International Journal of Research Publication and Reviews

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

The Heightening Effect of Social Media on Cybersecurity

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.5.0524.1401

ABSTRACT

The ease with which the social media, be it TikTok, Facebook, X, or any other, is accessible today on the cyberspace has led to many falling prey to one sort of exploitation or the other; thereby weakening cybersecurity. This study is undertaken by the author to access the heightening effect of social media on cybersecurity. The objectives of the study are as follows – to find out the appropriate ways of using the social media; the dangers associated with inappropriate usage of the social media; and to ascertain the practical ways through which one can avert cyberattacks. The methodology adopted is the use of questionnaire which is administered on the respondents to ascertain their responses to the nine (9) questions posed to them. The findings of this paper show that the proliferation of the ownership of internet-enabled devices, of which almost all of them operates an active social media account has a significant influence to the rising surge in cyberattacks.

Keywords: *Cyberattacks, Cybersecurity, Cyberspace, Internet-Enabled Devices, Social Media.*

1. Introduction

Globally, social media usage is agog as it cuts across all ages, culture and tribes. The cyberspace provides us with a viable platform to communicate across the globe. The ever-growing digitization of every facets of our lives, no doubt is of immense benefit to humanity. However, vulnerable devices used for surfing the social media has led to many becoming victims to cyberattacks in one way or the other.

Historically, breaches on people's records were seen to have attained an alarming rate of over 3.2 million in just ten (10) incidents between the months of January to June 2020 [1]. In November 2016, over £2.5m was lost by Tesco to cybercriminals that withdrew monies from the company's bank accounts. Despite the loss, Tesco was still fined to the tune of £16.4 million as damages for the compromising of the accounts of over 40,000 customers. UK's National Health Service (NHS) suffered a setback in May 2017 due to cyberattack that prevented the over 40 NHS service providers to attend to their patients. The attack was easily perpetuated due to the fact that the software was outdated [2]. All these negative impacts cannot be unconnected to the proliferation of users on social media platforms where many of them go as far as ignorantly divulging some sensitive information on themselves in the name of personal aggrandizement. This portrays a serious danger on our contemporary society.

To this effect, this paper intends to overview the heightening effect of social media on cybersecurity.

2. Problem Definition

Social media account openings are on the rise these days with little or no adequate check in place to regulate its activities. This lends to the increase in cyberattacks over the years as the social media is exploited by mischievous persons to extract some vital information about their targets. This study is undertaken to lend a voice geared towards suppressing the threats that social media is posing on the society.

3. Objectives of the Study

This study intends to –

1. Find out the appropriate ways of using the social media.
2. Find out the dangers one can face due to the inappropriate usage of the social media.
3. Ascertain the practical ways through which one can avert cyberattacks.

4. Research Questions

The research questions advanced for this study are as follows -

1. What are the appropriate ways of using the social media?
2. What are the dangers one can face due to the inappropriate usage of the social media?
3. What are the practical ways through which one can avert cyberattacks?

5. Literature Survey

Information is the key driver towards the attainment of one's goals and objectives – be it positive or negative. To ensure, the safety of information, the user has to be mindful of the following while using the social media – information security, operational security, disaster recovery and business continuity, and end-user education [3]. Information security refers to the protection of the "integrity and privacy of data, both in storage and in transmit". Operational security entails "the processes and decisions for handling and protecting data assets". Disaster recovery and business continuity entails the organization's ability to respond to any form of cybersecurity bridge that would lead to data loss during operations. Finally, the end-user stands for the persons that use the system because one can accidentally infect a supposed safe system through careless actions like opening links or downloading unverified data/app [3].

The cyberspace of an individual or cooperate entity can be compromised through one of these broad ways – the hardware/software vulnerability, phishing email, or carefree practices like using outdated software security kits [4]. Cyberattacks can happen through a number of ways. Foremost of these is through malware, which is a malicious software that is designed to break into a system. [5] defines malware as a form of attack that gains entrance into your device through surfing the net or downloads from unsafe sources. Malwares are categorized into two – adware and spyware. Adware refers to the pop-up adverts that normally happen when you visit certain webpages. Some could be safe while some others are not. Spyware refers to such that invades the system to steal viable information from its victim's computing device [5], [6], [7]. Another category of malware can come as a freeware offering. Freeware refers to applications that are offered to interested users free of charge. Sometimes, these applications can have spyware attached to it which eventually invades the victim's device. Spamming refers to the bulk sending of unsolicited messages to people's emails [6]. Furthermore, [8] talks about another form of malware known as ransomware. A ransomware is a type of malware which infects a device or devices by shutting it down until a ransom is paid. Denial of Service (DOS) attack is yet another form of cyberattack. It is a type of attack that prevents authorized users from gaining access to a website or even other systems [5]. An advanced DOS is the Distributed Denial of Service (DDOS) attacks. DDOS attacks occur when a network is gammed against itself thereby resulting to the inability of users accessing the network for service [8], [9]. Botnets are used to describe a collection of computing devices that has been compromised by a certain hacker. All such compromised devices will then be acting as "zombies" as they will be remotely controlled by the hacker [5], [9].

Other ways in which our devices can be compromised include – scareware, links, phishing, cyberstalking and skimmers. Scareware refers to a deceptive security warning that is geared towards deceiving the Internet user into downloading a fake security software. This, the victim will do thinking that the system is infected and needs such a software to supposedly safeguard his device [5]. Links are also used as an attack tool. The social media user may be deceived to open a link for a download or video which eventually compromises the device being used [5]. Phishing is an act of sending an email that is assumed to be coming from a viable source, such as a bank. When the victim opens the link or response to their request, the account is hacked/compromised [5], [9]. Cyberstalking refers to the type of attack in which the criminal sends lots of degrading emails/messages to its victim mostly to frighten the person into giving in to his demands. On the other hand, skimmers refer to criminals that steal information on people's credit cards using some techniques. Afterwards, such stolen information is used to make purchases in disguise of the original person/persons [9].

6. Practical Ways of Avoiding Cyberattacks

Avoiding cyberattacks is the main purpose of having robust cybersecurity measures in place while surfing the net. To avoid cyberattacks, the social media user needs to apply certain strategies such as data minimization, access control, encryption, regular audits, and training. Data minimization entails that personal data should not be deployed in full. Rather only basic information should be displayed. Access should be restricted to authorized persons [10]. Furthermore, observing some basic rules can guarantee the cybersecurity of your device. These rules include –

- Implementation of robust firewalls deemed to block suspicious domain sites and the attackers;
- Verifying every trial of accessing the organization's website to ensure the user is with best intentions;
- Configuring the system with best settings that would guarantee a high level of safety;
- Launching a program in the system that would trigger alerts when a malicious activity is detected;
- Safeguarding the system against malwares using appropriate antivirus kits; and
- Enlightening the users on safety methods [7].

On the other hand, [11] highlights that one must be cautious while surfing the net by taking the following precautions –

- Ensuring that one’s operating system and antivirus kits are always up-to-date;
- Using a strong password, and not sharing such;
- Apply two-steps verification;
- Avoiding public Wifi; and
- Avoiding opening unverified links as well as carrying out unsafe downloads.

Similarly, [6] holds same view on the use of password. Passwords usage must be strong, and a two-step verification can be added to safeguard our apps. It is also advisable to use a password manager installed in your device which will serve as a backup for the effective management of all your passwords.

7. Methodology

The main instrument used in carrying out this research is a questionnaire consisting of nine (9) questions that were administered on a total of eighty-seven (87) students of a tertiary institution. Out of this number, forty-seven (47) and forty (40) were sponsored by their parents and self-sponsored respectively. The author will derive its findings through the analysis of the responses obtained, and compare same to already existing findings by other authors on the subject matter – Cybersecurity. Table 1 shows the nine (9) questions and their responses to each of the questions.

Sn	Question	Yes	No	Uncertain
1.	Do you have an internet-enabled mobile phone?	80 92%	7 8%	0 0%
2.	Do you have a social media (e.g. Facebook) account?	78 90%	2 2%	7 8%
3.	Do you frequently access your social media account?	71 82%	9 10%	7 8%
3b	For what purpose do you normally access your social media account?	Open-ended	Open-ended	Open-ended
4.	Have you ever fallen victim to cybercrime while using the social media?	58 67%	20 23%	9 10%
5.	Have you ever opened a link on your social media account?	71 82%	9 10%	7 8%
6.	Has your social media account ever being hacked?	17 20%	61 70%	9 10%
7.	Are you using a strong password on your social media account?	7 8%	69 79%	11 13%
8.	Do you always ensure the safety of every link before opening it?	5 6%	70 80%	12 14%
9.	Do you normally log out from your account completely after each usage?	11 13%	67 77%	9 10%

Table I: Questions and their respective responses.

8. Results and Discussion

This research paper is geared towards ascertaining the heightening effect of the use of social media on cybersecurity. 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 level of appropriateness of the social media usage by the respondents.

Questions one (1) to three (3) were framed to address the first research question. The first question seeks to know whether they have an internet-enabled mobile device of which 80 out of the total of 87 respondents do have internet-enabled devices. This assertion shows that too many people are now using the Internet because of the proliferation of cheap mobile devices**.**

Question two (2) seeks to verify the number of the respondents that has an active social media account on their devices. The findings show that a vast majority do have a social media account on their phone because only two (2) respondents say that they do not have. This goes to proof that social media usage is very vast in our contemporary society.

Question three (3) seeks to know the extent that they are frequently using the social media for interaction. The responses show that seventy-one (71) respondents as against nine (9) responded "yes" and "no" respectively. Question 3b, which seeks to know what exactly they do while online on any social media platform, shows that majority of them use the social media for entertainment and as a way of whiling away time for fun and leisure. Only very few uses the social media for the sourcing of vital information. This shows that majority, especially our youths spend their valuable time on social media chatting as well as acting a clip and watching other peoples' clips. Figure 1 shows the bar chart representation of the responses received with regards to research question 1.

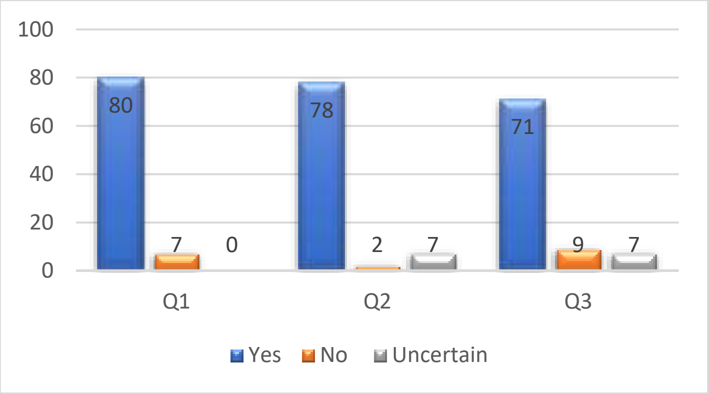

Fig. 1: Responses on the appropriate ways of using the social media

Questions 4 to 6 seeks to answer the research question 2 which wants to find out the possible dangers users of the social media could face due to its inappropriate usage.

Question 4 seeks to ascertain the number of the respondents that has ever fallen victim to cybercrime while using the social media. The responses show that 58 and 20 said "yes" and "no" respectively. This is so because the cybercriminals spread their tentacles targeting vulnerable devices to spy and see what they can get from their targets for their unjust course**.** When they see what they need in some devices, they can go ahead to hack it. This assertion is in line with the findings of [5] when it says that compromised devices are turned to "zombies" by the hacker. In other words, devices that do not have the vital information they need are left out.

Question 5 seeks to know whether they have ever opened a link in the course of their using the social media. The responses show that 71, 9 and 7 of the respondents responded "yes", "no", and "uncertain" respectively. This then follows that majority do open links indiscriminately while on social media. This action can make them to be easy targets for the cybercriminals. This assertion is in line with the findings of [5] and [9] when they say that an account can be hacked when a victim opens an unverifiable link. In like manner, [11] encourages users to avoid opening links as well as carrying out unsafe downloads to avoid fallen victim to cyberattacks.

Finally, question 6 seeks to know whether any of them has ever had his social media account hacked. The responses show that 17 of them have had their accounts hacked in the past while a vast majority of 61 respondents has never had the experience. This goes to show that they only target people that they are sure can fetch them high illicit profits. This is so because the main essence of the hackers is to defraud their unsuspecting victims. This assertion is in line with the findings of [5], [6], and [7] when they say that hackers invade their victims' computing devices to steal vital information (that would advance their nefarious activities). Figure 2 shows the bar chart representation of the responses obtained in respect of research question 2.

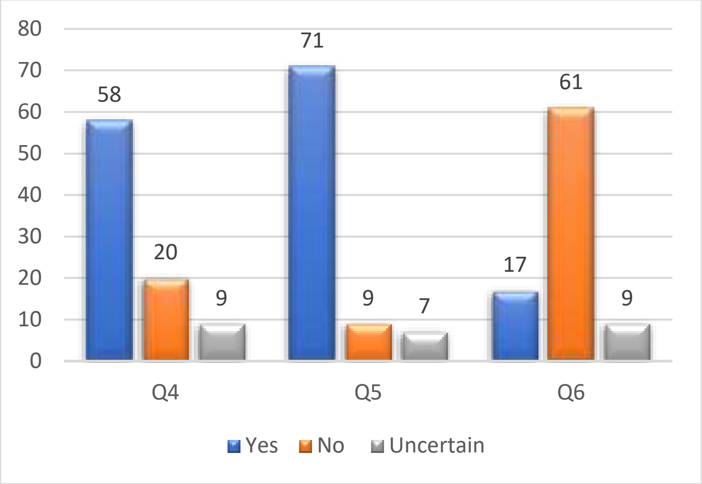

Fig. 2: Responses on the dangers of social media inappropriate usage.

Questions 7 to 9 are designed to ascertain the practical ways through which one can avert cyberattacks. Question 7 seeks to know whether they are using a strong password. Only seven (7) of the respondents agrees that they are using a strong password whereas a vast majority (69 to be precise) said that they are not using a strong password. This goes to show that people are not really aware of the need for them to always use strong passwords. Some social media platforms like Facebook, unlike other key apps, do not necessarily force you to use a strong password. This makes your account vulnerable to possible cyberattack or hacking.

Question 8 seeks to ascertain whether they ensure the safety of every link they open while interacting in the social media. Shockingly, only five (5) of the respondents say they do while a vast majority of 70 respondents do not watch out for any safety feature before opening any link on the social media. This discovery shows that many people are ignorant of the fact that they need to ensure the safety of every link before venturing to open it. This assertion is in line with the finding of [3] which says that a device can be accidentally infected through careless opening of links or unverified downloads. Furthermore, [5] affirms that links can be used as an attack tool.

Question 9 wishes to ascertain whether they normally log out completely each time they are done with their social media account. In response, only 11 of the respondents do log out while 67 respondents said that they don't. This points to the fact that most users are not enlightened on the need to completely log out their sessions when done for the safety of their devices. Therefore, enlightening the users on safety methods of surfing the net is key to a safer usage of the social media. This assertion is in line with the finding of [7] when it emphasises on the need of enlightening the users on safety methods of surfing the net. Figure 3 shows the bar chart representation of the respondents' responses in respect of research question 3.

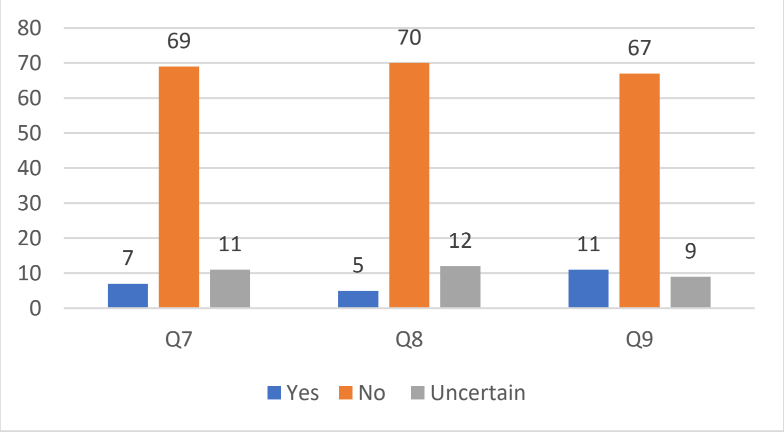

Fig. 3: Responses on the practical ways of averting cyberattack.

9. Conclusion

The social media is increasingly becoming popular by the day. The findings of this study have shown that the following aided the increase in cyberattacks –

a) the proliferation of internet-enabled devices;

b) the increasingly huge amount of people with social media accounts;

c) the inappropriate usage of the social media such as indiscriminate opening of links; and

d) the lack of adequate enlightenment on safe browsing techniques such as completely ending one's online sessions.

10. Recommendation

The social media being a vital tool for socialization has to be used viably and responsively. The author advices that all social media users should embrace safe browsing techniques to safeguard their devices from cyberattacks. Based on this paper findings, the author recommends the following –

a) Every social media account should be operated using a strong password;

b) Links opening and downloads should be done responsively; and

c) Whenever one is done with one's social media account, it is advisable to always log out.

References

[1] Udacity (2022). *"Introduction to cyber security".* Available at: https://d20vrrgs8k4bvw.cloudfront.net/documents/en-US/Intro+to+Cybersecurity+Nanodegree+Program+Syllabus.pdf

[2] Morgan, L. (2018). "*The importance of cyber security"* Available at: https://www.cpaireland.ie/CPAIreland/media/Education-Training/Study%20Support%20Resources/2019%20Articles/P2-AP-The-Importance-of-Cyber-Security.pdf

[3] Kaspersky Lab. (2023). "*What is cyber security?".* Available at https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[4] NCC (2017). *"Effects of cybercrime on foreign direct investment and national development".* A 100pp final report from the NCC Department of New Media and Information Security. Consultant: Newark Security Systems Ltd.

[5] Kingsborough.edu (2023). *"Why cyber security is important".* Available at: https://www.kingsborough.edu/its/data_computer_security/documents/why_cyber_security_is_important.pdf

[6] 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

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

[8] Brush, K. & Cobb, M. (2024). "*Cybercrime".* Available at: https://www.techtarget.com/searchsecurity/definition/cybercrime

[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] Bhushan, B. (2023). *"The growing importance of cyber security in the digital age". In* International Journal for Innovative Research in Multidisciplinary Fields, Volume 9, Issue 5, May 2023.

[11] Zope, A. P. & Chaudhari, R. R. (2022). *"A review paper on cyber security".* In International Journal of Engineering & Technology (IRJET), Volume 09, Issue 8, August 2022, pp. 1561- 1566.