UNIJERPS
Unizik Journal of Educational Research and Policy Studies VOL.18 (2);
July-December, 2024 https://unijerps.org
2023 Impact Factor:* 6.834;** 2022 ***Impact Factor: 5.156; ***2021 Impact Factor: 5.641;***
2020 Impact Factor: 5.355. *Indexing and Impact Factor URL: http://sjifactor.com/passport.php?id=21363*

LECTURERS' AWARENESS OF SECURITY THREATS AND PROTECTION MEASURES IN DIGITAL ASSESSMENT IN HIGHER INSTITUTIONS IN ANAMBRA STATE, NIGERIA

Lydia I. Eleje (Ph.D)
Department of Educational Foundations, Faculty of Education,
Nnamdi Azikiwe University Awka, Anambra State, Nigeria

Tel: +2348032756383; Emails: ijeomaexcite@gmail.com, li.eleje@unizik.edu.ng

Orcid A/c: http://orcid.org/0000-0002-8587-289X

Obiageli I Ikwuka (Ph.D)
Department of Educational Foundations, Faculty of Education,
Nnamdi Azikiwe University Awka, Anambra State, Nigeria
Email: oi.ikwuka@unizik.edu.ng
Orcid A/c: http://orcid.org/0000-0002-9466-1296

Ifeoma C. Metu (Ph.D)
Department of Educational Foundations, Faculty of Education,
Nnamdi Azikiwe University Awka, Anambra State, Nigeria.
Email: ic.metu@unizik.edu.ng
https://orcid.org/0000-0003-2968-2853

Nneka C. Ezeugo (Ph.D)
Department of Educational Foundations, Faculty of Education, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. Email: nc.ezeugo@unizik.edu.ng; nnekaezeugo@yahoo.com
https://orcid.org/0000-0002-3680-3150

Abanobi, C. C. (Ph.D)
Department of Educational Psychology
Federal College of Education (Technical), Asaba
Email: christopher.abanobi@fcetasaba.edu.ng, abanobichidiebere@gmail.com
Orcid A/c: https://orcid.org/0000.0003-4108-2308

Njideka G. Mbelede (Ph.D)

Department of Educational Foundations, Faculty of Education, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. Email: ng.mbelede@unizik.edu.ng
https://orcid.org/0000-0002-7889-0440

UNIJERPS
Unizik Journal of Educational Research and Policy Studies VOL.18 (2);
July-December, 2024 https://unijerps.org
2023 Impact Factor:* 6.834;** 2022 ***Impact Factor: 5.156; ***2021 Impact Factor: 5.641;***
2020 Impact Factor: 5.355. *Indexing and Impact Factor URL: http://sjifactor.com/passport.php?id=21363*

ABSTRACT

As digital assessments are increasingly being utilized in place of paper-based exams, instructors at higher education institutions have a serious obligation to be aware of the security risks that are peculiar to these assessments and the accompanying protective measures. Thus, 200 lecturers who were specifically selected from the education departments of government-owned postsecondary educational institutions in Anambra state, Nigeria, that offer degrees were the subjects of this study. Questionnaires were the instrument utilized to collect data. In data analysis, chi-square (χ^2) test, frequencies, and percentages were employed. A p-value of less than 0.05 was deemed significant. The study's findings demonstrated that instructors of both sexes had an equal understanding of the security risks and safeguards in digital assessment. Additionally, a higher percentage of non-professorial lecturers than professorial lecturers are knowledgeable about the security risks and safeguards in digital assessment. The authors suggest providing sufficient training opportunities to instruct lecturers on how to apply protection measures for digital assessments.

Keywords: Professorial cadre, non-professorial cadre, security threats, education discipline, higher institution.

Introduction

There are several benefits of digital learning, such as reducing costs, time and improving performance of learning. Al Rawashdeh et al., (2021) stated that digital learning provides scientific material in an interesting way. It increases the possibility of communication and interaction between students and with teacher, enables students to communicate with the teacher by e-mail at any time and any place. For a fact, digital learning also has become a way of life for many businesses. According to Gutierrez (2012), the corporate training market spent over $200 billion in 2012; digital learning accounted for $56 billion of that amount and was predicted to grow in the ensuing years. It is noteworthy that digital learning systems contain multiple security flaws pertaining to content protection and user privacy. The systems are also susceptible to other kinds of online attacks. Phishing and spyware assaults can be used by attackers to trick people into disclosing credit card numbers and other private information (Bercy Infos Particulars, 2023; Siddiqui & Verma, 2011). Attackers may use phishing and spyware attacks to induce individuals to reveal personal information, such as passwords and credit card numbers (Bercy Infos Particulars, 2023; Siddiqui & Verma, 2011). The attackers could also implement social intersection attack to identify the source of shared sensitive data with very high accuracy (Puttaswamy et.al, (2009). This attack effectively works in collaboration system like the digital learning, and nearly impossible to be detected. Using the stolen user credentials, the attackers easily gain access to the server.

Accordingly, Miguel et al. (2013) noted that challenges associated with digital assessment include low scores, plagiarism, and vulnerabilities related to cyber-security, such as inconsistent authentication. The security risks in digital assessment for e-learning puts the confidentiality, integrity, validity, and reliability of learners' assessment outcomes or the assessment data at risk according to research by Shonola and Joy (2014). Siraj, Othman, and Garba (2022) noted in their study that self-defense, internet addiction, and cyberbullying are examples of cyber security dangers that call for immediate action or an awareness campaign. In order to solve cyber security challenges, they also suggest that there is an urgent need for a well-thought-out plan to implement security threats in digital assessment awareness initiatives. According to a recent study on cyber security awareness by Algahtani (2022) based on software and email security, cyber security awareness can be improved by up to 19.2% if one has a good understanding of software security and pays attention to updating the program or application either manually or automatically. According to their research, cyber security awareness can rise by as much as 31.3% when people have a thorough understanding of email security and take safeguards like not replying to unknown senders and rejecting any account that demands personal information. However, is tertiary institution lecturers aware of the security risks associated with digital assessment? Do they know about the countermeasures for these security threats?

Despite the recent interest in digital assessment in tertiary institutions, there are scant literatures on lecturers' awareness of security threats and protection measures in digital assessment in higher institutions. The available study by Eleje et.al (2022) focused on the influence of cyber-security problems in digital assessment on students' assessment outcome but not on the awareness of security threats and protection measures in digital assessment. Since assessment is a vital lens from which education is viewed and a teamster of student performance, the authors considers it important to investigate into the lecturers' awareness of security threats and protection measures in digital assessment in higher institutions. In order to close this research gap pointed out, thus, the objective of this study is to investigate the awareness of security threats and protection measures in digital assessment by the lecturers in tertiary institutions. The efforts of the researchers were guided by four research questions:

1. What is the percentage of awareness of security threats in digital assessment depending on lecturers' gender?
2. What is the percentage of awareness of security threats in digital assessment depending on lecturers' cadre?
3. What is the percentage of awareness of security protection measures in digital assessment depending on lecturers' gender?
4. What is the percentage of awareness of security protection measures in

digital assessment depending on lecturers' cadre?

To carry out the study, the authors tested the following formulated research hypotheses for rejection or otherwise at 5% level of significance:

Ho 1: There is no significant difference between male and female lecturers' awareness of the security threats in digital assessment in higher institutions.

Ho 2: There is no significant difference between the awareness of the security threats in digital assessment in higher institutions of lecturers on professorial and non-professorial cadre.

Ho 3: There is no significant difference between male and female lecturers' awareness of the protection measures in digital assessment in higher institutions.

Ho 4: The lecturers' perceived awareness of the security threats in digital assessment in higher institutions did not significantly vary based on cadre.

Research Method

This study followed a descriptive quantitative methodological approach. Two hundred (200) lecturers were purposively selected from the 903 lecturers in education discipline from government owned, degree awarding tertiary institutions in Anambra State, Nigeria. Using the authors self-constructed and validated structured four-point 8-item scale questionnaire, to measure lectures' awareness of security threats and protection measures in digital assessment in higher institutions, the researchers collected the necessary data in response to the research questions and hypotheses. Percentages, frequencies and chi-square (χ^2) test were used in data analysis. Analysis was by Statistical Package for Social Sciences version 23 (SPSS v 23.0). A p-value ≤ 0.05 was taken as significant.

Analysis Result and Discussion

The collected data were analyzed and the resulting outcomes presented in Tables 1, 2, 3 and 4 based on the stated research questions and hypotheses.

Research question 1, and hypothesis 1:

What is the percentage of awareness of security threats in digital assessment depending on lecturers' gender?

There is no significant difference between male and female lecturers' awareness of the security threats in digital assessment in higher institutions.

In Table 1 is presented the frequency, percentage and chi-square of the lecturers' awareness of the security threats in digital assessment in higher institutions based on gender.

Table 1: Lecturers' Awareness of the Security Threats in Digital Assessment Based on Gender

S/N	Have you ever heard of these security threats in digital assessment?	Male (N= 86)		Female (N=114)		
		Frequency of yes	Frequency of No	Frequency of yes	Frequency of No	Chi-square p-value l
1	Virus/malware attack	78(90.70%)	8(9.30%)	98(85.96%)	16(14.04%)	0.308
2	Exploiting security breach/privacy	34(39.53%)	52(60.47%)	42(48.84%)	72(51.16%)	0.698
3	Data/result interference for malicious acts	74(86.05%)	12(13.95%)	92(80.70%)	22(19.30%)	0.319
4	Unauthorized access to assessment contents	72(83.72%)	14(16.28%)	96(84.21%)	18(15.79%)	0.926
5	Verification/authentication issue	72(83.72%)	14(16.28%)	96(84.21%)	18(15.79%)	0.926
6	Plagiarism issue	38(44.19%)	48(55.81%)	54(47.37%)	60(52.63%)	0.655
7	Impersonation	36(41.86%)	50(58.14%)	48(42.11%)	66(57.89%)	0.972
8	Espionage: illegal equipment/information	24(27.91%)	62(72.09%)	36(31.58%)	78(68.42%)	0.575
9	Technical software failures or errors (coding problems, unknown loopholes)	72(83.72%)	14(16.28%)	104(91.23%)	10(8.77%)	0.106
10	Acts of human error or failure (accidents, employee mistakes)	76(88.37%)	10(11.63%)	106(92.98%)	8(7.02%)	0.259
	Total	**576(66.98%)**	**284(33.02%)**	**772(67.72%)**	**368(32.28%)**	

Field survey data (2024)

The lecturers' level of awareness of security threats in digital assessment based on gender presented in Table 1 revealed that more of the lecturers of both genders are aware of the security threats in digital assessment mentioned in items 1, 3, 4, 5, 9, and 10. The security threat with the highest (90.70%) awareness from male lecturers is virus/malware attack while acts of human error or failure (accidents, employee mistakes) have the highest (92.98%) awareness from female lecturers. In total more of the female lecturers (67.72%) than the male lecturers (66.98%) are aware of the security threats in digital assessment. This finding shows that the lecturers of higher institution of the study area are responding to the Siraj et.al, (2022) proposal of an urgent need for a good plan implementation of cyber security awareness to address cyber security issues.

The observed variance in lecturers' percentage of awareness of security threats in digital assessment based on gender is not significant since χ^2 values for all the items at 0.05 significance level with degree of freedom of 1 is greater than 0.05 ($P > 0.05$; $df = 1$). The null hypothesis which states that there is no significant difference between male and female lecturers' awareness of security threats in digital assessment is then accepted. This study authors find it worthy that lecturers of both gender are equally aware of the security threats in digital assessment. It is a positive step that the lecturers in higher institutions are aware of the security threats in digital assessment, but there is need for a solution

to these digital learning issues. Likewise, Miguel et al (2014a) argued that security requirements cannot be accomplished with technology alone; hence new models such as trustworthiness approaches could complete the technological solutions and support the e-assessment requirement for e-learning. The authors proposed a methodological approach to build a normalized trustworthiness model. Miguel et al (2014c) justifies the need of trustworthiness model as a functional requirement devoted to improve the security issues in digital learning.

Research question 2, and hypothesis 2:
What is the percentage awareness of security threats in digital assessment depending on lecturers' cadre?

There is no significant difference between the awareness of the security threats in digital assessment in higher institutions of lecturers on professorial and non-professorial cadre.

In Table 2 is presented the frequency, percentage and chi-square of the lecturers' awareness of the security threats in digital assessment in higher institutions based on cadre.

Table 2: Lecturers' Awareness of the Security Threats in Digital Assessment in Higher Institutions Based on Cadre

S/N	Have you ever heard of these security threats in digital assessment?	Non-Professorial (N= 148)		Professorial (N=52)		
		Frequency of yes	Frequency of No	Frequency of yes	Frequency of No	Chi-square p-value l
1	Virus/malware attack	130(87.84%)	18(12.16%)	46(88.46%)	6(11.54%)	0.905
2	Exploiting security breach/privacy	68(45.95%)	80(54.05%)	8(15.38%)	44(84.62%)	0.000
3	Data/result interference for malicious acts	124(95.38%)	24(4.62%)	42(80.77%)	10(19.23%)	0.619
4	Unauthorized access to assessment contents	120(81.08%)	28(18.92%)	48(92.31%)	4(7.69%)	0.057
5	Verification/authentication issue	122(93.85%)	26(6.15%)	46(88.46%)	6(11.54%)	0.308
6	Plagiarism issue	76(51.35%)	72(48.65%)	16(30.77%)	36(69.23%)	0.056
7	Impersonation	68(45.95%)	80(54.05%)	16(30.77%)	36(69.23%)	0.049
8	Espionage: illegal equipment/information	50(38.78%)	98(66.22%)	10(19.23%)	42(80.77%)	0.035
9	Technical software failures or errors (coding problems, unknown loopholes)	126(85.14%)	22(14.86%)	50(96.15%)	2(3.85%)	0.035
10	Acts of human error or failure (accidents, employee mistakes)	134(90.54%)	14(9.46%)	48(92.31%)	4(7.69%)	0.702
	Total	**1,018(68.78%)**	**462(31.22%)**	**330(63.46%)**	**190(36.54%)**	

Field survey data (2024)

The lecturers' level of awareness of security threats in digital assessment based on gender presented in Table 2 revealed that more of the lecturers in professorial cadre (69.23%) are not aware of the exploiting security breach/privacy, plagiarism, impersonation, espionage: illegal equipment/information security issue in digital assessment. The security threat with the highest (96.15%) awareness from non-professorial lecturers is technical software failures or errors (coding problems, unknown loopholes) while data/result interference for malicious acts have the highest (95.38%) awareness from professorial lecturers. In total more of the non-professorial lecturers (68.78%) than the professorial lecturers (63.46%) are aware of the security threats in digital assessment. It is possible that the non-professorial cadre lecturers are from the youthful age and familiar with digital learning and assessment, hence they are more aware of the security threats in digital assessment.

The observed variance in lecturers' percentage of awareness of security threats in digital assessment based on cadre for items 2, 7, 8, and 9 is significant since χ^2 values for the items at 0.05 significance level with degree of freedom of 1 is less than 0.05 ($P > 0.05$; $df = 1$). The null hypothesis which states that there is no significant difference between non-professorial and professorial lecturers' awareness of security threats in digital assessment is then rejected. This study result is in line with that of Alharbi (2021), Eleje et.al (2022), and Hamat, Embi and Hassan (2012) who observed that young ones are frequent in using digital gadgets and are more in non-professorial cadre. Hence, the reason to this significant difference between non-professorial and professorial lecturers' awareness of security threats in digital assessment in their favour. The exposures of the lecturers in terms of experience, travels, and ICT awareness may have contributed to the significant disparity.

Research question 3, and hypothesis 3.
What is the percentage awareness of the security protection measures in digital assessment depending on lecturers' gender?

There is no significant difference between male and female lecturers' awareness of the security protection measures in digital assessment in higher institutions. In Table 3 is presented the frequency, percentage and chi-square of the lecturers' awareness of the security protection measures in digital assessment in higher institutions based on gender.

Table 3: Lecturers' Awareness of the Security Protection Measures in Digital Assessment in Higher Institutions Based on Gender

S/N	Have you ever heard of these security protection measures in digital assessment?	Male (N= 86)		Female (N=114)		Chi-square p-value l
		Frequency of yes	Frequency of No	Frequency of yes	Frequency of No	
1	Availability of e-assessment to be performed at the scheduled time and during the time period	68(79.07%)	18(20.93%)	96(84.21%)	18(15.79%)	0.349
2	Authorship/data integrity	30(34.88%)	56(65.12%)	38(33.33%)	76(66.67%)	0.819
3	Improving Identification- students are who they say they are when performing evaluation activities	54(62.79%)	32(37.21%)	82(71.93%)	32(28.07%)	0.170
4	Confidentiality/access control: Students only access e-assessments specifically prepared for them	66(76.74%)	20(23.26%)	92(80.70%)	22(19.30%)	0.496
5	Confidentiality/access control: tutors only access e-assessments following the established evaluation process	66(76.74%)	20(23.26%)	100(87.72%)	14(12.28%)	0.41
6	Non repudiation: protection against false denial of involvement in e-assessments	12(13.95%)	74(86.05%)	26(22.81%)	88(77.19%)	0.114
7	Training of digital assessment operators	72(83.73%)	14(16.28%)	98(85.96%)	16(14.04%)	0.660
8	Installing anti-virus software	78(90.70%)	8(9.30%)	100(87.72%)	14(12.28%)	0.505
	Total	**446(64.83%)**	**242(35.17%)**	**632(69.30%)**	**280(30.70%)**	

In Table 3 is revealed that the greater percentage of lecturers from both genders have heard about the security protection measures in digital assessment in higher institutions listed. The security protection measure in digital assessment with the least percentage awareness from male and female lecturers is non-repudiation: the protection against false denial of involvement in e-assessments. In total more of the female lecturers (69.30%) than the male lecturers (64.83%) are aware of the security protection measures in digital assessment.

The observed variance in lecturers' percentage awareness of the security protection measures in digital assessment based on gender is not significant since χ^2 values for all the items at 0.05 significance level with degree of freedom of 1 is greater than 0.05 ($P > 0.05$; $df = 1$). The null hypothesis which states that there is no significant difference between male and female lecturers' awareness of the security protection measures in digital assessment is then accepted.

Research question 4, and hypothesis 4:
What is the percentage awareness of security protection measures in digital assessment depending on lecturers' cadre?

The lecturers' perceived awareness of the security threats in digital assessment in higher institutions did not significantly vary based on cadre. In Table 4 is presented the frequency, percentage and chi-square of the lecturers' awareness of the security protection measures in digital assessment in higher institutions based on cadre.

Table 4: Lecturers' Awareness of the Protection Measures in Digital Assessment in Higher Institutions Based on Cadre

S/N	Have you ever heard of these security protection measures in digital assessment?	Non-Professorial (N= 148)		Professorial (N=52)		
		Frequency of yes	Frequency of No	Frequency of yes	Frequency of No	Chi-square p-value l
1	Availability of e-assessment to be performed at the scheduled time and during the time period	60(40.54%)	88(59.46%)	8(15.38%)	44(84.62%)	0.001
2	Authorship/data integrity	120(81.08%)	28(18.92%)	44(84.62%)	8(15.38%)	0.568
3	Improving Identification- students are who they say they are when performing evaluation activities	96(64.86%)	52(35.14%)	40(76.92%)	12(23.08%)	0.109
4	Confidentiality/access control: Students only access e-assessments specifically prepared for them	114(77.03%)	34(22.97%)	44(84.62%)	8(15.38%)	0.248
5	Confidentiality/access control: tutors only access e-assessments following the established evaluation process	120(81.08%)	28(18.92%)	46(88.46%)	6(11.54%)	0.223
6	Non repudiation: protection against false denial of involvement in e-assessments	34(22.97%)	114(77.03%)	4(7.69%)	48(92.31%)	0.016
7	Training of digital assessment operators	126(85.14%)	22(14.86%)	44(84.62%)	8(15.38%)	0.928
8	Installing anti-virus software	134(90.54%)	14(9.46%)	44(84.62%)	8(15.38%)	0.240
	Total	**804(67.91%)**	**380(32.09%)**	**274(65.87%)**	**142(34.13%)**	

Field survey data (2024)

Table 4 reveals that least percentage of the lecturers in non-professorial and professorial cadre aware of the security protection measures in digital assessment mentioned are in items 1 and 6. The security protection measures with the highest percentage (90.54%) awareness from non-professorial lecturers is installing anti-virus software while confidentiality/access control - tutors only access e-assessments following

the established evaluation process have the highest percentage (88.46%) awareness from professorial lecturers. In total more of the non-professorial lecturers (67.91%) than the professorial lecturers (65.87%) are aware of the security protection measures in digital assessment.

The observed variance in lecturers' percentage of awareness of security protection measures in digital assessment based on cadre for items 1 and 6 is significant since χ^2 values for the items at 0.05 significance level with degree of freedom of 1 is less than 0.05 ($P > 0.05$; $df = 1$). Their null hypothesis which states that there is no significant difference between non-professorial and professorial lecturers' awareness of the security protection measures in digital assessment is then rejected. Since there still exist drawbacks which limit digital assessment potentials in collaborative learning activities despite being widely adopted in many educational institutions over the last decade (Marais et.al, n.d; Miguel et.al, 2015), it is good that lecturers of all cadres are aware of the security threats and protection measures in digital assessment. The lecturers can be on the lookout of these drawbacks.

Conclusion

Lecturers from non-professorial cadre showed comparatively more significant awareness of security threats and protection measures in digital assessment, but gender of the lecturers has no substantial influence on their awareness of security threats and protection measures in digital assessment. Giving proper consideration to this is necessary while offering digital assessment to students especially as digital learning and evaluation is widely used.

Recommendations

The following recommendations were made by the authors based on the study results;

1. The government and school authorities can provide adequate training opportunities that will educate the lecturers on the implementation of protection measures in digital assessment.
2. A further investigation on the extent protection measures in digital assessment reduces bias in digital assessment outcome.

REFERENCES

Algahtani, M. A. (2022). Cybersecurity awareness based on software and e-mail security with statistical analysis. *Computational Intelligence and Neuroscience*, 2022:6775980. doi: 10.1155/2022/6775980

Alharbi, T., & Tassaddiq, A. (2021) Assessment of cybersecurity awareness among students of Majmaah University. *Big Data Cogn. Comput*, 5(23). Retrieved from https://doi.org/ 10.3390/bdcc5020023

Al Rawashdeh, A. Z., Mohammed1, E. Y., Al Arab, A. R., Alara, M., & Al-Rawashdeh, B. (2021). Advantages and Disadvantages of Using e-Learning in University Education: Analyzing Students' Perspectives. *The Electronic Journal of e-Learning*, 19(2), 107-117. Retrieved from www.ejel.org

Bercy Infos Particulars (2023). *How to protect yourself against phishing?* https://www.economie.gouv.fr/particuliers/phishing-hameconnage-filoutage

Eleje, L. I., Metu, I. C., Ikwelle, A. C., Mbelede, N. G., Ezeugo, N. C., Ufearo, F. N., Okenwa-Fadele, I. A., & Ezenwosu, N. E. (2022). Influence of cyber-security problems in digital assessment on students' assessment outcome: lecturers' perspective. *Journal of Scientific Research & Reports*, *28*(10), 11-20. DOI: 10.9734/JSRR/2022/v28i1030551

Gutierrez, K. (2012). 18 Mind-blowing e-learning statistics you need to know. SH!FT Disruptive E-Learning: SHIFT's E-learning Blog, 29 November 2012. [Online]. Retrieved from http://info.shiftelearning.com/blog/bid/247473/18-Mind-BlowingeLearning-Statistics-You-Need-to-Know

Hamat, A., Embi, M. A., Hassan, H. (2012). The use of social networking sites among Malaysian university students. *International Education Studies,* 5(3), 56. DOI:10.5539/ies.v5n3p56

Marais, E., Argles, D., & Solms, B. V. (2006). *Security issues specific to E-assessments*. Retrieved from https://eprints.soton.ac.uk/261433/

Miguel, J., Caball´e, S., & Prieto, J. (2013). Providing information security to MOOC: Towards effective student authentication. In 5-th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2013), 2013; 289 – 292. DOI 10.1109/INCoS.2013.52 14.

Miguel, J., Caballe, S., Xhafa, F., & Prieto, J. (2015). Security in online web learning assessment providing an effective trustworthiness approach to support e-learning teams. *World Wide Web,* 18, 1655–1676. DOI: 10.1007/s11280-014-0320-2

Puttaswamy, K. P. N, Sala, A., & Zhao, B. Y. (2009). StarClique: guaranteeing user privacy in social networks against intersection attacks, in Proceedings of the 5th international conference on Emerging networking experiments and technologies, pp. 157-168, 2009.

Siddiqui, M. S., & Verma, D. (2011). Cross site request forgery: A common web application weakness. DOI: 10.1109/ICCSN.2011.6014783

Shonola, S.A., & Joy, M.S. (2014). Mobile learning security issues from lecturers' perspectives (Nigerian Universities Case Study)'. In 6th International Conference on Education and New Learning Technologies, 7-9 July, 2014, Barcelona, Spain. 2014; 88: 7081.

Siraj, M. M., Othman, S. H., & Garba, A. A. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *International Journal of Electrical and Engineering*, 12(1): 572-584. DOI:10.11591/ijece.v12i1.pp572-584