



Cyber Security Education and Awareness

Aliyu A. Muhammad Zabi

Federal Polytechnic Kaltungo/Department of Computer Science, Gombe,770109, Nigeria.

aliyuzabi@federalpolyilaro.edu.ng

Adamu B. Abdullahi Adams and Abdulrahman C. Yakubu

Abubakar Tafawa Balewa University/Department of Computer Science, Bauchi, 740272, Nigeria

Email: {adamuabdullahiadams, abdulrahmanyakubu}@federalpolyilaro.edu.ng

Abstract: *This study aimed to investigate the level of students' awareness of cybersecurity and cyber security education in Nigerian Polytechnics. The survey objective was to assess the extent to which students in this developing country are adequately educated about cyber security, aware of cyberattacks, and knowledgeable in mitigating these attacks. Additionally, the study sought to determine if there is an inclusion of cybersecurity awareness and education programs within the Polytechnic curriculum. Initial findings revealed that while students claimed to possess basic knowledge of cybersecurity, they lacked sufficient understanding of data protection methods. Moreover, it was observed that most Polytechnics lacked an active cybersecurity awareness program to enhance students' knowledge of safeguarding themselves against cyber threats. The surveyed students expressed a desire for increased awareness and further education in the field of cybersecurity.*

Keywords: (Cyber, security, awareness, education, threat).

Introduction

Cybersecurity refers to a collection of principles and methods that are implemented to protect one's computing resources and online information from potential threats. The primary objective of cybersecurity is to decrease the likelihood of cyber-attacks and prevent unauthorized exploitation of network, technological, and system resources. According to Dunn-Cavelty (2019), cybersecurity encompasses "the insecurity created through the use of cyberspace and the technical and non-technical aspects of making it more secure." This assertion shows that cybersecurity is not solely a "technical" concern, typically classified within computer science, cryptography, or information technology. Numerous studies have investigated cybersecurity issues in recent years, including Vacca (2018) and McLean (2018). Currently, over 61% of entire industry transactions take place online; thus, the sector requires high-quality security measures to facilitate secure and direct transactions.

Related Reviews

Cybersecurity is concerned with the vulnerability created by and through this emerging space, as well as the practices or procedures to enhance its security (Kumar, & Somani, 2018). Therefore, cybersecurity has become a prominent issue. Modern technologies such as cloud services, mobile devices, E-commerce, internet banking, and various others necessitate stringent security measures. These transactions involve sensitive and crucial user information, highlighting the need for adequate security measures. Enhancing

cybersecurity and protecting sensitive data and infrastructures are of utmost importance and a top priority for every country (Panchanatham, 2019).

According to FraudWatch International (2018), cyber security awareness refers to the level of knowledge end-users possess about cyber security threats, the risks they may introduce, and the best practices to mitigate them.

Increasing awareness can reduce the occurrence of cyber-attacks. As McDaniel (2018) contends, cybersecurity awareness programs should include essential elements such as security policies and rules designed to achieve desired outcomes. Katz (2020) explains that university systems are continuously prone to attacks due to the accessibility of information and the vast amount of power worth connecting. Moreover, Knapp, Marshall, Rainer, and Ford (2019) suggest that there is a direct relationship between preventive measures and information security awareness, which can enhance security performance.

Cybersecurity education aims to provide knowledge and awareness to technology users regarding the potential risks associated with internet communication tools. These tools include social media, chat platforms, online gaming, email, and instant messaging. In the United Kingdom (UK), there is a proposal to incorporate Information and Communications Technology as a fundamental skill in early education curricula (Education and Training Foundation, 2019). Additionally, efforts are being made to educate children on online safety (Sutton, 2011) and the



ability to identify fake news (Cockburn, 2019). ICT use is now intertwined with Internet use. It then follows that anyone using the Internet, whatever their age, also needs to know how to secure their devices because forewarned is forearmed (Renaud et al., 2016). Safety and security are semantically different concepts (Waldron, 2016) requiring different kinds of knowledge and skill sets. Smartphone users, of all ages, should know that their phones are vulnerable to attack, and also know how to improve device security. Because education is at the heart of security awareness and capability (Siponen, 2018), it is imperative for cyber security education to reach all of society and all ages. Cyber security education has two elements: first people need to become aware of the need to take precautions, and then teachers need to impart the skills they require to take the required precautions. We plan to assess awareness, as an essential prerequisite to mastering cyber security skills.

Materials and Methods

This research will employ a quantitative approach to design a questionnaire-based survey aimed at collecting data using an online method. The survey will assess participants' level of cybersecurity education and awareness, focusing on students attending tertiary institutions in Nigeria. These students have been chosen due to their active engagement with daily activities and their potential future employment in various organizations.

The survey link will be disseminated specifically to students of polytechnics in Nigeria. Based on the aforementioned objectives, the questionnaire will be formulated, and an online platform will be utilized for students to access and complete the questionnaire. The survey will consist of 15 primary questions, with response options limited to "Yes," "No," and "Maybe." Additionally, five demographic questions will be included.

The estimated time for a participant to complete the survey is around 15 to 20 minutes. The questions will be design to provide answers to the objective of the paper, the key focus area includes Basic knowledge of cybersecurity Trust, Privacy, Password management, the desire to learn cybersecurity and cybersecurity awareness program as a course. The protocol of this questions was adopted based on the study carried out by (Moallem, 2018; Al-Janabi & Al-Shourbaji, 2016).

Method of data collection

The data collection method refers to the specific procedures used to gather information for the study. In this research, both primary and secondary methods of data collection will be employed. Primary data will be gathered through conducting in-depth interviews with selected informants. Meanwhile, secondary data will be obtained

from various sources such as journals, magazines, textbooks, newspapers, encyclopedias, previous theses, seminar presentations, and other relevant secondary sources. Additionally, information will be retrieved from pertinent electronic websites and official documents from international organizations. The utilization of the secondary method will complement the primary method in this study.

Results and Discussion

The link for the questionnaire was distributed and takes one month for respondents to answer the questions before the link was disabled. A total number of 400 students was selected, with 40 students from different institutions that filled the questions and all questions from each participant was filtered to see if some questions were not answered or left blank. Among the questions given a total number of answers identified to be valid, analysis was conducted using these samples.

The completed survey consists of demography data which include age and gender were collected. Out of 400 responders, 18- 20 ages are 185 students, 21- 26 are 95 students, and 27 –31 are 120 respectively and in gender, males are 280, and females are 120 and those that answered prefer not to say are 8. From this analysis is shown most responders are male and between the age of 26 to 31.

The questions for the survey are as follows:

1. Basic Knowledge about Cybersecurity

The question was asked, do you consider yourself knowledgeable about the concept of cybersecurity, to determine the basic knowledge of cybersecurity.

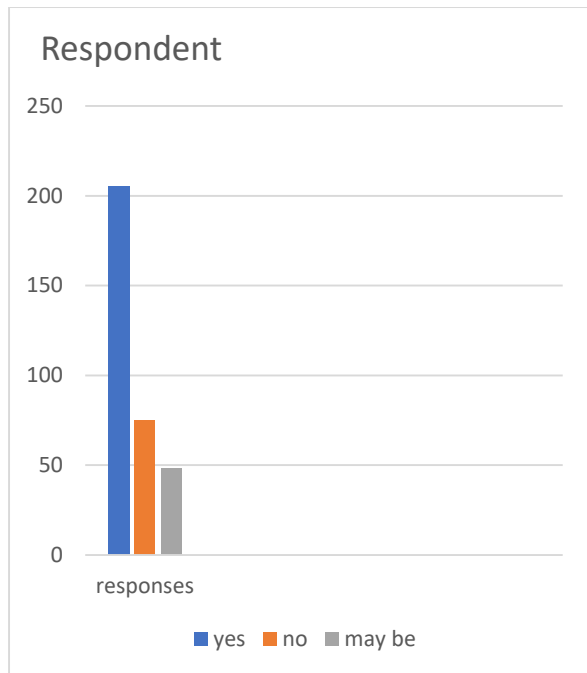


Fig.01: Response on Cyber Security

Figure 1 shows the response on Q1, from this chart it shows the number of students that have basic knowledge is 205 and 75 said No and others are not sure answered maybe which is 48. This shows the majority of the students have some basic knowledge about cybersecurity but few were not sure about the concept of cybersecurity but when the number of ‘no’ and ‘maybe’ are combined is 123 which is more than half. This shows that there is a need to educate the students on the concept of cybersecurity.

2. Desire to Learn Cybersecurity

This question was part of the objective to know if students want to learn more about cybersecurity.

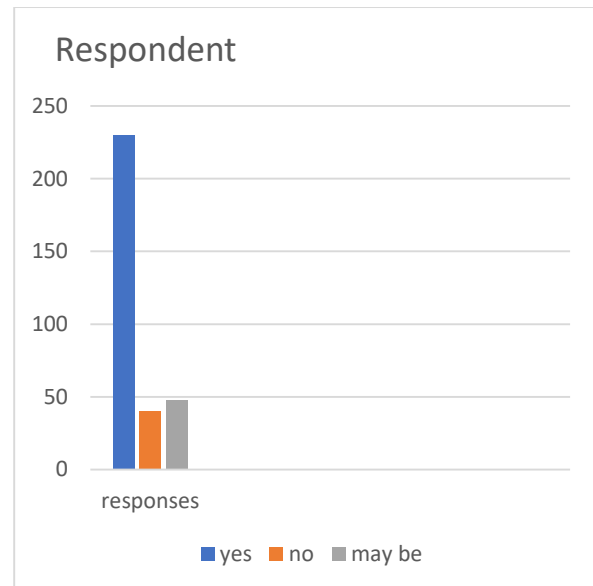


Fig. 2: Response on Desire to Learn Cyber Security

Figure 2 shows the response on the question, a total of 235 students said yes, 39 said No, and 48 said maybe. This result indicates the interest and needs for the students to learn more about cybersecurity. This shows awareness is highly needed.

3. Desire to have cyber security education as a course

The student was asked if they want cyber security education as a course in their various institutions.

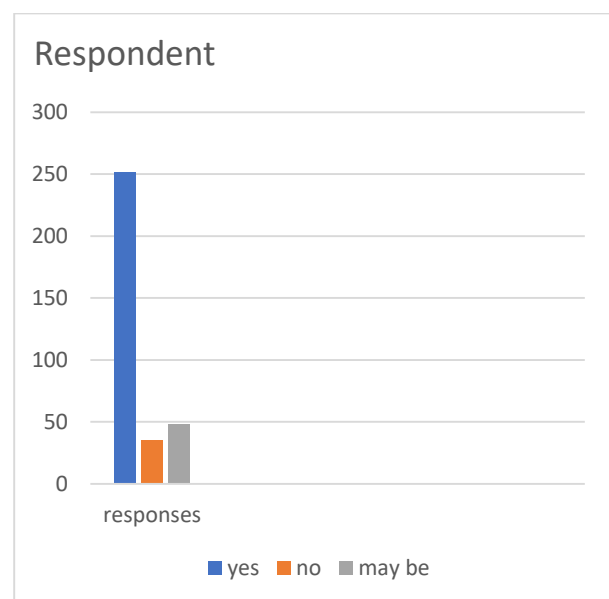


Fig. 3: Response on Cyber Security Education

Figure 3 shows the response on the question: Desire to have cyber security education as a course and wonderful result



outcome on whether the students are willing to take cybersecurity education as a course in their curriculum and the result shows an impressive consensus. A total number of 251 said yes 40 said no and 48 said may be this shows that polytechnics are lacking cybersecurity education as a course and this prompts to awareness of the NBTE.

4. Cybersecurity Awareness Program

This question was asked to know if the student have ever attended any cyber security awareness program online or physical in their various institutions.

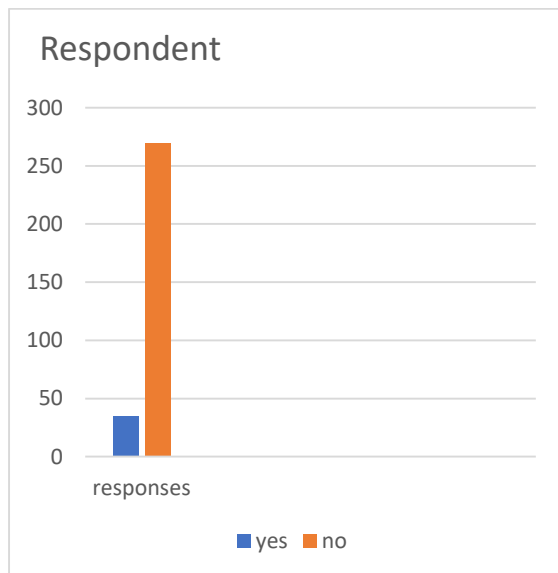


Fig. 4: Response on Cyber Security Awareness Program

Figure 3 shows the response on the question: have you attended any cyber security awareness program and the responses was not encouraging, 40 students said yes, and about 255 students said no which indicate that there is need for conducting cyber security awareness program to create awareness to the student on the importance of cyber security on our daily lives as we are in a digital world.

Conclusion and Future Works

In conclusion, cybersecurity education and awareness are indispensable in today's digital age to secure people, organizations, and their businesses from cyberattacks. By increasing knowledge and understanding about cyber threats and providing people with the tools to take preventative measures. So, also cybersecurity education can help minimize the risk of cyber-attacks as people will be more aware about the cyber threats. Therefore, cybersecurity education and awareness must remain a paramount importance in both our personal and professional lives to ensure the security and privacy of our digital information.

For future work in this regard there is need to develop framework that will help in creating awareness about cyber security among students in tertiary institutions and strategies to combat cyber-crimes in real time. Furthermore, future research in this area additionally should focus on development of real time cyber security awareness, cyber-attack detection and mitigation.

References

- Awareness and Practices.Proceedings-2016 Cybersecurity Symposium CYBERSEC 2016,68–73
<https://doi.org/10.1109/CYBERSEC.2016.018>
- AMcDaniel, E. (2018). Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness. *Issues in Informing Science and Information Technology*, 10(2017), 313–324.
<https://doi.org/10.28945/1813>
- Aloul, F. A. (2018). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, 3(3).
<https://doi.org/10.4304/jait.3.3.176-183>
- Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information and Knowledge Management*, 15(1).
<https://doi.org/10.1142/S0219649216500076>
- Bendovschi, A. (2019). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 24-31.
 doi:10.1016/S2212-5671(15)01077
- Cabaj, K., *et al.* (2018). Cybersecurity: trends, issues, and challenges. *EURASIP Journal on Information Security*.doi:10.1186/s13635-018-0080-0
- Cybersecurity awareness survey: An analysis from Bangladesh perspective. 5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017, 2018-January, 788–791.
<https://doi.org/10.1109/R10-HTC.2017.8289074>
- Chan, H. (2019). Significance of Information Security Awareness in the Higher Education Sector. *60(10)*, 23–31.
- Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2017). A video game for cyber security training and awareness. *Computers and*



- Security, 26(1), 63–72.
<https://doi.org/10.1016/j.cose.2017.10.005>
- Dun N. and Pullet K, —The urgency for cybersecurity education: The impact of early college innovation in hawaii rural communities, Information System Education Journal, vol. 16, no. 4, pp. 41-52, 2019.
- Dervojeda, K., *et al.* (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.
- Exploitation: Developing a Strategy for Education, Training, and Awareness. Issues in Informing Science and Information Technology, 10(2018),313–324.
<https://doi.org/10.28945/1813>
- Evaluation Methodology. Information Security Journal, 21(6),328–345.
<https://doi.org/10.1080/19393555.2012.747234>
- Exploitation: Developing a Strategy for Education, Training, and Awareness. Issues in Informing Science and Information Technology, 10(2012), 313–324.
<https://doi.org/10.28945/1813>
- Exploration .ProQuest Dissertations and Theses, D.I.T.(August).Retrieved from
http://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF8&rft_id=info:sid/Dissertations+%2526+Theses+%2540+Capella+University&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&rft.genre=dissertations+%252
- Gade, N. R., & Reddy, U. G. (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. Retrieved from
https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies
- Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018 Information Privacy and Security, 8(4), 3–26.
- <https://doi.org/10.1080/15536548.2012.10845664>
- Moallem, A. (2019). Cybersecurity Awareness Among Students and Faculty. In Cybersecurity Awareness Among Students and Faculty (Vol. 2). <https://doi.org/10.1201/9780429031908>
- Pramod, D., & Raman, R. (2019). A study on the user perception and awareness of smartphone security.
- Panchanatham, D. N. (2020). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.
- Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. (2018). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes,44(4),606–622.
<https://doi.org/10.1108/K-12-2014-0283>
- Sharma, R. (2019). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).
- Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. 2016 14th Annual Conference on Privacy, Security and Trust, PST 2016, 223–228.