MBJLIS – Middlebelt Journal of Library and Information Science, Vol. 21, 2023
ISSN: 1596 - 1595
Journal homepage: https://www.mbjlisonline.org/

PRESENCE ON SOCIAL NETWORKING SITES AND SOCIAL ENGINEERING ATTACK AMONG STUDENTS OF TWO SELECTED TERTIARY INSTITUTION IN ADAMAWA STATE

SUGABSEN MARTINS
Assistant Librarian,
American University of Nigeria Library
sugabsen.martins@aun.edu.ng
07038015309

Submitted: 03/08/2023 ***Accepted: 04/10/2023*** ***Published: 08/11/2023***

ABSTRACT

There has been steady increase of the incidences of cyber-attacks in tertiary institutions in the last decade. These incidences are in diverse forms and focuses on students of the tertiary institutions. Students complaint of their phones and laptops being hacked. This study sought to find out how frequent undergraduate students make posts and how that relates to cyber-attack on social media at the Federal College of Education and the American University of Nigeria. The study area has a population of 3756. The study used deductive, quantitative research; therefore, hypothesis was made and tested using the Pearson's Product Moment Correlation (PPMC) in the Statistical Package for Social Sciences (SPSS). The philosophical underpinning adopted in the study was the positivist paradigm. A structured questionnaire was employed as an instrument for data collection, and using a simple random sampling method, was distributed to students. The study focused on Facebook. The research selected 0.05 as the level of significance. It was found that there is a strong correlation between a cyber-attack and frequent activeness on social media. It found that there is a strong correlation between cyber-attack and frequenting the social media but there is no significant evidence to conclude same on the population. It suggested that further research be carried out using a qualitative research approaches so that respondents may be observed through interview.

Introduction

Cyber security breaches have caused a great deal of anxiety among cyber and information security specialists. In the last decade there has been increase of assault on tertiary institutions and this has caused worry and concern to tertiary institution administrators. Thomas, (2018) argued that researchers have spent a lot of time and money looking into possible solutions to the issue, yet it still exists and is becoming worse. People are increasingly using smart phones to connect to the internet and utilize their favorite Social Networking Sites (SNS) or applications to interact with others and share material in new ways. It is worth remembering, though, that hundreds of thousands of individuals are unknowingly cyber-attack victims.

MBJLIS – Middlebelt Journal of Library and Information Science, Vol. 21, 2023
ISSN: 1596 - 1595
Journal homepage: https://www.mbjlisonline.org/

Quinlan (2020) argued that cyber fraudsters stole an estimated $5 billion utilizing Social Engineering (SE) tactics between 2013 and 2016. This constitutes a huge problem that needs thorough enquiry. The human aspect of computer security is critical and warrants additional exploration to secure persons and organizations. According to Sekhar (2021), a company's technological vulnerability is not the sole reason for a cyber-attack, in the cyber security chain; the human person is the most susceptible. As a result, students at tertiary institutions are vulnerable. Researchers have invested large resources exploring various approaches to alleviate the issue of social engineering assault, yet the problem still exists and is becoming more severe (Thomas, 2018). The frequency of this issue is disturbing, necessitating more investigation.

The nature of the problem is of great magnitude. According to Alsulami et al. (2021), social engineering assaults may cost businesses more than $100,000 in each occurrence. The most crucial part of effective social engineering assaults, according to Krombholz et al. (2015), is social methods. The study aimed at adding to the discourse on students' vulnerability to social engineering assaults on social media was based on gaps identified in the literature. While many studies have shown some of the cyber security threats that users face on social networking sites, they have been neglected to concentrate on students' social media practices that make them vulnerable to social media cyber security assaults. Yasin, Fatima, Liu, Yasin, and Wang (2018), De Bona and Paci (2020), and Zolotarev et al. (n.d.) for example, the study focused on persuasive strategies used in cyber-attacks on social media, but it did not examine consumption behaviors. Regarding social media use, the majority of study on social networking sites and cyber security has focused on persons or groups but the majority of study has not focused on students, who are a critical component of an educational institutions' information security.

Klimburg-Witje and Wentland (2021), Thomas (2018), Li et al. (2019) focused their research on social engineering attacks against employees that occur during their working hours and while using a company's or institution's IT infrastructure. They did not pay attention to students' personal time when they use the institution's IT infrastructure remotely. Significant studies regarding social engineering and tertiary institutions on social media focused largely on awareness, vulnerability, and impact on the institutions but not on usage habits of students. For example, Ulven and Wangen(2021), De Bona and Paci (2020), Nagahawatta et al. (2020) Al-Janabi and Al-Shourbaji (2016), focused their research on the awareness, vulnerability, and impact of social engineering attacks on universities. They did not pay attention to the social media usage habit of students. Therefore, the research will fill in the gap that exists.

The purpose of this study was to see if students at higher institutions in Jimeta and Yola metropolis who are frequently active on social networking sites were vulnerable to social engineering attacks. Two campuses were investigated to achieve this. The American University of Nigeria, and the Federal College of Education, Yola.

Review of Related Literature

Alharbi and Tassaddiq (2021) used a scientific questionnaire based on many safeties online to explore and assess the degree of cyber security knowledge and user compliance among undergraduate students at Majmaah University, Saudi Arabia. To assess and examine their

MBJLIS – Middlebelt Journal of Library and Information Science, Vol. 21, 2023
ISSN: 1596 - 1595
Journal homepage: https://www.mbjlisonline.org/

hypotheses, they employed quantitative research techniques to perform ANOVA, Kaiser–Meyer–Olkin (KMO), and Bartlett's tests. The study found that 22% of the respondents were unfamiliar with two-factor authentication and hence did not understand how it provided a layer of protection. Again, 75% of them checked their email from a public Wi-Fi network without utilizing a Virtual Private Network (VPN) or trying to encrypt the connection. The study did not focus on the frequency of use of Internet.

Alsulami et al. (2021) conducted another study on assessing the amount of social engineering awareness in the educational sector in Saudi Arabia, to provide a measurement of social engineering awareness in the Saudi educational sector. They conducted a quantitative survey and evaluated the results using the SPSS. Teachers and instructors, students, workers, and others were included in the sample. The findings revealed substantial disparities in security behaviors and abilities between individuals who had previous knowledge of social engineering and those who did not. According to the findings, 66% of the people polled had no idea what social engineering was. However, because that the survey encompassed people from various walks of life, it lacked focus and attention on students.

When social engineers strike, they do not attack at random; instead, they choose their targets meticulously. Some social engineers, according to a recent study, prefer to target the educational sector and higher institutions. In their research on assessing awareness of social engineering attacks in the educational sector in the Kingdom of Saudi Arabia, Alharbi and Tassaddiq (2021) discovered that most academic institutions do not incorporate active cyber security awareness and training programs in their strategic plans. As a result, social engineers profit from the scenario. This finding was similar to that of Alsulami et al (2021). Also, Al-Janabi and Al-Shourbaji, (2016) suggested that the availability of technology and sophisticated computing environments, especially in educational settings, opens the door to security risks from cybercriminals and hackers looking to exploit flaws in their systems.

Even though the research looked at the educational environment, it did not focus on students. Bhatnagar and Pry (2020) looked into students' views of personal social media hazards as well as their understanding of how to use privacy and security settings in social media applications. They conducted a survey of 107 students on the campus of a Clariont university in western Pennsylvania. Their research goals were to analyze student perceptions of social media privacy, determine if security is important to college students, and determine whether colleges should provide improved cyber-security instruction. Their findings demonstrate that while students are aware of the privacy and security dangers associated with social networking sites, they still require further training in this area. This finding coincided with that of Alharbi and Tassaddiq (2021). The study was limited only to Pennsylvania.

Methodology

The research followed a scientific (Positivist) paradigm. This is because the positivist paradigm is a logical approach to research that result in the scientific validation of the study hypothesis. Again, this is quantitative research in which data is gathered through a questionnaire and turned into quantifiable numbers and quantities. This study corresponds with positivism,

MBJLIS – Middlebelt Journal of Library and Information Science, Vol. 21, 2023
ISSN: 1596 - 1595
Journal homepage: https://www.mbjlisonline.org/

which holds that hypotheses are the natural approach to producing and confirming scientific knowledge. For the examination of the acquired data, Pearson's product-moment correlation coefficient (PPMCC) at a 0.05 level of significance was used to determine the strength of relationship between two variables. Quantitative research design was adopted for the study. The study area has a population of 3756 (Adamawa State Ministry of Education, 2022). Based on Krejcie and Morgan sampling technique, a sample size of 120 was drawn at 95 percent confidence level and +5% estimate error. Data for the study was collected using a questionnaire and simple random sampling method was used. Each question item was tallied against the 5-point Likert scale. Cronbach's Alpha was used to examine the reliability of the research instrument. The institutions involved for the research are the Federal College of Education (FCE) Yola, and the American University of Nigeria (AUN) Yola.

Data Analysis and Results

Data collected was analyzed using Pearson's Product Moment Correlation (PPMC) in the Statistical Package for Social Sciences (SPSS). There was 93.6% return rate of the distributed questionnaire.

Table 1: Frequency of Respondents' Publishing on Facebook

S/No	Item	Not at All	Less Frequent	Frequent	Highly Frequent	Very Highly Frequent
1.	Asking questions on Facebook	30(9.1%)	135 (40.9%)	66(20%)	63 (19.1%)	36(10.9%)
2.	Click on links posted by others on Facebook?	24(7.3%)	144 (43.6%)	78 (23.6%)	48 (14.5%)	36(10.9%)
3.	Chatting with unknown people	42 (12.7%)	153 (46.4%)	81 (24.4%)	27(8.2%)	27(8.2%)
4.	Sharing personal information with strangers on Facebook	108(32.7%)	117(35.5%)	3(0.9%)	48(14.5%)	54(16.4%)
5.	Commenting freely on topics of discussion on Facebook	27 (8.2%)	96 (29.1%)	33 (10.0%)	117 (35.5%)	57(17.3%)
6.	Expressing opinion on friends' posts on Facebook	18 (5.5%)	72(21.8)	54 (16.4%)	78 (23.6%)	108(32.7%)
7.	Posting favorite activities like vocation, outings, occasions, on Facebook	45 (13.6%)	96(29.1%)	54 (16.4%)	87 (26.4%)	48(14.5%)
8.	Posting on Facebook, pictures snapped at places traveled to	66(20%)	93(28.2%)	36 (10.9%)	75 (22.7%)	60(18.2%)
9.	Posting of accomplishments on Facebook	108 (32.7%)	135 (40.9%)	27 (8.2%)	30(9.1%)	30(9.1%)

MBJLIS – Middlebelt Journal of Library and Information Science, Vol. 21, 2023
ISSN: 1596 - 1595
Journal homepage: https://www.mbjlisonline.org/

The above table shows the frequency of publishing on Facebook by the respondents. The result holds that 30% of the respondents do not post questions while 10.9% very highly frequently click on posted links by others. More so, 24.4% of them indicated that they frequently chat with people they don't know. Likewise, 32.7% admitted that they have never shared personal information with strangers. Frequently commenting views freely on topics of discussion on Facebook was testified by 35.5%. Also, 32.7% of them comments on their friends' posts very highly frequently. Again, the percentage of who publish favorite activities like vocation, outings, occasions, etc. frequently stood at 26.4%. Furthermore, 22.7% posted pictures snapped at the place travel to. Again, 8.2% account for the number of those who post their accomplishments frequently.

Ho_1: *Frequency of activeness on social media makes students potential targets.*

Table 2: Regression Coefficient on Frequent Activeness and Attack on Social Media

		I have been attacked before on social media	I do share my accomplishments on social media.
I have been attacked before on social media	Pearson Correlation	1	-.092
	Sig. (2-tailed)		.095
	N	330	330
I do share my accomplishments on social media.	Pearson Correlation	-.092	1
	Sig. (2-tailed)	.095	
	N	330	330

From the table, the result of the test hypothesis shows a strong negative relationship between sharing personal preferences and attacks on social networking sites with a value of -0.092. Again, the p-value is 0.095 which is greater than the alpha value (0.05). This implies that the researcher has failed to reject the hypothesis that the frequency with which students are active on social media makes them potential targets.

Discussion of the Findings

This study was meant to find whether frequency of students on social media can lead to them becoming cyber-attack victims. Key findings from this study demonstrate a strong correlation between cyber-attacks on social media and posting personal achievements frequently. This might be due to the fact that tertiary educational institutions house a body of research documents that a hacker might be interested in. This reiterates the findings of Al-Janabi and Al-Shourbaji (2016) who found that availability of technology and sophisticated computing environments, especially in educational settings, opens the door to security risks from cybercriminals and hackers looking to exploit flaws in their systems.

Again, it also found a strong correlation between security breach and frequent activeness on social media. Students in tertiary institutions can be target of hackers because their attention can be drawn to the social life students portray on social networking sites. This research adds to the theoretical understanding of how habitual social media engagement exposes students to social

MBJLIS – Middlebelt Journal of Library and Information Science, Vol. 21, 2023
ISSN: 1596 - 1595
Journal homepage: https://www.mbjlisonline.org/

engineering attacks. The researcher has failed to reject the null hypotheses therefore the hypotheses holds true that frequent activeness on social media makes students potential targets. This might be because of the nature of activity one engages in such as by making posts that portrays certain lifestyles while on social media.

Conclusion

Based on the findings, it is safe to conclude that frequent activeness on social media can lead to cyber assault, implying that it is safe to minimize frequency and prolonged usage of the social media. It appears that a more in-depth interaction with respondents would have revealed hidden subtleties about regular social media activity, as well as how these factors may contribute to being susceptible to social engineering attacks.

Recommendations

Based on the findings, it is hereby recommended that:

i. It is recommended that a more in-depth study of the respondents should be carried out to revealed hidden subtleties about lifestyle exposure and regular social media activity, as well as how these factors may contribute to being susceptible to social engineering attacks.
ii. future research should focus more on using qualitative research to monitor respondents via interviews.

REFERENCES

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management, 15*(1), 7- -13 DOI: 10.1142/S0219649216500076

Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., Alotaibi, K. G., & Alharthi, S. S. (2021). Measuring awareness of social engineering in the educational sector in the kingdom of Saudi Arabia. *Information*, *12*(5), 208 -217.

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information System Educational Journal,18*(1), 48–58.

De Bona, M., & Paci, F. (2020). A real world study on employees' susceptibility to phishing attacks. *Proceedings of the 15th International Conference on Availability, Reliability and Security*, *1*(4) 1–10.

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? social engineering and the construction of the "deficient user" in cybersecurity discourses. *Science, Technology, & Human Values*,*46*(6) 016224392199284.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122.

Quinlan, L. (2020). A solution for human vulnerabilities to Social Engineering attacks: The Social Engineering defence model. https://doi.org/10.13140/RG.2.2.35328.66562

MBJLIS – Middlebelt Journal of Library and Information Science, Vol. 21, 2023
ISSN: 1596 - 1595
Journal homepage: https://www.mbjlisonline.org/

Sekhar, B. C. (2021). Systematic review on social engineering: Hacking by manipulating humans. *Journal of Information Security*, *12*, 104-114. doi: 10.4236jis.2021. 121005.

Thomas, J. E. (2018). Individual cyber security: empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management,12*(3), 1-23. doi:10.5539/ijbm.v13n6p1

Ulven, J. B., & Wangen, G. (2021). A systematic review of cyber security risks in higher education. *Future Internet*, *13*(2), 39 - 50. https://doi.org/10.3390/fi13020039

Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. *Security and Privacy*,*2*(4), 12-23

Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., & Wei, Z. (2021a). Understanding and deciphering of social engineering attack scenarios. *Security and Privacy*, *4*(4), 1–17.

AUTHOR'S PROFILE

Mr. Sugabsen Martins works as team lead for cataloging unit at the American University of Nigeria (AUN) where he coordinates the organization of information resources for researchers and students alike. Prior to becoming a team lead, he was a cataloger at the same institution. He has seven years of experience in the Library and Information Science profession. He believes in learning and helping students to learn. He specializes in cataloging using Library Management Systems (KOHA) and Digital Institutional Repositories (DIR). He holds a Bachelor of Technology from the Abubakar Tafawa Balewa University Bauchi and a Master of Science degree from the National Open University of Nigeria. He is a Certified Librarian of Nigeria (CLN) and a member of Nigerian Library Association (NLA). His personal and professional goal is to make learning easier for students. Sugabsen Martins has had the privilege to attend many workshops, and training in the field of information organization and retrieval. He loves to read and teach.