WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Vulnerability and Safety of Computing Devices on the Internet

Chapman Eze Nnadozie[1], Mrs. Benisemeni Esther Zakka[2]

[1]Principal Lecturer, Computer Science Department, Abubakar Tatari Ali Polytechnic, Bauchi, Bauchi State, Nigeria
[2]Principal Lecturer, Computer Science Department, Federal Polytechnic Bauchi, Bauchi state, Nigeria.
DOI: https://doi.org/10.55248/gengpi.5.0524.1428

A B S T R A C T

The Internet, a collection of inter-connected computing devices on a global scale, has come to stay with its inevitable benefits and risks. Cybersecurity, a framework that portrays the safeguarding of computing devices from cyberattacks, is vital in ensuring one's safety while surfing the net for services. The objectives of this study are to identify some of the key constraints to cybersecurity which comes in the form of cyberattacks, its effects on their victims, and to highlight the key proactive preventive measures as well as proffering some remedies. The methodology undertaken in this study is the use of questionnaires collaborated with existing literatures to ascertain the veracity or otherwise of the outcome. The findings show that more awareness need to be created on why users need to - have backups of their essential data, terminate their online sessions once done, avoid public networks; and possibly subscribe to a Virtual Private Network (VPN).

Keywords: B*ackups, Computing Devices, Cyberattacks, Cybersecurity, Internet, Safeguarding, Virtual Private Network.*

1. Introduction

The Internet, being the fastest growing infrastructure in our contemporary world, needs adequate measures to be taken by users in order to safeguard their data while online. The proliferation of mobile devices and services on the Internet makes it inevitably impossible for anyone to intentionally avoid the usage of the internet.

Historically, the Internet was discovered in the 1960s solely for the use of the US defense and researchers. The attacks were only limited to opponent's computers to damage it. In the 1980s, viruses were first introduced and heard which led to the malfunctioning of infected computers. Officially, the Internet was launched to be used by the public in 1996 [1], [2].

During the covid19 pandemic era in 2020, online communication was re-enforced which eventually led to the rapid increase in the use of the Internet [3]. This invariably led to a consequential increase in the level of cyberattacks. Therefore, there is urgent need to checkmate the cyberspace by taking adequate preventive measures to counter to some extent the growing threats that is portrayed on the cyberspace.

Cybercrimes cuts across all strata of our society – be it an individual, family, group, organization or even government. This paper examines vulnerability of our computing devices while on the Internet and possible ways through which we can enhance the safety of our devices while online.

2. Problem Definition

The growing need for Internet access has been on the rise right from the Covid19 pandemic era till date. The sudden rise on the usage of the Internet has also given rise to an increased rate in cyberattacks as cybercriminals search the Internet restlessly for vulnerable devices to invade. This study intends to explore the vulnerabilities and safety measures that is needed to safeguard our devices on the Internet.

3. Objectives of the Study

This study intends to –

1. Identify the constraints to cybersecurity;
2. Identify the effect of cyberattacks on its victims;
3. Identify possible proactive preventive measures as well as possible practical remedies that can be taken to guarantee a good level of safety while surfing the net.

4. Research Questions

The research questions advanced for this study are as follows -

1. What are the constraints to cybersecurity?
2. What are the effects of cyberattacks on its victims?
3. What are the possible proactive preventive measures as well as practical remedies that can be taken to guarantee safety of the users' browsing sessions?

5. Literature Survey

Cybersecurity can be defined as "the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access" [4]. It can be divided into five segments namely – application security, cloud security, critical infrastructure security, mobile security, and network security. Application security outlook is to ensure that individual/organizational network is safe from cyberattacks. Cloud computing is utilised by organizations like Google, Microsoft and Amazon to protect activities undertaken in their respective clouds through the use of robust authentication methods geared towards protecting the user's data. Mobile security is designed to protect individual devices on the cyberspace from cyberattacks. Network security is designed to ensure that organizations network is safeguarded from every form of disruption and abuse from within and outside the organization [5]. Similarly, this view on cybersecurity is upheld by [6] which holds similar view on the segments of cybersecurity but however added disaster recovery, identity management and data security. Identity management and data security entails that every organization should have a seamless process procedure which would enhance the safety of its customers. Disaster recovery refers to putting good strategies in place which would guarantee the continuity of organization's information system despite any unforeseen eventuality like natural disaster.

Cyberthreats is getting more sophisticated by the day as no organization can claim to be completely free from cyberattacks. Cyberattack target can be directed to a user, group or organization's infrastructure. These attacks can be perpetuated through phishing, identity theft, malware, etc. Attacks directed at the infrastructure can be malware, Distributed Denial of Service (DDOS), etc [3].

6. Constraints to Cybersecurity

There are several things that can pose as hindrances to an effective cybersecurity. Some of these constraints include improper configuration of firewall, high cost of setting up a robust cybersecurity, human error, lack of regular updates on the software used, shortage of skilled professionals, and lack of backups.

Improper configuration of firewall can lead to unnecessary delays on the system's processing ability thereby hampering its safety [5]. The cost of setting up a robust cybersecurity model for any organization is often huge. Therefore, enough may not be budgeted for it, especially for a struggling organization [3], [7]. Human errors or system failure can compromise the cybersecurity of systems as these sometimes can energize pending threats [3], Similarly, [8] holds same view when it says that negligence on the part of the user can lead to losses. In ensuring a secured cybersecurity environment, regular updates on applications, data, network, cloud and mobile infrastructure have to be done timely. Furthermore, shortage of enough skilled professionals on cybersecurity is another factor because they are the people that are trained to understand fully the dynamics behind cybercrimes. [7], [9]. In a similar development, [1] advocates the need to have an Incident Monitoring Team in every organization whose duty would be to monitor and detect security bridges early enough and block such before they succeed. Lack of backups for our data also poses a constraint to the safety of our computing devices. It is needful to always create backups for data, protect your passwords, and update software regularly [10].

In furtherance to the constraints, factors like corruption, increasing rate of poverty, and unemployment is fuelling cybercrimes [11]. When a cyberattack occurs, it rocks havoc on the victim in particular and the society at large. Attacks had predominantly been through phishing, ransomware, virus, DOS, and DDOS. However, with the advent of artificial intelligence, hackers can now use some sophisticated tools like bots to further penetrate vulnerable devices [12]. Therefore, it is imperative that everyone needs to be guided against these constraints that endangers proper cybersecurity of one's computing devices.

7. Techniques for Safe Preservation of Data

There are several techniques that can be undertaken by a user to ensure the safe preservation of one's data. One of them is through the creation of backup for essential data.

Backup of data is needed to ensure that recovery from threats like hardware failure or severe virus attack will not be difficult to achieve. In addition, users are advised to always observe best practices on protecting their devices from cyberattacks [5]. Online sessions should always be completely terminated when one is done with the Internet at every point in time to avoid bridges [10]. The infrastructure of every organization is designed to be protected with firewalls so that it can detect and prevent cyberattacks. Therefore, review on cybersecurity techniques need to be done frequently to ensure enhanced safety of data and infrastructure [3]. Cybersecurity framework as proposed by NIST are to identify, protect, detect, respond and recover from any form of incident as the case may be. Therefore, it is needful to always keep applications updated, secure files by having some backups, use strong passwords,

and logging out properly whenever a session is ended [13]. To protect the infrastructure, measures like storing securely, limiting physical access to equipment, sending reminders on what and when to update, and keeping stock of events needs to be taken seriously [13]. In similar fashion, [14] pinpoints some steps to cybersecurity to include – network security, malware protection, constant monitoring of the infrastructure, putting in place proper incident management, creating adequate awareness among users, and ensuring that only trusted removable media is used on the system. Using passwords on files is always advisable. This is because passworded files need authentication before it can be accessed. Data downloads have to be done with uttermost care to ensure that the source is genuine and safe. Firewalls must always be embedded in every system [6], [15].

Finally, the use of Virtual Private Network (VPN) makes your system to be hidden from every other person on the web thereby making your session protected from detection, tracking and monitoring. However, this weapon of VPN has a negative effect as it is also used by some advanced hackers to make it difficult for them to be detected and monitored. Originally, VPN technology was designed for governments and large organizations to use and protect their systems and infrastructures. This then implies that VPN has both positive and negative consequences. The positive consequences, is that it can be used to protect personal or organizational devices/networks from attacks while the negative consequence is that hackers use it to avoid detection and monitoring from authorized personnel [6], [16].

8. Remedies

It is important to have a good cybersecurity strategy in place for your computing devices. However, this does not mean that you are completely free from any form of cyberattack. Therefore, if eventually an attack happens, you need to have a means of remedying the situation. Some of the remedies that can be put in place are as follows –

- It is a myth to presume that once you have a password, you are totally immune from cyberattacks [6]. If you have your password compromised, the two-factor password can help you out in your quest to regain control of your app or system. If you did not have a two-factor authentication earlier, then it is a certain remedy that you need to put that in place to avert future occurrence.
- Confidentiality, a means of ensuring that data is made inaccessible to unauthorized persons, is key to data safety. If your device had been compromised, confidentiality of data can be enhanced by using a two-factor password, security tokens, and biometric verification [4].
- An organization can engage a cyber forensics expert to examine their systems and rectify any seen lapses to avert any future incident [1]. Cyber forensics deal with the investigation of digital data to get facts that can be used to prove a case in court, if need be.
- Companies infrastructure is often designed in such a way that peradventure the system is compromised, it can still be able to recover quickly from such attacks [3].
- Carelessness may have led to the compromising of the system. Therefore, individuals/organizations should ensure that cyber ethics and legislations are followed to the later by all and sundry at all times [9]. In addition, personal data processing should be guided by certain principles which include the consent of the owner before the disposal of one's data, as well as ensuring that the processing of one's personal data is always done in a confidential and safe manner [17].
- Training and retraining of users must be undertaken in order to avert future occurrences [6], [9], [11].
- Improved international cooperation can serve as a remedy towards averting future attacks. This can come in terms of harmonization of methods adopted by various states for fighting cybercrimes, and promotion of intelligence sharing [17].
- One should always avoid the use of public WIFI as well as downloading from unverified links/sources to avoid possible compromising of the system [18].

9. Methodology

The main instrument used in carrying out this research is the use of questionnaire. A total of nine (9) questions is drawn from the three (3) research questions earlier stated, and administered on seventy-eight (78) respondents. They were all tertiary institution students consisting of forty (40) that are dependents and thirty-eight (38) that are self-sponsored. The author will derive its assertions through the analysis of the responses obtained, and compare same to already existing findings by other authors on the same subject matter – Cybercrime. Table 1 shows the questions and their respective responses.

Sn.	Question	Yes	No	Uncertain
1.	Are you using any security software on your computing device(s)?	71 91%	7 9%	0 0%
2.	Are you satisfied with the protection it guarantees?	64 82%	8 10%	6 8%
3.	Do you have backups for your essential data?	37 47%	39 50%	02

				3%
4.	Do you normally terminate your online sessions once done?	31 40%	45 58%	2 2%
5.	Do you normally browse using a public network?	53 68%	21 27%	4 5%
6.	Have you ever fallen victim to any form of cyberattack?	75 96%	3 4%	0 0%
7.	Do you have a private VPN on your computing device?	8 10%	64 82%	6 8%
8.	What was the kind of security bridge you experienced?	Open-ended	Open-ended	Open-ended
9.	Which remedy did you apply to mitigate the bridge?	Open-ended	Open-ended	Open-ended

Table I: Questions and their respective responses.

8. Results and Discussion

This research paper is geared towards ascertaining the vulnerabilities of computing devices on the Internet and their possible solutions. The findings will be discussed based on the three (3) research questions posed to the respondents by the author. Research question one (1) seeks to ascertain the constraints that are posed on users in respect to cybersecurity. Questions one (1) to three (3) were framed to address this. Question 1 seeks to know whether the respondents are using any security software on their devices. The responses show that 71 out of the 78 respondents affirms to it while the remaining 7 says “no”. This implies that majority of the respondents are using one form of security software or the other on their devices. This is needed to secure their devices. Question 2 seeks to know whether the respondents are satisfied with the level of protection that their security software guarantees. In response, 64, 8, and 6 responded “yes”, “no”, and “uncertain” respectively. This shows that majority of the respondents are satisfied with the protection that their devices guarantees. This is not to say, however, that they are not aware that their devices can still be subjected to cyberattacks. In order to ensure that they remain safe, there is need for them to be guarded by cybersecurity ethics and legislations. This assertion is in line with the finding of [9] which says that people should ensure that cyber ethics and legislations are followed to the later. Similarly, [3] affirms that human errors can lead to the compromising of the system. Question 3 wishes to ascertain whether the respondents do have backups for their essential data. The responses show that only 37 do have backups whereas 39 do not have. This shows that more awareness is needed for people to understand the need to always have backups for their data, which is seen as good practice. This will ensure that they can easily recover from hardware failure or any form of virus attack. This assertion is in line with the finding of [5] which says that users should always observe best practices on protecting their devices from cyberattacks. Similarly, the assertion is in line with [14] which emphasises on the need of creating adequate awareness among users. Figure 1 shows the graphical representation of the responses obtained from the respondents in respect of research question 1.

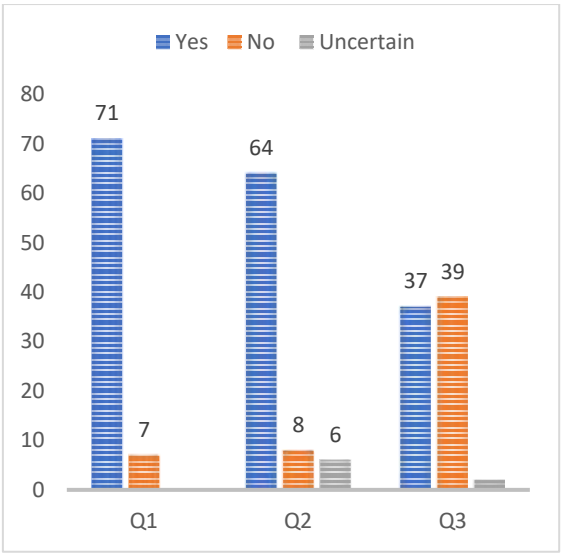

Fig. 1: Responses on the constraints to cybersecurity.

Questions 4 to 6 seeks to ascertain the effects of cybercrime on its victims. Question 4 wants to know whether they terminate their online sessions once done with browsing. In response, only 31 respondents do end their sessions completely while 45 say they do not. Majority of the respondents (58% to be precise) do not know that it is always advisable to terminate your online sessions when you are done browsing at each point in time. This will ensure that you are always protected. That is why most essential apps like banking apps terminates sessions automatically after a specific time frame of sluggish activity or outright inactivity. This assertion is in line with the findings of [10] and [13] which stipulate that online sessions should always be completely terminated when one is done online. Question 5 seeks to know whether they browse using a public network. In response, majority of them (53 to be precise) said "yes" while 21 and 4 of the respondents say "no" and "uncertain" respectively. This implies that majority of the respondents still use public networks, especially the students to browse. What people do not know is that it poses some dangers to the users because all the activities can be remotely monitored and controlled by the administer of such a public network. Also, cyberattack is very easy to be perpetuated in such cases. This assertion is line with the finding of [18] which says that one should always avoid using public WIFI in order not to warrant any possible compromising of one's device. Question 6 seeks to know whether they have fallen victim to any form of cyberattack. From the responses, a vast majority representing 96% of the respondents had at one point or the other fallen victim to cyberattacks. This means that cyberattacks are very rampant and often has a lasting effect on its victims. Cyberattack can be as a result of a fallout from the improper configuration of firewall, human error, lack of regular updates and opening of a phishing email/link. Generally, one must be guided against any form of negligence. This assertion is in line with the finding of [3] which holds that human errors can compromise the cybersecurity of any system. Similarly, [8] holds that negligence on the part of the user can lead to losses.

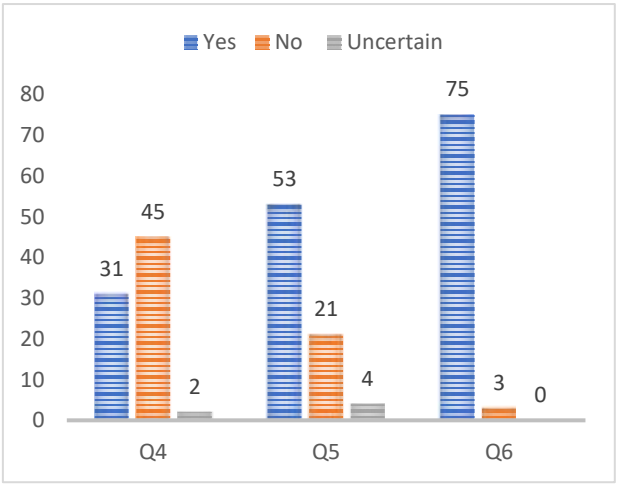

Fig. 2: Responses on the effects of cybersecurity on its victims.

Questions 7 to 9 seeks to verify the possible proactive measures as well as practical remedies that can be taken to guarantee a good level of safety while surfing the net. Question 7 seeks to know whether they are using a private VPN on their computing devices. the responses show that only a minority of the respondents do use a private VPN as 8, 64, and 6 respondents responded "yes", "no", and "uncertain" respectively. This shows that a vast majority (82%) of the respondents do not use a Virtual Private Network (VPN) on their devices. This is mostly because it often attracts extra costs. However, in some devices such as Apple devices, there is an app called Safari which is capable of shielding the user from trackers or hackers. The use of VPN guarantees your online sessions from being seen or monitored by anyone anywhere. This assertion is line with the findings of [6] and [16] which say that VPN makes your system hidden from every other person. Question 8 which seeks to know the kind of security bridges each of them had ever experienced

is an open-ended question. Analysing the responses, the most prevalent bridge has always been seeing embarrassing pop-ups that would not allow the user to do anything meaningful while browsing. Others stated the appearance of pop-ups requesting them to download an app that would protect their devices. Some others also stated that they experience bridges that often lead to their running apps closing abruptly while they are still not done.

Question 9 seeks to know the remedy they undertook in order to mitigate the bridge. Analysing the responses, many of the respondents say that they overcame the challenge by simply going to settings and reverting to factory settings of their devices. some others had to resort to overall scanning of the device to correct the errors. Also, some had to overhaul their apps and uninstalling any suspicious app in their device. Some others had to take their devices to specialised technicians to repair for a fee.

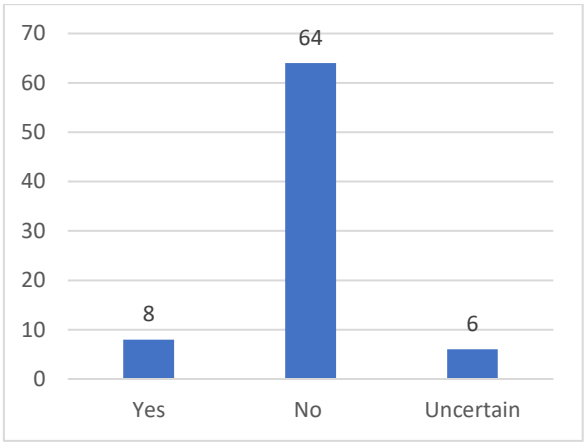

Fig. 3: Responses on the use of Virtual Private Network (VPN).

10. Conclusion

The use of the Internet has come to stay. Therefore, everyone has to embrace it and do all that needs to be done to surf the net safely. The findings of this study have shown that people use security software on their devices, and are satisfied with what it has to offer. Furthermore, the findings have shown that there is a disconnect on the level of awareness in respect of certain issues that the users need to know which happens to be in terms of the following -

a) Awareness on the need to often have backups for one's essential data;

b) Awareness on the need for one to always terminate one's internet sessions whenever one is done with the app;

c) Awareness on the need to avoid the use of public network, especially on transaction-related apps;

d) Awareness on the need to subscribe for a Virtual Private Network (VPN) if possible, to use on one's devices.

References

[1] Pande, J. (2017). *"Introduction to cyber security".* Haldwani: Uttarakhand Open University Available at: https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

[2] Baylon, C. (2014). "*Challenges at the intersection of cyber security and space security : Country and International Institutions Perspectives.* London: The Royal Institute of International Affairs, Charthan House.

[3] Callejas, J. F., et al. (2021). "*Cybersecurity in the United Nations System Organizations".* Report of the Joint Inspection Unit of the United Nations.

[4] Malla Reddy College (2021). *"Digital notes on cyber security (R18A0521)",* A lecture note from the Department of Information Technology, Malta Reddy College of Engineering & Technology, India.

[5] Kelley, K. (2023). "*What is cybersecurity and why it is important?".* Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

[6] Kelley, K. (2023). *"What is cybersecurity and why it is important".* Last updated October 25, 2023. Simplilearn Solutions.

[7] ThoughLab (2023). *"Cybersecurity solutions for a riskier world".* Available at: https://thoughtlabgroup.com/cyber-solutions-riskier-world/

[8] NIST (2023). "*Users are not stupid: Six cyber security pitfalls overturned".* Available at: https://csiac.org/wp-content/uploads/2022/06/New-Users-Are-Not-Stupid_FINAL.pdf

[9] Ebelogu, C. U., et al. (2019). *"Cybercrime, its adherent negative effects on Nigerian youths and the society at large: Positive solutions". In International Journal of Advances in Scientific Research and Engineering (1), vol. 5 (12), December, 2019.*

[10] Ebelogu, C. U., Ojo, D. S. et al. (2019). *"Cybercrime, its adherent negative effects on Nigerian youths and the society at large: Possible solutions"* In International Journal of Advances in Scientific Research and Engineering (IJASERT), volume 5, issue 12, December 2019, pp. 155 – 164.

[11] Onodugo, I. C. & Itodo, S. M. (2016). *"Cyber crime and Nigerian business environment"* In National Journal of Advanced Research, volume 2, issue 2, March 2016, pp. 28 – 38.

[12] Gillis, A. S. & Pratt, M. K. (2023). *"Cyber attack".* Available at: https://www.techtarget.com/searchsecurity/definition/cyber-attack

[13] Federal Trade Commission, et al. (2021). "*Cybersecurity for small businesses: Cybersecurity basics."* A 24-page documentation from Federal Trade Commission. Available at: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/basics.

[14] Saraswat, V. K. (2018). "*Cyber Security".* Available at https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

[15] Kabilan, S. (2023). "*Overview of cyber security and its safety measures",* International Journal of Humanities & Social Science Studies, Vol. 12 Issue 1, No. 20, January – June 2023, pp.162 – 166.

[16] Mujovie, V. (2018). *"Where does cybercrime cone from? The origin and evolution of cybercrime".* Available at: https://www.le-vpn.com/history-cyber-crime-origin-evolution/

[17] African Union (2014). "*African Union convention on cyber security and personal data protection".* Adopted by the twenty-third ordinary session of the Assembly, held in Malabo, Equatorial Guinea, 27th June 2014.

[18] Zope, A. P. & Chaudhari, R. R. (2022). *"A review paper on cyber security".* In International Journal of Engineering & Technology (IRJET), Volume 09, Issue 08, August 2022, pp. 1561- 1566.