attack traffic". One of the tools mostly used in spoofing attacks is **phishing** which on the word of Tutorialspoint (n.d.) "is a kind of social engineering attack where a person steals the sensitive information of user in a fraud manner by disguising as a legitimate person. In phishing, an attacker sends a phony ("spoof") message to deceive a human victim into giving personal information or allowing harmful software, such as ransomware, to be installed on the victim's infrastructure". The dimension of these attacks keep changing by adopting more novel tricky tactics as further emphasized in the following that "phishing attacks have evolved to the point that they now often transparently mirror the site being attacked, allowing the attacker to watch everything the victim does while surfing the site and cross any further security barriers alongside the victim. For example, hackers may request an OTP or secret PIN for a bank transaction via communication while posing as a bank employee, which is a kind of fraud".

iii. Malware, Spyware and Ransomware

These are types of computer virus that are designed to inflict different degree of harm to the system. According to Scale Technology (2020) "Malware is a broad term that refers to any software that is specifically designed to

Cite this article as
Egbe, O. D., Eze, C. C., Oladimeji, B. S., & Agoha, U. K. (2021). Internet Fraud in Nigeria :The Security loopholes exploited, its dimension and impact. *THE COLLOQUIUM*,9(1), 175-181

THE COLLOQUIUM -A Multi disciplinary Thematic Policy Journal
www.ccsonlinejournals.com
Volume 9 , Number 1 , 2021 Pages 175 – 181
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

harm your computer. There are different types of malware, including spyware and ransomware. Cybercriminals use malware to gain unauthorized access to "devices, corrupt files, or even lock down computers". Malware often operates undetected, and you will only know that your computer is infected when harm is already done". While spyware advance the cause of malware by spying on the systems and IT infrastructures to collect sensitive data, security information such as passwords and other user's login details from unsuspecting users, spyware often attached itself to user's software by monitoring online activities on websites and social media. Ransomware is another form of malware that takes charge of computers and network infrastructures for a ransom, this malicious software often takes charge of a system and its resources and asked the user for a fee to unlock the system.

iv.Identity Theft

This is the impersonation of individuals and organizations for financial and other illicit fraud. Vadza (2013) added that "Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes".

v.Unauthorized Access

This is gaining access to data without permission. The hackers use different means to extract security details from people and use such information to steal money and compromise cooperate network. Omodunbi et al., (2017) throw more light on the operation of those who use unauthorized access to penetrate into people's account and private information "Fraudsters make use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using POS, or at the ATM". An insider attacks are also probable using financial and identity credentials such ATM pins, bank verification number (BVN), and national identification number (NIN).

Hence, this paper provides an overview of Cybercrime and Cyber-security loopholes that are exploited for attacks, its dimension and impact.

Research questions

1. What types of cybercrimes are most prevalent in our clime?
2. Does gender influence participation in cybercrime?
3. What method of operation do cyber criminals adopt for their operation?
4. What are the factors that influences cybercrimes?

Methodolgy

The research adopted a quantitative approach, the data analysed was sampled from the six geopolitical zones in Nigeria, 40 structure questionnaires were assigned to each zone, with a total of 240 questionnaires administered and collated. This approach enables the researchers to analysed the collated questionnaires to make prediction by representing the percentages of respondents responses on each item using colum and pie charts as shown below.

Table 1: **Demographic Charateristic of the respondents**

Ages of Respondent	Frequency	Percentage
20 - 30 Years	85	35%
31 – 41 Years	92	38%
42 – 52 Years	46	19%
53 – 60 Years	17	7%

Cite this article as
Egbe, O. D., Eze, C. C., Oladimeji, B. S., & Agoha, U. K. (2021). Internet Fraud in Nigeria :The Security loopholes exploited, its dimension and impact. *THE COLLOQUIUM*,9(1), 175-181

THE COLLOQUIUM -A Multi disciplinary Thematic Policy Journal
www.ccsonlinejournals.com
Volume 9 , Number 1 , 2021 Pages 175 – 181
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

Sex		
Male	125	52%
Female	115	48%
Occupation of the respondent		
Undegraduate	53	22%
Postgraduate	48	20%
Civil Servant	98	40%
Business Owners	41	17%
Cybercrime by exposure		
Perpetrators	15	6%
Victims	25	10%
Non-victims/non-perpetrators	200	83%

What types of cybercrimes are most prevalent in our clime?

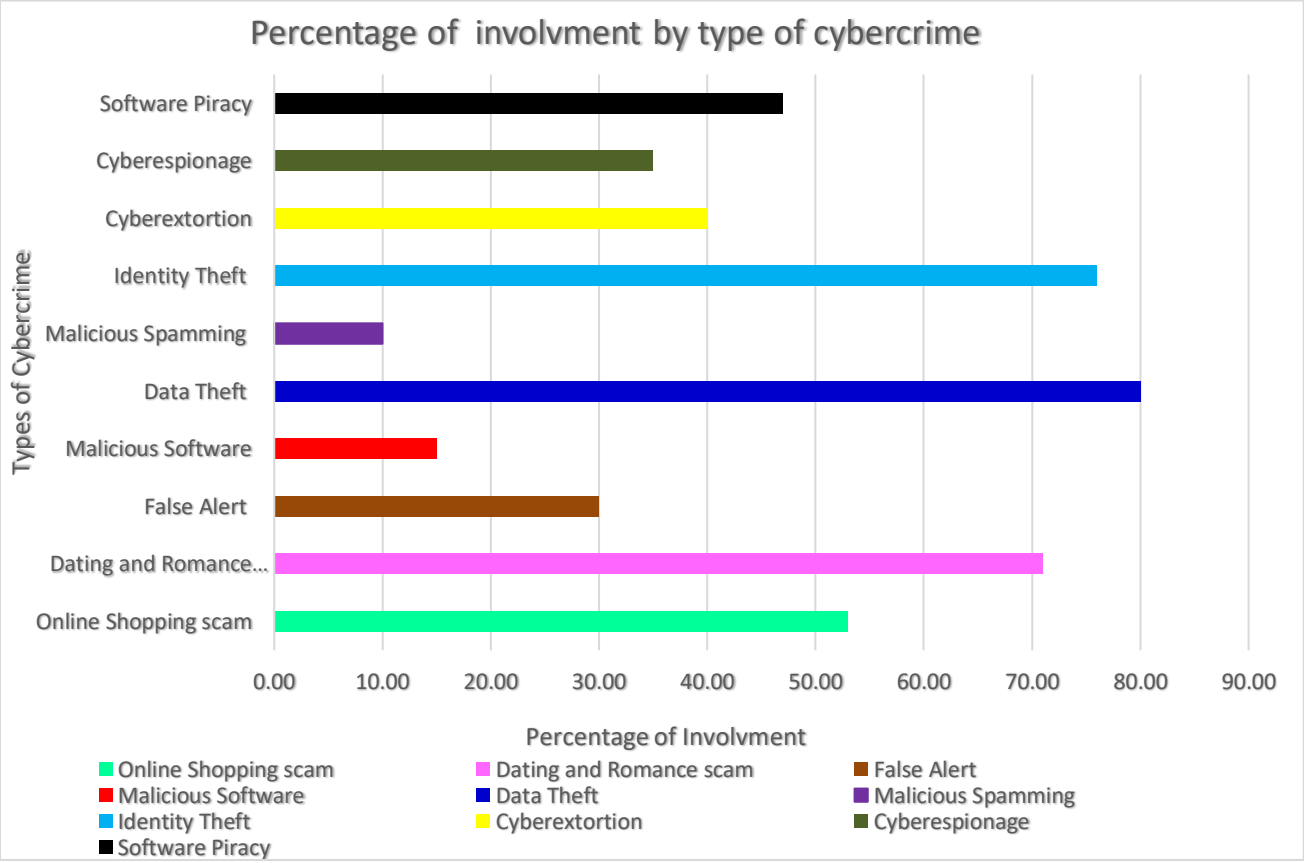

Figure 1: Percentage of involvment by type of cybercrime

From the chart in figure 1 above, the type of cyber crime that has witness the highest percentage of involvment is data theft, where scammers steal information of internet users from the cyber space and use those data to exploit their victims. Which is in agreement with Nigerian Deposit Insurance Corporation (NDIC) statistic, that report that between January and September 2020 Banks lost over 5 billion naira to fraudsters, and the channel and

Cite this article as
Egbe, O. D., Eze, C. C., Oladimeji, B. S., & Agoha, U. K. (2021). Internet Fraud in Nigeria :The Security loopholes exploited, its dimension and impact. *THE COLLOQUIUM*,9(1), 175-181

THE COLLOQUIUM -A Multi disciplinary Thematic Policy Journal
www.ccsonlinejournals.com
Volume 9 , Number 1 , 2021 Pages 175 – 181
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632
instrument through which the fraud and forgeries were perpertrated was through deceitful data theft on the internet (Egbe, 2021). ATM/card related fraud had the highest frequency accounting for 49.79 percnt of the fraud cases.

Do gender influence participation in cybercrime?

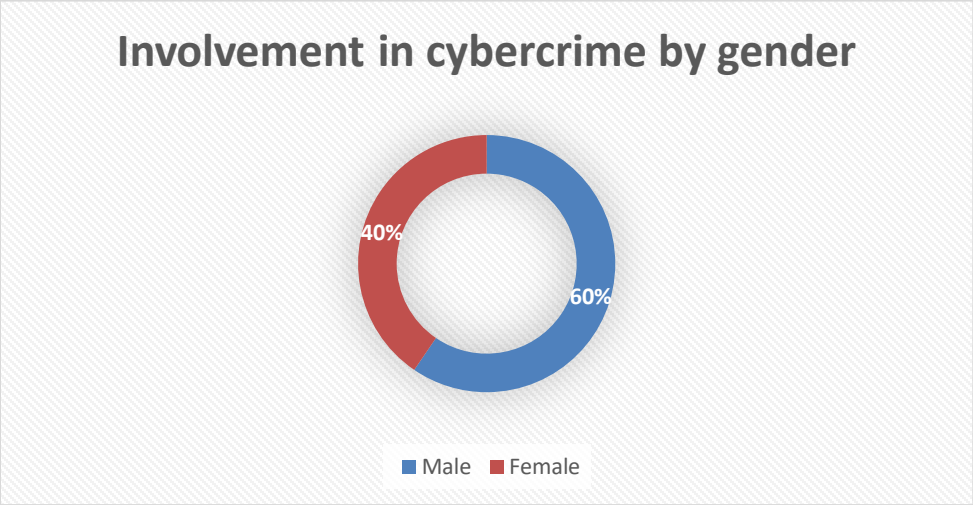

Figure 2: Cybercrime Involvement in cybercrime by gender

In the chart above, it is reveaved that, the male gender at 60 percent have higher involvment in cyber related crimes compared to their female counterpart at 40 percent.

What method of operation do cyber criminals adopt for their operation?

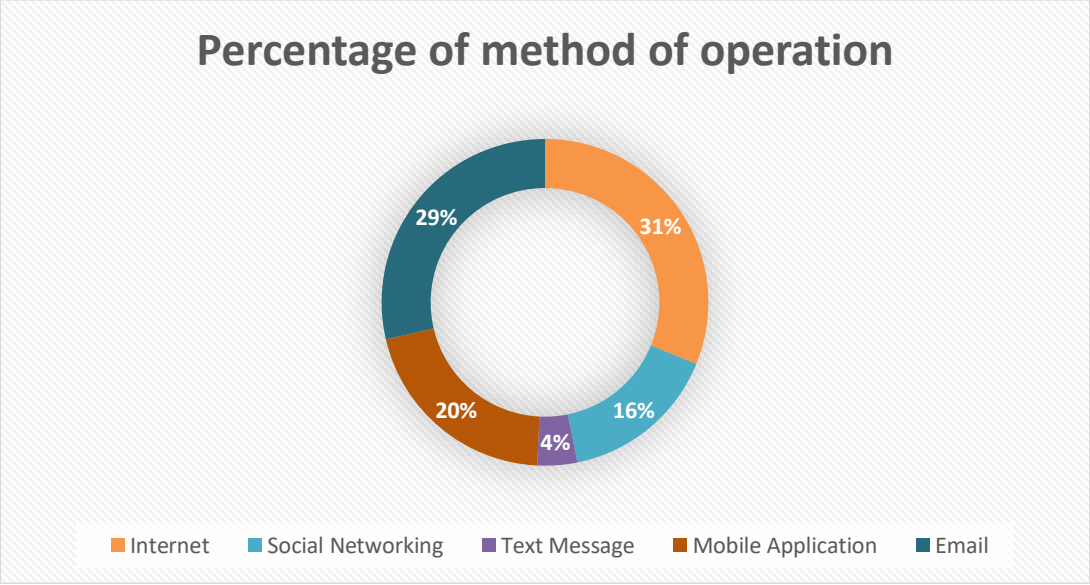

Figure 3: Percentage of method of operation

In figure 3 above the most common mode of operation is through the internet which accounted for 31 percent which is in line with NIDC report that the value of losses were higher in web-based internet banking fraud at 21.02 percent against other method operation (Egbe, 2021).

Cite this article as
Egbe, O. D., Eze, C. C., Oladimeji, B. S., & Agoha, U. K. (2021). Internet Fraud in Nigeria :The Security loopholes exploited, its dimension and impact. *THE COLLOQUIUM*,9(1), 175-181

THE COLLOQUIUM -A Multi disciplinary Thematic Policy Journal
www.ccsonlinejournals.com
Volume 9 , Number 1 , 2021 Pages 175 – 181
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

What are the factors that influenced cybercrimes?

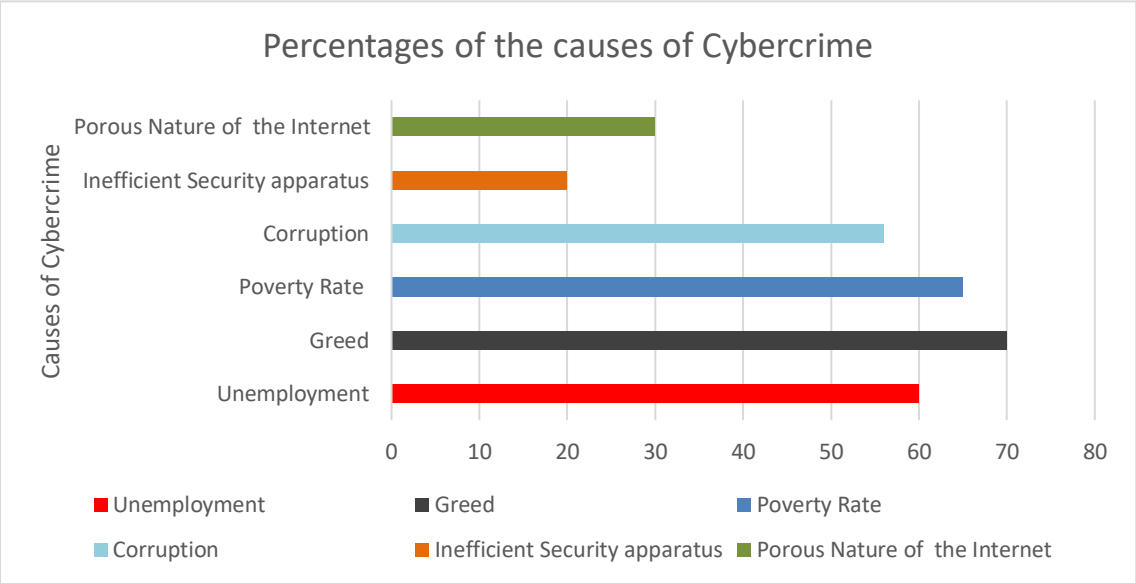

Figure 4**: Causes of Cybercrime**

In figure 4 above, even though poverty and umployment accounted for the major cases of cybercrimes in Nigeria. While Greed was indicated as the highest driving force as indicated on the chart with 70 percent. Proverty and uneployment stood at 60 and 65 percent respectively. While inefficient security framwork and porous nature of the internet were indicated as the causes of cybercrime.

Conclusion

Every IT systems are vulnerable, and most cybercriminals understood those vulnerabilities that is why robust security framework must be implemented to secure IT systems and infrastructures. In this study we have deduced from research question 1 that the most common avenue used to perpetrate various cybercrime is through data theft which is used as an opening for all manner of malicious operations leading to financial and data loss. This study also established that more male gender participate in cyber-related crimes than female. The internet account for the highest means of operation which was followed closely by social networking and greed, poverty and unemployment account for the facors that provoked and engendered cybercrime with greed at the top of the rank.

References

Adeyemi, A. (2022, August 03). Cybercrime rises as phishing hits 174% in Nigeria, 438% in Kenya. *The Guardian*. https://guardian.ng/business-services/cybercrime-rises-as-phishing-hits-174-in-nigeria-438-in-kenya/

Albert, K. D. (2018). Hacking Vs Cracking: What is the difference? https://www.dignited.com/31529/hacking-vs-cracking-difference/

Cite this article as
Egbe, O. D., Eze, C. C., Oladimeji, B. S., & Agoha, U. K. (2021). Internet Fraud in Nigeria :The Security loopholes exploited, its dimension and impact. *THE COLLOQUIUM*,9(1), 175-181

CC-BY-NC-SA 4.0 International **Print ISSN : 2971-6624** **eISSN: 2971-6632**

Maitanmi, O., & Ayinde, S. (2013), Impact of Cyber Crimeson Nigerian Economy, The *International Journal of Engineering and Science IJES*, 2(4), 45–51

Chinedu, A. (2021, March 18) Nigeria ranked 16th in FBI global cybercrime victims report. *The Cable*. https://www.thecable.ng/nigeria-ranked-16th-in-fbi-global-cybercrime-victims-report/amp

CompTIA (n.d.) What Is Spoofing? https://www.comptia.org/content/articles/what-is-spoofing#:~:text=Spoofing%20happens%20when%20cybercriminals%20use,protocols%20that%20run%20the%20internet.

Egbe, R. (2021, March 8). Banks lose N5bn to fraudsters in nine months – NDIC. *The Nation*. https://thenationonlineng.net/banks-lose-n5bn-to-fraudsters-in-nine-months-ndic/

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. *Journal of Engineering and Technology*, (1)1, 579-617

Scale Technology (2020). What is the difference between spyware, malware and ransomware? https://www.letscale.com/what-is-the-difference-between-spyware-malware-and-ransomware/

Tutorialpoint (n.d.) Difference between Spoofing and Phishing. https://www.tutorialspoint.com/difference-between-spoofing-and-phishing#:~:text=Spoofing%20is%20an%20identity%20theft,confidential%20information%20from%20a%20user.

Vadza, K. C. (2013). Cybercrimes and its categories. *Indian Journal of applied research*, 3 (5), 130-143.

Cite this article as
Egbe, O. D., Eze, C. C., Oladimeji, B. S., & Agoha, U. K. (2021). Internet Fraud in Nigeria :The Security loopholes exploited, its dimension and impact. *THE COLLOQUIUM*,9(1), 175-181