TSS
Trends in
Social Sciences

OPEN ACCESS

Gender and Academic-Level Variations in Awareness of Digital Assessment Security Risks and Safeguards among Nigerian Students

[1]Lydia I. Eleje, [1]Nneka C. Ezeugo, [1]Elizabeth I. Anierobi, [1]Chioma C. Akunaeme, [1]Victor U. Ezeonwumelu, [2]Ndidi L. Okeke and [3]George U. Eleje

[1]Department of Educational Foundations, Faculty of Education, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria

[2]Department of Educational Management and Policy, Faculty of Education, Nnamdi Azikiwe University, Awka, Anambra, Nigeria

[3]Department of Obstetrics and Gynecology, Faculty of Medicine, Nnamdi Azikiwe University, Awka, Anambra, Nigeria

ABSTRACT

Background and Objective: As digital assessments become increasingly prevalent in higher education, concerns about data security, academic integrity, and ethical technology use are rising. However, there is limited evidence on students' awareness of these risks, particularly in Nigerian higher institutions. This study aimed to examine students' understanding of digital assessment risks and their familiarity with security tools, with attention to differences by gender and academic level. **Materials and Methods:** A descriptive quantitative design was employed, involving 210 education students (61 males, 149 females; 114 undergraduates, 96 postgraduates) from public higher institutions in Anambra State, Nigeria. Data were collected using structured questionnaires based on digital literacy and security awareness frameworks. Descriptive statistics and comparative analyses were performed to explore variations across gender and academic level. **Results:** Students demonstrated high a wareness of common digital assessment risks, including malware, identity verification issues, and human error. Gender differences were minimal, with females showing slightly higher awareness. Undergraduates were more attuned to technical vulnerabilities, whereas postgraduates showed a stronger understanding of ethical issues such as plagiarism and impersonation. Familiarity was highest with antivirus tools, access controls, and identity validation, but lower for advanced safeguards such as non-repudiation and data authorship. **Conclusion:** The study highlights the need for targeted interventions to enhance digital assessment security: Technical training for undergraduates and ethical awareness for postgraduates. These findings provide evidence to inform policies and educational strategies that promote secure and responsible digital assessment practices in Nigeria, while suggesting directions for future research on improving digital literacy and ethical technology use among students.

KEYWORDS

Academic integrity, security-risk awareness, digital evaluations, gender differences, higher institution

ISSN: 3105-1340 (Online)
ISSN: 3105-1332 (Print)
https://doi.org/10.21124/tss.2026.14.23

Received: 08 Nov. 2025
Accepted: 02 Feb. 2026
Published: 10 Feb. 2026

INTRODUCTION

Digital assessment has become an essential component of contemporary university education due to its ability to enhance flexibility, reduce instructional costs, and expand access to learning resources. Through electronic learning (e-learning) platforms, higher education institutions are able to deliver instruction and assessment beyond traditional classroom boundaries using multimedia tools such as videos, simulations, and interactive content[1]. These platforms are supported by digital infrastructure, including computers, internet connectivity, and specialized software for managing academic content, assignments, and assessments[2], as well as communication tools that enable real-time feedback, discussion forums, and live lectures[3]. The rapid shift to online learning has prompted higher education institutions to invest in technologies that support student-centered learning. Studies indicate that digital instruction and assessment improve educational outcomes while reducing operational costs for both learners and institutions[4,5]. Students also benefit from being able to access learning materials at their convenience, which supports varied learning and assessment preferences and reduces scheduling conflicts[6]. Additionally, the use of web-based instructional tools in universities has expanded students' exposure to global knowledge systems and collaborative learning opportunities.

Despite these benefits, the growing reliance on digital assessment systems has raised significant security concerns. Online platforms store and transmit sensitive data such as examination content, grades, and personal student information, making them attractive targets for cybercriminal activities, including phishing, malware attacks, data breaches, and unauthorized access. The education and research sector has been identified as one of the most targeted globally, with an average of 2,314 cyberattacks per institution weekly[7]. These threats pose serious risks to data integrity, student privacy, and institutional reputation. Despite the increasing dependence on online platforms for instruction and assessment, many university students lack adequate awareness of security risks in digital assessment. Studies have shown that students often underestimate the importance of password management, data encryption, and secure browsing, leaving them exposed to threats like authentication issue, plagiarism issue, impersonation, espionage, and virus/malware attack[8,9]. Moreover, digital assessment security safeguards - installing anti-virus software, authorship, identification, and non-repudiation - while improving, are not always uniformly implemented or clearly communicated to students. Learning management systems (LMS) are often managed by institutional IT departments, which restrict user autonomy and make it difficult for students to customize their digital learning and assessment environment or secure their personal data independently[10,11].

The issue is particularly critical in low- and middle-income countries such as Nigeria, where digital infrastructure is still developing, and cybersecurity protocols are often weak or inconsistently implemented[12,13]. Although learning management systems typically include safeguards such as password protection, multi-factor authentication, encrypted communication, antivirus software, authorship verification, identification, and non-repudiation mechanisms, their effectiveness depends largely on student awareness and compliance[10]. Studies show that students frequently disable or avoid security features due to perceived inconvenience, highlighting a gap between the availability of safeguards and actual user behavior[14,15]. Furthermore, communication regarding these safeguards is often inadequate, with students rarely receiving updates or practical training on protecting their digital identities[16,17]. In Nigeria, limited digital literacy, insufficient orientation programs, and weak institutional communication further exacerbate students' exposure to security risks, particularly among younger undergraduates who are inexperienced with digital systems[18].

This study is guided by the Protection Motivation Theory (PMT), which explains how individuals' awareness of threats and perceived ability to adopt protective behaviors influence their security-related actions. The PMT provides a useful lens for understanding how students' perceptions of digital assessment risks and safeguards may affect their engagement with secure practices. Although existing studies suggest that demographic factors such as gender and academic level may influence cybersecurity awareness, findings emain inconsistent, and there is a notable paucity of research focusing specifically on students' awareness of security risks and safeguards in digital assessments within the Nigerian higher education context[13]. Addressing this gap is essential for informing targeted interventions.

Therefore, the present study investigates Nigerian university students' awareness of security risks and safeguards associated with digital assessment, with particular attention to differences based on gender and academic level. By identifying gaps in awareness and preparedness, the study aims to provide evidence-based insights that can support institutional strategies for improving digital literacy, strengthening cybersecurity awareness, and promoting safer engagement with e-learning and digital assessment platforms.

MATERIALS AND METHODS

Study area: The study was conducted in Anambra State, located in the Southeastern Region of Nigeria. Anambra State is one of the major educational hubs in the region, hosting several government-owned, degree-awarding tertiary institutions that offer education-related programs. The choice of Anambra State as the study area was considered appropriate because most of the researchers reside within the state, which facilitated access to participants and data collection. In addition, to the best of the researchers' knowledge, no previous empirical study has specifically examined students' awareness of security risks and safeguards in digital assessment within this geographical context, thereby justifying the relevance of the area.

The study was carried out during the 2023/2024 academic session, which spanned from September, 2023 to August, 2024. This period was selected to ensure that participants had adequate exposure to digital assessment platforms during an active academic cycle. The population of the study comprised students in the education discipline drawn from government-owned, degree-awarding tertiary institutions in Anambra State, Nigeria.

This study investigated students' awareness of security risks and safeguards in digital assessments within higher education institutions in Anambra State, Nigeria. The objective was to determine how students perceive security risks and safeguards in digital assessment platforms, and to examine whether these perceptions differ by gender or level of study. To guide this investigation, the following research questions were proposed:

- What is the level of awareness among higher education students regarding security risks in digital assessments?
- What safeguards are students aware of in digital assessments?
- Are there differences in awareness based on gender or level of study (undergraduate vs. postgraduate)?

Based on these questions, the following hypotheses were tested:

- **H_o1:** There is no significant difference between male and female students' awareness of security risks in digital assessments
- **H_o2:** There is no significant difference between undergraduate and postgraduate students' awareness of security risks in digital assessments
- **H_o3:** There is no significant difference between male and female students' awareness of safeguards in digital assessments
- **H_o4:** Students' awareness of safeguards in digital assessments does not significantly vary by level of study

Research design: A descriptive quantitative research design was adopted for this investigation. This approach was selected because it allows for the collection of numerical data from a defined population, enabling the researchers to quantify students' awareness and compare responses across defined categories such as gender and academic level. The use of descriptive statistics, along with hypothesis testing, supports clear analysis of trends and relationships in the data.

Study population and sampling: The target population consisted of students enrolled in education-related programs at public, degree-granting higher education institutions in Anambra State, Nigeria. A purposive sampling technique was employed to select a total of 210 students, comprising 61 males and 149 females, and 114 undergraduates and 96 postgraduates. The selection criteria ensured the inclusion of students who had been exposed to digital assessment systems at their respective institutions. The purposive sampling approach was necessary to gather responses specifically from students with direct experience in digital assessments.

Instrumentation: Data were collected using a self-constructed and validated questionnaire. The instrument was designed to assess students' awareness of both security risks and the safeguards implemented in digital assessments. The questionnaire was divided into three main sections:

- Section A captured demographic data, including gender and academic level
- Section B contained ten structured items related to awareness of security risks
- Section C consisted of eight structured items related to awareness of digital security safeguards. These items were presented on an alternative response form, with response options of yes or no

The questionnaire development process began with a review of literature and identification of key themes around security risks such as unauthorized access, cheating, data breaches, and awareness of institutional safeguards like authentication, encryption, and secure platforms. To establish content validity, the initial items were reviewed by experts in educational technology, measurement, and evaluation. Following expert input, a pilot test was conducted with 20 students who were not part of the final sample. Feedback from the pilot informed minor adjustments in wording for clarity. Internal consistency reliability was measured using Cronbach's alpha, which confirmed that the instrument produced reliable results for the two main constructs: awareness of security risks and awareness of safeguards.

Data collection procedure: Data collection was conducted through both electronic and printed questionnaires, allowing students to choose their preferred mode of response. This ensured higher participation and accommodated varying levels of internet access among students. Informed consent was obtained from all participants, and anonymity was maintained throughout the study.

Data analysis: Collected data were coded and analyzed using descriptive and inferential statistics. Descriptive statistics such as frequencies and percentages were calculated to determine the general level of awareness among students. To test the stated hypotheses, chi-square tests were conducted. These tests were used to examine:

- Differences in awareness of security risks between male and female students (H_o1)
- Differences in awareness of risks between undergraduate and postgraduate students (H_o2)
- Differences in awareness of safeguards between male and female students (H_o3)
- Differences in awareness of safeguards based on level of study (H_o4)

All analyses were conducted using SPSS software, and results were interpreted at a significance level of $p<0.05$.

Ethical statement: Ethical approval for this study was obtained from the Anambra State Ministry of Health Research Ethics Committee (ASMOHREC), with approval reference number ASMOHREC/2024/04112024/25. Additional administrative permission was granted by the Anambra State Ministry of Education, the Local Government Education Commission, and the Heads of Department of the participating education faculties in the selected government-owned, degree-awarding tertiary institutions.

All participants were adequately informed about the purpose of the study, the voluntary nature of their participation, and their right to withdraw at any stage without any consequences. Informed consent was obtained from all respondents before data collection. To ensure confidentiality and anonymity, no personally identifiable information, such as names or registration numbers, was collected. Data were used strictly for research purposes, securely stored, and accessible only to the researchers. These measures were implemented in line with established ethical standards for research involving human participants.

RESULTS

In Table 1 the frequency count, percentage, and chi-square of the students' awareness of the security risk in digital assessment in higher institutions based on gender. The data shows that students, particularly females, reported high awareness of various security risks in digital assessments, with the greatest awareness seen in issues like human error, verification problems, and malware attacks. Although female students consistently reported higher awareness across all categories, chi-square tests revealed that none of these gender differences were statistically significant. Therefore, while gender-based differences in awareness exist descriptively, they do not have a meaningful statistical impact in this sample.

The frequency count, percentage and chi-square of the students' awareness of the security risk in digital assessment in higher institutions based on student level (undergraduate and post graduate) are displayed in Table 2. Table 2 compares undergraduate and postgraduate students' awareness of various security risks in digital assessments, revealing several statistically significant differences using chi-square tests. Undergraduates showed higher awareness of technical threats like malware and authentication

Table 1: Awareness of security risk in digital assessment by students' gender

Have you ever heard of these security risks in digital assessment?	Response	Male count	Female count	Total count	Total Male (%)	Total Female (%)	Total (%)	Chi-square p-value
Virus/malware attack	Yes	45	117	162	21.4	55.7	77.1	0.456
	No	16	32	48	7.6	15.2	22.9	
Exploiting security breach/privacy	Yes	30	79	109	14.3	37.6	51.9	0.613
	No	31	70	101	14.8	33.3	48.1	
Data/result interference	Yes	43	104	147	20.5	49.5	70.0	0.921
	No	18	45	63	8.6	21.4	30.0	
Unauthorized access	Yes	43	107	150	20.5	51.0	71.4	0.848
	No	18	42	60	8.6	20.0	28.6	
Verification/authentication issue	Yes	52	118	170	24.8	56.2	81.0	0.311
	No	9	31	40	4.3	14.8	19.0	
Plagiarism issue	Yes	30	86	116	14.3	41.0	55.2	0.259
	No	31	63	94	14.8	30.0	44.8	
Impersonation	Yes	37	89	126	17.6	42.4	60.0	0,901
	No	24	60	84	11.4	28.6	40.0	
Espionage (illegal info)	Yes	28	70	98	13.3	33.3	46.7	0.887
	No	33	79	112	15.7	37.6	53.3	
Technical software issues	Yes	52	112	164	24.8	53.3	78.1	0.109
	No	9	37	46	4.3	17.6	21.9	
Human error/failure	Yes	55	123	178	26.3	58.9	85.2	0.192
	No	6	25	31	2.9	12.0	14.8	

Table 2: Awareness of security risk in digital assessment by students' level

Have you ever heard of these security risks in digital assessment?	Response	UG count	PG count	Total count	Total UG (%)	Total PG (%)	Total (%)	Chi-square p-value
Virus/malware attack	Yes	100	62	162	47.6	29.5	77.1	0.00
	No	14	34	48	6.7	16.2	22.9	
Exploiting security breach/privacy	Yes	48	61	109	22.9	29.0	51.9	0.02
	No	66	35	101	31.4	16.7	48.1	
Data/result interference for malicious acts	Yes	87	60	147	41.4	28.6	70.0	0.30
	No	27	36	63	12.9	17.1	30.0	
Unauthorized access to assessment contents	Yes	92	58	150	43.8	27.6	71.4	0.01
	No	22	38	60	10.5	18.1	28.6	
Verification/authentication issue	Yes	103	67	170	49.0	31.9	81.0	0.00
	No	11	29	40	5.2	13.8	19.0	
Plagiarism issue	Yes	49	67	116	43.0	69.8	46.7	0.00
	No	65	29	94	57.0	30.2	53.3	
Impersonation	Yes	58	68	126	27.6	32.4	60.0	0.003
	No	56	28	84	26.7	13.3	40.0	
Espionage: Illegal equipment/information	Yes	43	55	98	20.5	26.2	46.7	0.005
	No	71	41	112	33.8	19.5	53.3	
Technical software failures/errors (e.g., coding issues)	Yes	96	68	164	45.7	32.4	78.1	0.20
	No	18	28	46	8.6	13.3	21.9	
Acts of human error/failure (accidents, mistakes)	Yes	101	77	178	48.3	36.8	85.2	0.127
	No	13	18	31	6.2	8.6	14.8	

UG: Under graduate and PG: Post graduate

Table 3: Awareness of safeguards in digital assessment by gender

Have your ever heard of these security risks in digital assessment?	Response	Male count	Female count	Total count	Total Male (%)	Total Female (%)	Total (%)	Chi-square p-value
Availability at the scheduled time	Yes	54	109	163	25.7	51.9	77.6	0.247
	No	7	40	47	3.3	19.0	22.4	
Authorship/data integrity	Yes	17	39	56	8.1	18.6	26.7	0.910
	No	44	110	154	21.0	52.4	73.3	
Identification (student identity validation)	Yes	49	120	169	23.3	57.1	80.5	0.542
	No	12	29	41	5.7	13.8	19.5	
Confidentiality (students only access their own assessments)	Yes	54	123	177	25.7	58.6	84.3	0.466
	No	7	26	33	3.3	12.4	15.7	
Confidentiality (tutors follow protocol for access)	Yes	51	109	160	24.3	51.9	76.2	0.210
	No	10	40	50	4.8	19.0	23.8	
Non-repudiation (protection from false denial)	Yes	14	29	43	6.7	13.8	20.5	0.136
	No	47	120	167	22.4	57.1	79.5	
Training of digital assessment operators	Yes	53	123	176	25.2	58.6	83.8	0.838
	No	8	26	34	3.8	12.4	16.2	
Installing anti-virus software	Yes	58	127	185	27.6	60.5	88.1	0.051
	No	3	22	25	1.4	10.5	11.9	

issues, while postgraduates were more aware of academic integrity concerns such as plagiarism, impersonation, and espionage. These findings suggest that awareness levels vary by education level, though not consistently across all types of risks.

Table 3 compares male and female students' awareness of the various security safeguards in digital assessment in higher institutions. The frequency count, percentage and chi-square results displayed in Table 3 shows that, while female students consistently reported higher awareness of digital assessment safeguards than male students, none of the gender differences were statistically significant. The only exception approaching significance was awareness of installing anti-virus software (p = 0.051). Overall awareness was highest for safeguards like anti-virus software (88.1%), identification (80.5%), and confidentiality of student access (84.3%). The lowest awareness was observed for non-repudiation (20.5%) and authorship/data integrity (26.7%).

Table 4: Awareness of safeguards in digital assessment by students' level

Have you ever heard of these security risks in digital assessment?	Response	UG count	PG count	Total count	Total UG (%)	Total PG (%)	Total (%)	Chi-square p-value
Availability at scheduled time	Yes	85	78	163	40.5	37.1	77.6	0.150
	No	29	18	47	13.8	8.6	22.4	
Authorship/data integrity	Yes	25	31	56	11.9	14.8	26.7	0.801
	No	89	65	154	42.4	31.0	73.3	
Identification (validating student identity)	Yes	90	79	169	42.9	37.6	80.5	0.972
	No	24	17	41	11.4	8.1	19.5	
Confidentiality (students access only their assessments)	Yes	98	79	177	46.7	37.6	84.3	0.280
	No	16	17	33	7.6	8.1	15.7	
Confidentiality (tutors access following process)	Yes	83	77	160	39.5	36.7	76.2	0.106
	No	31	19	50	14.8	9.0	23.8	
Non-repudiation (no false denial of involvement)	Yes	19	24	43	9.0	11.4	20.5	0.570
	No	95	72	167	45.2	34.3	79.5	
Training of digital assessment operators	Yes	95	81	176	45.2	38.6	83.8	0.439
	No	19	15	34	9.0	7.1	16.2	
Installing anti-virus software	Yes	105	80	185	50.0	38.1	88.1	0.045
	No	9	16	25	4.3	7.6	11.9	

UG: Under graduate and PG: Post graduate

Table 4 portray the frequency count, percentage, and chi-square of the undergraduate and postgraduate students' awareness of the safeguards in digital assessment in higher institutions. The Table 4 results show that undergraduate students generally reported higher awareness of digital assessment safeguards compared to postgraduates. However, the only statistically significant difference was in awareness of installing anti-virus software (p = 0.045), where 50% of undergraduates were aware versus 38.1% of postgraduates. For all other safeguards, awareness levels were similar across both groups, with no significant differences. The lowest awareness for both groups was in the area of non-repudiation, with only 20.5% overall awareness.

DISCUSSION

The results of this study contribute to a clearer understanding of students' awareness of security risks and safeguards in digital assessments in higher education. The analysis, organized by gender and academic level, reveals descriptive trends in awareness and identifies statistically significant differences that can inform institutional strategies to improve digital assessment security. Table 1 addresses awareness of digital assessment security risks across gender. Female students reported higher levels of awareness in all categories, including human error, verification issues, and malware attacks. Despite these descriptive differences, none of the results reached statistical significance based on the chi-square tests. These findings support the null hypothesis (H_o1) that gender does not significantly influence students' awareness of digital assessment risks. Although females appear more informed, the lack of statistical significance indicates that the variation could be due to chance rather than a meaningful difference in awareness. This suggests that awareness-building interventions may not need to be gender-targeted but should instead focus on the general student population. This aligns with previous research indicating that while females often exhibit higher cybersecurity awareness, such differences may not always reach statistical significance[9-16].

In contrast, when differences based on academic level was examined, comparing undergraduate and postgraduate students. The results demonstrated statistically significant differences in certain categories. Undergraduates showed greater awareness of technical risks such as malware and authentication issues, likely reflecting their greater interaction with platform functionality and security features. Meanwhile, postgraduates were more attuned to academic integrity concerns, including plagiarism and impersonation. These differences indicate that academic level influences the types of security risks students are more likely to be aware of. This supports the rejection of the null hypothesis (H_o2), suggesting that educational interventions may need to be tailored according to the student's academic level. This finding supports the notion that awareness of security risks evolves with level of knowledge or academic progression, as students encounter more complex digital environments and ethical dilemmas[13]. For example, undergraduates might benefit more from training on data protection and phishing, while postgraduates may need support in understanding the consequences of academic misconduct in digital settings.

Table 3 focused on awareness of digital safeguards by gender. Again, female students reported higher awareness across all categories, with the highest awareness levels seen in antivirus installation, user identification, and access confidentiality. However, none of these differences were statistically significant, except for antivirus awareness, which approached significance (p = 0.051). These findings support the null hypothesis (H_o3), confirming that gender-based differences in safeguard awareness are not statistically meaningful in this sample. This suggests that while females may be more attuned to certain safeguards, the differences are not substantial enough to warrant gender-specific interventions[9,16]. Nonetheless, the consistent pattern of females reporting higher awareness may suggest a slight tendency toward greater caution or familiarity with preventive measures. Institutions may choose to maintain gender-neutral training strategies but should remain attentive to potential engagement differences that could emerge in larger or more diverse samples.

Table 4 presents data on safeguard awareness by academic level. Unlike gender-based findings, one statistically significant difference emerged: A higher proportion of undergraduates (50%) were aware of antivirus software compared to postgraduates (38.1%), with a p-value of 0.045. This leads to the rejection of the null hypothesis (H_o4). For all other safeguards, awareness was generally similar between groups, indicating that significant level-based differences in awareness are not widespread. Nonetheless, the observed difference in antivirus awareness may reflect more recent exposure to basic digital safety training among undergraduates or institutional orientation sessions emphasizing such topics. This suggests that postgraduate students, despite their academic maturity, may require reinforcement of basic security practices, especially if their prior exposure occurred before the expansion of digital platforms[8].

Across all groups, the overall awareness of certain safeguards such as non-repudiation (20.5%) and authorship/data integrity (26.7%) remained low. These are technical areas of security often less familiar to users without a background in information security or computer science. The low awareness rates signal a critical gap in student knowledge, irrespective of gender or academic level. Institutions must address these gaps by integrating digital security content into mandatory orientation or digital literacy programs. According to a study, student misconceptions about cybersecurity are often tied to limited exposure to technical concepts[19]. Addressing this knowledge shortfall could reduce institutional vulnerability to both external attacks and internal breaches caused by user negligence[20]. While gender-based differences in awareness exist descriptively, they are not statistically significant. In contrast, academic level influences awareness in both risk and safeguard categories, with undergraduates and postgraduates showing different strengths. These findings emphasize the importance of tailoring security training to students' needs based on academic progression while also ensuring that all students receive foundational cybersecurity education.

Implications for practice and policy:

- Curriculum designers should embed digital security and assessment ethics modules tailored to students’ academic levels
- Policy makers in higher education could mandate regular digital assessment security training to enhance institutional integrity
- Course leaders may improve assessment integrity by aligning safeguards with students’ awareness levels

- Instructional designers should differentiate technical and ethical content in digital assessment platforms
- University administrators can reduce risks by promoting awareness of advanced safeguards like non-repudiation and authorship verification

CONCLUSION

This study emphasizes the need for targeted cybersecurity education in higher education, particularly in relation to students' academic levels. While female students showed higher awareness of security risks and safeguards in descriptive terms, these differences were not statistically significant, suggesting that awareness initiatives should address the entire student population rather than focusing on gender-specific interventions. In contrast, academic level significantly influenced awareness patterns: Undergraduates were more attuned to technical threats, whereas postgraduates demonstrated greater awareness of academic integrity issues such as plagiarism and impersonation. The overall low awareness of certain safeguards particularly non-repudiation and data authorship points to the need for more inclusive cybersecurity training that addresses both technical and ethical aspects. Institutions should implement practical, level-specific training to strengthen student knowledge and promote a safer digital assessment environment.

SIGNIFICANCE STATEMENT

This study discovered the patterns of students' awareness of digital assessment risks and security tool familiarity across gender and academic levels, which can be beneficial for higher education institutions, policymakers, and instructional designers seeking to strengthen secure digital assessment practices. By highlighting gaps in advanced security and ethical safeguards, the findings inform targeted training and policy formulation. This study will help researchers to uncover the critical areas of digital literacy, ethical technology use, and assessment security that many researchers were not able to explore. Thus, a new theory on differentiated digital assessment preparedness may be arrived at.

REFERENCES

1. Arkorful, V. and N. Abaidoo, 2014. The role of e-learning, the advantages and disadvantages of its adoption in higher education. Int. J. Educ. Res., 2: 397-410.
2. Luaran, J.E., N.N. Samsuri, F.A. Nadzri and K.B.M. Rom, 2014. A study on the student's perspective on the effectiveness of using e-learning. Procedia Social Behav. Sci., 123: 139-144.
3. Kattoua, T., M. Al-Lozi and A. Alrowwad, 2016. A review of literature on e-learning systems in higher education. Int. J. Bus. Manage. Econ. Res., 7: 754-762.
4. Nurul Islam, M. Beer and F. Slack, 2015. E-learning challenges faced by academics in higher education: A literature review. J. Educ. Training Stud., 3: 102-112.
5. Songkram, N., 2015. E-learning system in virtual learning environment to develop creative thinking for learners in higher education. Procedia Soc. Behav. Sci., 174: 674-679.
6. Aparicio, M., F. Bacao and T. Oliveira, 2016. An e-learning theoretical framework. Educ. Technol. Soc., 19: 292-307.
7. Afolalu, O. and M.S. Tsoeu, 2025. Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. Future Internet, Vol. 17. 10.3390/fi17120575.
8. Ahamed, B., M.R.H. Polas, A.I. Kabir, A.S.M. Sohel-Uz-Zaman, A. Al Fahad, S. Chowdhury and M.R. Dey, 2024. Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era. Sage Open, Vol. 14. 10.1177/21582440241228920.
9. Eleje, L.I., O.I. Ikwuka, I.C. Metu, N.C. Ezeugo, C.C. Abanobi and N.G. Mbelede, 2025. Lecturers' awareness of security threats and protection measures in digital assessment in higher institutions in Anambra State, Nigeria. Afr. J. Educ. Manage. Teach. Entrepreneurship Stud., 14: 329-339.
10. Sarrab, M., L. Elgamel and H. Aldabbas, 2012. Mobile learning (M-learning) and educational environments. Int. J. Distrib. Parallel Syst., 3: 31-38.

11. Adeshola, I. and D.I. Oluwajana, 2025. Assessing cybersecurity awareness among university students: Implications for educational interventions. J. Comput. Educ., 12: 1283-1305.
12. Yaseen, K.A.Y., 2022. Importance of cybersecurity in the higher education sector 2022. Asian J. Comput. Sci. Technol., 11: 20-24.
13. Altarawneh, M.H.M., A. Althunibat, M.H. Almajali and N. Alzriqat and S. Alazzam, 2025. Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps. Int. J. Innovative Res. Sci. Stud., 8: 1516-1529.
14. Ibrahim, M., 2024. 10 benefits of multi-factor authentication (MFA). SuperTokens.
15. Magunje, C. and W. Chigona, 2024. Perceptions of school management on cyber threats: The case of resource-constrained schools in South Africa. EPiC Ser. Educ. Sci., 6: 53-39.
16. Guo, H. and H. Tınmaz, 2023. A survey on college students' cybersecurity awareness and education from the perspective of China. J. Educ. Gifted Young Sci., 11: 351-367.
17. Aljohni, W., N. Elfadil, M. Jarajreh and M. Gasmelsied, 2021. Cybersecurity awareness level: The case of Saudi Arabia university students. Int. J. Adv. Comput. Sci. Appl., 12: 276-281.
18. Eleje, L.I., I.C. Metu, A.C. Ikwelle, N.G. Mbelede and N.C. Ezeugo *et al*., 2022. Influence of cyber-security problems in digital assessment on students' assessment outcome: Lecturers' perspective. J. Sci. Res. Rep., 28: 11-20.
19. Thompson, J.D., G.L. Herman, T. Scheponik, L. Oliva and A. Sherman *et al*., 2018. Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. J. Cybersecur. Educ. Res. Pract., Vol. 2018. 10.62915/2472-2707.1030.
20. Hakimi, A.A. and M.F. Zolkipli, 2024. An awareness of cybersecurity risk assessment and management among students. Borneo Int. J., 7: 22-27.