Journal of Applied Technology and Innovation
Vol. **09,** Issue 4, 2025**,** pp. **25-32**
e-ISSN:2600-7304-ISSN
DOI: https://doi.org/10.65136/jati.v9i4.37

Cyber Security Awareness and Challenges: A Study of Undergraduates at Adeyemi Federal University of Education, Ondo State, Nigeria.

Sina Opeoluwa Ayelaagbe [1*]

[1] Department of Educational Technology, Adeyemi Federal University of Education, Ondo State, Nigeria.
*Corresponding Author: oayelaagbe@yahoo.com

Abstract

Cyber security education is the process of receiving or giving systematic justification in a school or university or online on the proper use of technological processes, networks and data from cyber-attacks. This study investigated into cyber security education, awareness and challenges among undergraduates at Adeyemi Federal University of Education (AFUED), Ondo, Ondo State, Nigeria. The descriptive survey was adopted for this study. The population comprises of all undergraduates at Adeyemi Federal University of Education, Ondo, Ondo State, regardless of their levels, gender and departments. The respondents were selected using simple random sampling technique and the sample size consisted of 560 undergraduates selected from the five faculties in the universities. 102 respondents were selected from Faculty of Arts, 140 were selected from Faculty of Education, 120 from Faculty of Social Sciences and Management, 93 from Faculty of Sciences and 105 were selected from Faculty of Vocational and Technical Education. The Instrument for data collection was the researcher's self-developed questionnaire titled "Cyber Security Awareness and Challenges: A Study of Undergraduates Questionnaire. "CSACASUQ". The instrument was validated by 3 lecturers from Department of Computer Science, Adeyemi Federal University of Education, Ondo, Ondo State. The reliability Coefficient was obtained using Cronbach Alpha 0.85 value for awareness and 0.91 values for challenges for using cyber security. Research questions were answered using mean and standard deviation. The finding of the study showed that Nmaps was the most used cyber security tools and that the awareness of cyber security was very high among undergraduates. The study therefore recommends that the cyber security facilities should be adequately provided, and workshops, conferences and seminars should be organized to increase the awareness level of undergraduates.

Keywords: *Cyber Security Education, Online Awareness, Challenges, Undergraduate Computer Science.*

1. Introduction

The inception of the internet allows humans to benefit from two realms: real life and the virtual world (Lokman, et al., 2019). Search engines such as Google and Yahoo, as well as video-sharing sites including YouTube, make information widely accessible and instantly available. Nevertheless, the continuing expansion of global cyberspace can also expose users to harmful outcomes, including cybercrime. Cyber Security can be seen as protecting networks, devices, electronic systems, and data from penetration, disruption, modification, or illegal entry, use, or exploitation through cyber-attacks, affecting victims

ranging from business enterprises to personal devices (Cisco, 2020). In practice, this protection spans multiple domains, including network security, application security, information security, organizational security, disaster recovery, and business continuity. Network protection and application security focus on safeguarding networks and ensuring that hardware and software are free from threats and vulnerabilities. Disaster recovery describes an organisation's response in the event of data loss and the effort to regain operating capabilities in order to continue its work (Kaspersky 2020). In addition, smartphone users of all ages should recognise that mobile devices can also be vulnerable to attack and should understand ways to strengthen device security. Education is at the heart of security awareness and capability (Zabi et al., 2025); therefore, Cyber Security Education needs to reach all segments of society and all age groups.

Cyber security education includes both awareness and competence. First, people need to understand why precautions are necessary; second, they need practical skills to apply appropriate safety measures. A central objective of cyber security education is to educate technology users about potential risks associated with internet communication tools: social media, chat applications, online gaming, e-mail, and instant messaging, so that they can protect themselves against cyber threats. Cyber Security is a significant issue affecting internet users not only in higher institutions of learning but also in schools across Nigeria. Cyber security awareness refers to the level of knowledge end-users possess about cyber security threats, the risks these threats introduce, and best practices for mitigating them. Improving awareness can reduce the incidence of cyber-attacks.

A related aspect of cyber security education involves familiarity with and comprehension of frequently utilized cyber security tools. Hamzat, (2022) listed various cyber security tools along with their functions, categorizing them into groups like network security monitoring tools, encryption tools, web vulnerability scanning tools, wireless network defense tools, firewalls, penetration testing tools, antivirus programs, packet sniffers, and public key infrastructure. Alabi, (2023) similarly pointed out that many tools are employed across these domains and threats, including Nmaps, Wireshark, Metasploit, Burp Suite, John the Ripper, Tcpdump, Aircrack-ng, Cain and Abel, Nikto, and Snort. Alabi, (2023) characterized Nmap as a popular tool due to its free and open-source nature, which allows it to scan IT systems and networks for security weaknesses. Gaining knowledge about the tools undergraduates frequently utilise can shed light on their exposure to cyber security practices and the practical aspects of their understanding..

Empirical studies across contexts have reported varying levels of cyber security awareness. Sezer et. al. (2015) examined levels of awareness in Turkish schools concerning cyber bullying, measuring teachers' awareness and the extent to which it influenced daily life, with emphasis on personal cyber security and possible precautions. The study revealed that teachers had a medium level of awareness about cyber bullying in general. Ismailova and Mullametjanova (2016) examined information security awareness levels among students in the Kyrgyz Republic and reported that, despite frequent reports of cybercrime, awareness of cybercrime was quite poor among students. Their findings also indicated that students were often unaware of many categories of computer crime, despite extensive use of information technology. SenthilKumar and Easwaramoorthy, (2017) carried out a survey on cyber security awareness among college students in Tamil Nadu, focusing on three major cyber-attacks: virus attacks, phishing via emails, and threats involving the spread of personal details. The authors reported that 70% of students were aware of virus attacks and used antivirus software, and they concluded that the overall degree of awareness among students was at a good level that could help them protect themselves from cyber-attacks. Within Nigeria, Zabi et al. (2003) investigated cyber security education and awareness in Nigerian polytechnics and found that most polytechnics lacked an active cyber security awareness programme to enhance students' knowledge of how to safeguard themselves against cyber threats.

At the same time, schools and higher institutions face persistent challenges in implementing cyber security education effectively. Social media platforms such as Facebook, WhatsApp, Istagram, LinkedIn,

YouTube, Twitter, and e-mail are widely used internet applications in Nigeria, increasing the number of daily online interactions and, potentially, exposure to threats. Several constraints have been identified in efforts to implement cyber security in educational settings, including lack of expertise, funding and resources, and teachers' limited knowledge and competence regarding cyberspace. In addition, schools and government ministries may lack the facilities and resources required to implement cyber security education effectively (Salamzada et. al., 2015). The rapid pace of technological change also introduces new risks that require new solutions, creating ongoing pressure for teachers to update their knowledge and ensure that students remain safe. Lack of access to learning materials further constrains teachers' ability to provide effective instruction (Rahman et. al., 2020).

Beyond institutional capacity, the literature has repeatedly highlighted workforce constraints. Mountrouidou, et al. (2019), Choudhury (2022) and Nobles (2018) described a significant shortage of cyber security professionals and specialists who can provide cyber leadership and who can train, test, and secure digital systems used by people. Armstrong Carter et al. (2018) reported that the lack of qualified professionals to guide high school and college students in pursuing cyber security careers contributes substantially to this shortage. The lack of mentors has also limited the number of women prepared to become cyber security specialists. Burrell, (2020) similarly reported that a shortage of experts and professionals discourages young people from pursuing cyber security careers because role models and mentors are unavailable to guide them.

Curriculum and programme challenges also remain. Sanzo et al. (2021) observed that, although schools attempt to update their information security courses, shortages of specialists make it difficult for institutions to keep pace with the changing cyber security environment. Alrabaee et al. (2022) reported a lack of standardized cyber security educational programmes and noted challenges in updating courses, alongside concerns that cyber security graduates may be ill-equipped with the skills demanded by the job market; factors that can discourage students from seeking cyber security as a career.

Research and education have transformed extensively in this generation, leading many researchers and students to spend extended periods online for teaching and learning activities, academic communication, research, and social engagement on various social media platforms. In this context, there is a need to include cyber security education in the school curriculum, as any individual connected to the internet can become vulnerable at different times and may be targeted by cyber criminals or attackers. As students and teachers increase their online presence, cybercriminal activity and influence may also expand, reinforcing the importance of educating learners and educators about safe practices in cyberspace. Therefore, this study investigated the awareness and challenges of cyber security among undergraduates in Adeyemi Federal University of Education (AFUED), Ondo, Ondo State, Nigeria. Specifically, the study sought to (1) investigate the most used cyber security tools among undergraduates at AFUED, Ondo; (2) assess the level of awareness of undergraduates regarding cyber security at AFUED, Ondo; and (3) find out the challenges faced by undergraduates in relation to cyber security at AFUED, Ondo. In line with these objectives, the study addressed the following research questions: (1) What is the most used cyber security tools among the undergraduates at AFUED, Ondo? (2) What is the level of awareness of undergraduates using cyber security at AFUED, Ondo? and (3) What are the challenges of cyber security among undergraduates at AFUED, Ondo?

2. Methodology

The study used a quantitative research design based on a survey method through questionnaire. Survey method was employed on this research study because it is an efficient way for collecting information from large number of respondents. Simple random sampling technique was used for this research study and the population consisted all undergraduates at Adeyemi Federal University of Education (AFUED), Ondo, Ondo State, Nigeria.

There are five (5) faculties presently at AFUED were used for this research study regardless of the departments and gender. In order to give all the respondents equal opportunity for been selected, a random sampling technique was adopted to select five hundred and sixty (560) respondents from the five faculties at AFUED Ondo. From Faculty of Arts 102 respondents were selected, Faculty of Education 140 respondents, Faculty of Social Sciences and Management 120 respondents, Faculty of Sciences 93 respondents, Faculty of Vocational and Technical Education 105 respondents were selected respectively. The main instrument for this study is researcher's designed questionnaire "Cyber Security Awareness and Challenges: A Study of Undergraduates Questionnaire, "CSACASUQ". The questionnaire consists of two sections: Section "A" contains Demographic data of respondents while section "B" contains items on Cyber Security Education awareness and challenges among Undergraduates. The questionnaire was subjected to both face and content validity to check the appropriateness and adequacy of the content of the instrument. Three (3) lecturers from Department of Computer Science from Adeyemi Federal University of Education, Ondo, Ondo State validated the instrument. After they deemed it fit to be validated their advice and suggestions were used to modify the questionnaire to produce final draft.

The questionnaire was tested for reliability on fifty (50) randomly selected undergraduates from Wesley Universities of Science and Technology, Ondo, Ondo State, who were not part of this study. The data gathered from the trial test was analysed to check for internal consistency in reliability. The Cronbach Alpha was used and the values obtained were 0.85 for awareness and 0.91 for challenges for using Cyber Security Education among university undergraduates. This indicated that the research instrument was highly reliable. The researcher with the help of research assistants in the five (5) faculties at AFUED administered copies of e-questionnaire through various social media platforms of the selected respondents.

At the end of the exercise, 560 valid responses of the e-responses were retrieved from the undergraduates upon which analysis of the result were carried out using mean and standard deviation to answer the research question raised.

3. Results

3.1 Research Question 1: What is the most used Cyber Security tools used in education among the Undergraduates?

Table 1:

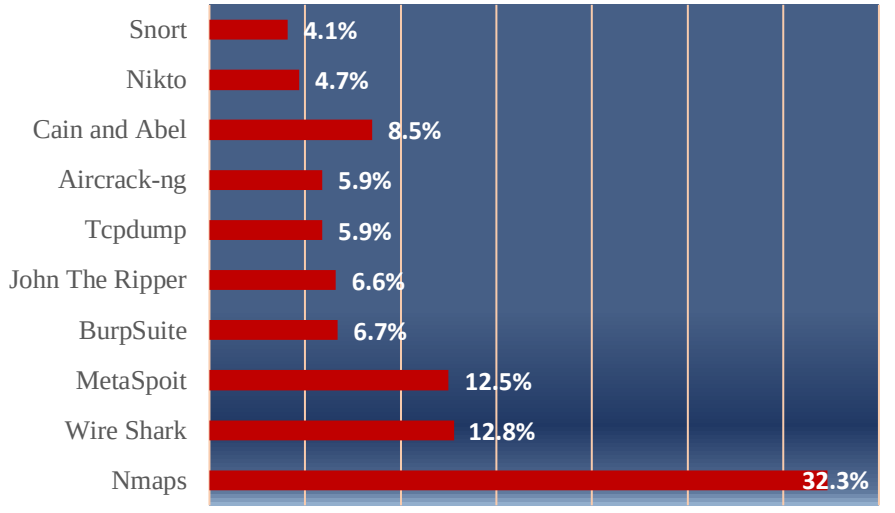
Most Used Cyber Security Tools (CST) among Undergraduates (No of responses = 833)

Cyber Security Tools	**Multiple Responses**	
	Frequency (N)	Percent (%)
Nmaps	269	32.3
Wire Shark	107	12.8
MetaSpoit	104	12.5
BurpSuite	56	6.7
John The Ripper	55	6.6
Tcpdump	49	5.9
Aircrack-ng	49	5.9
Cain and Abel	71	8.5
Nikto	39	4.7
Snort	34	4.1

Table 1 above shows the most used cyber security tools among undergraduates. Overall, Nmaps was indicated as the most used cyber security tools used with (32.3%), followed by Wire Shark (12.8%), MetaSpoit (12.5%), Cain and Abel (8.5%) and BurpSuite (6.7%). John The Ripper had (6.6%), Tcpdump

with (5.9%), Aircrack-ng (5.9%), Nikto (4.7%) while the least used cyber security tool is Snort (2.0%). Therefore, the most used cyber security tools among undergraduates in classroom are: Nmaps, Wire Shark, and MetaSpoit. Figure 1 further presents the result from the table in a bar chart.

Figure 1: Bar Chart showing the Usage of Cyber Security Tools



3.2 Research Question 2: What is the level of awareness of using cyber security by undergraduates?
Table 2
Level of Awareness of Using Cyber Security by Undergraduates

Item	SA	A	D	SD	Mean	Std. D
I think the internet is safe for me.	289	167	75	29	3.28	.88
I am aware that shopping online is safe	203	240	89	28	3.10	.84
I think using the internet with my mobile phone is more secure than using my laptop.	184	143	169	64	2.80	1.02
I frequently scan my laptop and storage devices	223	201	45	91	2.99	1.06
My passwords is always change regularly.	220	185	85	70	2.99	1.02
I don't open my emails from unknown sender.	320	189	44	7	3.48	.69
Cyber security should be taught in schools	178	242	95	45	2.99	.90
Undergraduates should be taught about cyber security.	168	173	166	53	2.81	.97
Higher institutions of learning should be provided with user-friendly teaching materials online.	174	195	138	53	2.88	.96
Cyber security education is important when using software	182	202	100	76	2.88	1.02
Weighted Average					**3.02**	

Key; *SD* = Strongly Disagree, **D** = Disagree, **A** = Agree, **SA** = Strongly Agree
Decision Value: ***Low*** = 0.00-2.49, ***High*** = 2.50-4.00

Table 4.3 shows the level of awareness of using cyber security by undergraduates. The table shows that the students agreed to the following items: think the internet is safe($\bar{x}$ = 3.28), aware that shopping online is safe ($\bar{x}$ = 3.10), I think using the internet with my mobile phone is more secure than laptop ($\bar{x}$

= 2.80), scan my laptop and storage frequently($\bar{x}$ = 2.99), my passwords always changes regularly ($\bar{x}$ = 2.99), I don't open my emails from unknown sender ($\bar{x}$ = 3.48), cyber security should be taught in school ($\bar{x}$ = 2.99), undergraduates should be taught about cyber security ($\bar{x}$ = 2.81), higher institutions of learning should be provided with user-friendly teaching materials online ($\bar{x}$ = 2.88), cyber security education is important when using software ($\bar{x}$ = 2.88). Meanwhile, based on the value of the weighted average (3.02 out of 4.00 maximum value obtainable) which falls, within the decision value for ***high,*** it can be inferred that the level of awareness of using cyber security by undergraduates is high.

3.3 Research Question 3: What are the challenges of using Cyber Security among Undergraduates?
Table 3
Challenges of Using Cyber Security Among Undergraduates

Item	SA	A	D	SD	Mean	Std.D	Remark
Lack of cyber security officials	294	183	57	26	3.33	.84	Accepted
Inadequate funding and resources	214	129	100	117	2.78	1.16	Accepted
Lack of access to learning materials in schools	188	118	125	129	2.65	1.17	Accepted
Lack of mitigation and resources	232	138	89	101	2.89	1.13	Accepted
Rapidly change of Technology	130	140	178	112	2.51	1.06	Accepted
Unaware of cyber rights	301	196	56	7	3.41	.72	Accepted
Lack of standardized cyber security educational programmes	167	259	109	25	3.01	.82	Accepted
Complex cyber attacks	217	178	117	48	3.01	.97	Accepted
Human errors	162	241	113	44	2.93	.90	Accepted
Teachers lack of knowledge about cyber security.	235	215	84	26	3.18	.85	Accepted

Key; *SD* = Strongly Disagree, **D** = Disagree, **A** = Agree, **SA** = Strongly Agree
Decision Value for Remark: ***Not Accepted*** = 0.00-2.49, ***Accepted*** = 2.50-4.00

Table 3 presents the challenges of using Cyber Security among undergraduates. The table shows that students generally accepted all the items are: lack of cyber security officials ($\bar{x}$ = 3.33), inadequate funding and resources ($\bar{x}$ = 2.78), lack of access to learning materials ($\bar{x}$ = 2.65), lack of mitigation and resources ($\bar{x}$ = 2.89), rapidly change of Technology ($\bar{x}$ = 2.51), unaware of cyber rights ($\bar{x}$ = 3.41), lack of standardized cyber security educational programmes ($\bar{x}$ = 3.01), complex cyber-attacks ($\bar{x}$ = 3.01), human errors ($\bar{x}$ = 2.93), and teachers lack of knowledge about cyber security ($\bar{x}$ = 3.18). Based on the results from Table 3 and the mean score acceptance by the decision rule, the challenges of using Cyber Security among Undergraduates are: lack of cyber security officials, inadequate funding and resources, lack of access to learning materials in schools, lack of mitigation and resources, rapidly change of Technology, unaware of cyber rights, lack of standardized cyber security educational programmes, complex cyber-attacks, human errors, and lack of knowledge about cyber security.

4. Discussions

Findings of this study revealed the most used cyber security tools among undergraduates. It was revealed that Nmaps was the most used among undergraduates. This could be because it is a free, open-source tool that is effective and adaptable. Hamzat (2022) and Alabi (2023) enumerated various cyber security tools and supported the use of Nmaps because of its usefulness among the undergraduates.

The result of this research study showed that the level of awareness of using cyber security by undergraduates is high. This was supported by Senthilkumar and Easwaramoothy (2017) that the degree of awareness of cyber security among college students in Tamil Nady was at a good level. But the findings

of Ismailova and Mullametianova (2016) contradicts findings of this study and they pointed out that student's awareness of cyber security was poor. This disparity could be attributed to some factors such as, location, provision of ICT infrastructure and adequate and professional cyber security experts.

Also, from the finding it was revealed that there are challenges/threats facing the use of cyber security among undergraduates. Some of the challenges/threats are lack of cyber security officials, inadequate funding and resources, lack of access to learning materials in schools and so on. This finding is in consonance with the findings of Rahman et al. (2020), Mountroulded et al. (2019), Choudhury, (2022), Nobles, 92018), Burrell (2020) and Sanzo et al. (2021) described in their various studies that challenges/threats facing the use of cyber security in schools. Their findings are in line with the findings of this study.

5. Conclusion

The use of cyber security education in schools is very important and this has been revealed in this study. It was revealed from this study that undergraduate used Nmaps mostly in their respective schools because it is a free and open source cyber security tool.The respondents agreed on the level of awareness of Cyber Security among undergraduates. Despite their awareness of the use of cyber security. There are challenges facing the usage of cyber security and this was revealed in this study.

Based on the findings of this study, it is recommended that schools be adequately equipped with relevant cyber security facilities to broaden undergraduates' access to, and practical use of, a wider range of cyber security tools. In addition, education stakeholders should further strengthen undergraduates' cyber security awareness through regular workshops, conferences, and seminars that emphasise safe digital practices and emerging threats. Finally, stakeholders should make deliberate budgetary provisions for both cyber security infrastructure and qualified professionals, as this will help to address the constraints and reduce the challenges undergraduates face in applying cyber security measures within the school environment.

References

Alabi, F. (2023). *Cyber security tools and their uses*. ResearchGate. https://www.researchgate.net/publication/375775829_CYBER_SECURITY_TOOLS_AND_THEIR_USES

Alrabaee, S., Aldaajeh, S., Seleous, H., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cyber security strategies on the improvement of cyber security education. *Computers & Security*, *119*, Article 102754. https://doi.org/10.1016/j.cose.2022.102754

Armstrong, M. E., Jones, K. S., Namin, A. S., & Newton, D. C. (2018). The knowledge, skills, and abilities used by penetration testers: Results of interviews with cybersecurity professionals in vulnerability assessment and management. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *62*(1), 709–713. https://doi.org/10.1177/1541931218621161

Burrell, D. N. (2020). An exploration of the cybersecurity workforce shortage. In *Cyber warfare and terrorism: Concepts, methodologies, tools, and applications* (pp. 1072–1081). IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch063

Choudhury, M. D. (2022, January 15). *Shortage of cybersecurity professionals a key worry for firms in '22*. Mint. https://www.livemint.com/technology/shortage-of-cybersecurity-professionals-a-key-worry-for-firms-in-22-11642015098080.html

Cisco. (2020). *What is cybersecurity?* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Hamzat, L. (2022). *Cyber Threat Intelligence (CTI): Tools and applications* [Conference presentation]. Nigeria Computer Society (NCS) International Conference. https://www.ncs.org.ng

Ismailova, R., & Muhametjanova, G. (2016). Cybercrime risk awareness in the Kyrgyz Republic. *Information Security Journal: A Global Perspective*, *25*(1–3), 32–38. https://doi.org/10.1080/19393555.2015.1132800

Kaspersky. (2020). *What is cyber security?* https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lokman, H. F., Nasri, N. M., & Khalid, F. (2019). The effectiveness of using Twitter application in teaching pedagogy: A meta-synthesis study. *International Journal of Academic Research in Progressive Education and Development*, *8*(2), 205–212. https://doi.org/10.6007/IJARPED/v8-i2/5707

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the human: A review of literature on social engineering in computer science education. *Proceedings of the 2019 ACM Conference on Innovation and Technology in Computer Science Education*, 157–176. https://doi.org/10.1145/3344429.3372506

Nobles, C. (2018). The cyber talent gap and cybersecurity professionalizing. *International Journal of Hyperconnectivity and the Internet of Things*, *2*(1), 42–51. https://doi.org/10.4018/IJHIOT.2018010104

Rahman, N. A., Sairi, I. H., Zizi, N. A., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Salamzada, Z., Zarina, S., & Bakar, M. A. (2015). A framework for cyber security strategy for developing countries: Case study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia*, *4*(1), 1–10. https://journal.ukm.my/apjitm/article/view/26990

Sanzo, K. L., Paredes Scribner, J., & Wu, H. (2021). Designing a K-16 cybersecurity collaborative: The CIPHER initiative. *IEEE Security & Privacy*, *19*(2), 73–79. https://doi.org/10.1109/MSEC.2021.3050246

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering*, *263*(4), Article 042043. https://doi.org/10.1088/1757-899X/263/4/042043

Sezer, B., Yilmaz, R., & Karaoglan Yilmaz, F. G. (2015). Cyberbullying and teachers' awareness. *Internet Research*, *25*(4), 674–687. https://doi.org/10.1108/IntR-01-2014-0023

Zabi, A. A., Adams, A. B. B., & Yakubu, A. C. (2023). Cybersecurity education and awareness. *Ilaro Journal of Science and Technology*, *3*, 1–11. https://sciencetechjournal.federalpolyilaro.edu.ng/