AMERICAN JOURNAL OF ICT AND INNOVATION (AJICTI)

VOLUME 1 ISSUE 1 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of ICT and Innovation (AJICTI)
Volume 1 Issue 1, Year 2026
https://journals.e-palli.com/home/index.php/ajicti

Utilisation of Cybersecurity Applications as Predictors of Secure Digital Learning Among Computer Science Undergraduates in Public and Private Universities in Enugu State, Nigeria

Adesegun Nurudeen Osijirin[1]*, Leonard C. Anigbo[2], Oliver Okechukwu[2]

Article Information

Received: April 11, 2026
Accepted: June 23, 2026
Published: August 03, 2026

Keywords
Computer Science Undergraduates, Cybersecurity Applications, Digital Learning Platforms, Firewall Technologies, Secure Digital Learning, Virtual Private Networks (Vpns)

ABSTRACT

The study compared cyber security apps for the protection of digital learning platforms among computer science undergraduates at public and private universities in Enugu State, Nigeria. The study particularly focused on the variations in the use of antivirus software, firewall technologies and Virtual Private Network (VPN) technologies and their predicted impact on secure digital learning. Comparative descriptive survey research design was employed. The study population was 4416 (computer science undergraduate students) from which a sample of 393 respondents was selected by using multi-stage selection process. However, out of the 393 questionnaires administered, only 364 were successfully recovered and used for analysis (93% response rate). Data collection was conducted through the Cybersecurity Application Utilisation for Safeguarding Digital Learning Platforms Questionnaire (CAUSDLPQ). The Cronbach's Alpha reliability coefficient of the instrument was 0.75 overall. Data were examined using mean, standard deviation, independent-samples t-test and multiple regression analysis. The results showed that the undergraduates in both public and private institutions used antivirus software, firewall technologies, and VPN technologies to a low degree for the protection of digital learning platforms. However, the data showed significantly greater levels of usage of cyber security applications among undergraduates in private universities than their counterparts in public universities across all categories of cyber security applications. The results also indicated that cybersecurity apps were major predictors of secure digital learning with antivirus software being the top predictor followed by firewall technologies and VPN technologies. The study indicated that cybersecurity applications contribute greatly to secure digital learning but are not adequately used by university undergraduates. The study recommended the enhancement of cybersecurity awareness and practical training programs, the enhancement of effective utilization of cybersecurity applications, the incorporation of cybersecurity education in university curricula, and the enhancement of institutional cybersecurity infrastructure to enhance secure digital learning environments in higher education institutions.

INTRODUCTION

The rapid development of digital technologies has changed the landscape of higher education worldwide. Universities are turning to digital learning platforms such as Learning Management Systems (LMS), virtual classrooms, institutional portals, cloud-based educational services, e-assessment systems, video conferencing tools and mobile learning applications more and more to support teaching, learning, research and academic administration. The COVID-19 epidemic has further expedited the broad deployment of these technologies as educational institutions globally were forced to employ remote and hybrid learning methods to maintain continuity of education (UNESCO, 2021). Digital learning environments are, therefore, essential components of higher education nowadays.

Digital learning technologies provide a number of advantages including enhanced accessibility, flexibility, collaboration and continuity of learning. But as they have become more dependent on internet-enabled teaching systems, universities have also become more vulnerable to cyber-security attacks. Open network architectures, decentralised information systems, big user populations and large stores of sensitive academic and personal data make higher education institutions appealing targets for hackers (Ulven & Wangen, 2021). Cybersecurity problems such as phishing attacks, ransomware, malware infections, credential thefts, identity compromise, denial-of-service assaults, and unauthorized access to institutional systems are increasingly faced by universities (ENISA, 2023). These dangers provide substantial concerns to academic records, research data, institutional operations and the digital identities of undergraduates.

To address these difficulties, cybersecurity has become a fundamental necessity for sustaining secure and robust digital learning environments. According to the National Institute of Standards and Technology (NIST, 2020), cybersecurity is the protection of information systems and digital assets to assure confidentiality, integrity and availability of information. Effective cybersecurity in higher education is not only about technological infrastructure but also about security behaviours of users and use of cybersecurity solutions that are meant to secure digital learning activities.

[1] Department of Healthcare Management, Federal University of Allied Health Sciences, Enugu, Nigeria
[2] Department of Mathematics and Computer Science Education, Enugu State University of Science and Technology, Nigeria
* Corresponding author's email: adesegunosijirin@fuahse.edu.ng

Cybersecurity apps are important technology measures that assist secure online learning settings against cyber threats. Such programs include antivirus software, firewalls, and Virtual Private Networks (VPNs). These technologies are important to protect against cyberattacks, protect academic material, improve access control, enhance online privacy, and provide secure participation in online learning activities (Alshaikh, 2020; CISA, 2023). Therefore, the efficient use of these applications is essential for the security and sustainability of digital learning platforms in institutions.

Thus, despite growing relevance of cybersecurity in higher education, there may be considerable differences in cybersecurity readiness and technological capabilities of universities. Nigerian public and private universities differ significantly in terms of their financial systems, digital infrastructure, internet access, institutional technology support and investment in information and communication technologies. The public universities are sometimes challenged by low financing, lack of infrastructure, limited bandwidth for the Internet and crowded ICT facilities that might affect the effective deployment and use of the cybersecurity technology. On the other hand, private universities are frequently more flexible in their technology investments, have stronger institutional support systems and more robust digital infrastructures, owing to competitive pressures and comparatively smaller student bodies.

Institutional variations could impact undergraduates' cybersecurity practices and use of cybersecurity applications in digital learning settings. The Nigerian National Digital Learning Policy acknowledges the necessity of digital infrastructure, institutional support and technology-enabled learning environments for safe and effective digital education. Therefore, analysing differences in cybersecurity application use between university ownership categories is vital for improving the cybersecurity resilience of institutions and protecting digital learning systems.

Research has shown that cybersecurity practices are affected by several factors, including institutional support, digital literacy, understanding about cybersecurity, and technological infrastructure. Bada, Sasse and Nurse (2019) found that cybersecurity awareness programs may not always be translated into genuine protective cybersecurity behaviour, implying that consumers may be informed but not regularly practise good cybersecurity. Similarly, Alharbi and Tassaddiq (2021) showed that university undergraduates demonstrated moderate understanding of cybersecurity but little engagement in the practical use of cybersecurity technologies. Recent research from Nigeria also reveals that undergraduates may have a relatively high level of cybersecurity awareness but yet show variations in the implementation of preventative cybersecurity behaviours (Osijirin *et al.*, 2026a). This implies that awareness does not necessarily transfer into effective cybersecurity behaviour.

Previous studies have explored cybersecurity awareness, digital literacy, online safety practices and technology adoption in educational contexts. Nevertheless, empirical evidence on institutional differences in the use of cybersecurity applications among university undergraduates is hardly available. Existing research have mostly focused on knowledge and vulnerabilities rather than real use of cybersecurity technologies supporting secure digital learning. Little is also known regarding whether undergraduates in public and private institutions differ significantly in their usage of cybersecurity applications for the protecting of digital learning platforms.

This knowledge gap is especially significant in Enugu State, Nigeria, where public and private universities are increasingly relying on digital learning tools for academic activity. Understanding differences in the use of cybersecurity applications between institutions can help educational policy makers, university administrators, ICT units and cybersecurity professionals to improve the security of digital learning and the institution's cyber resilience.

Against this backdrop, this study comparatively assessed the utilisation of cybersecurity applications for safeguarding digital learning platforms among undergraduates in public and private universities in Enugu State, Nigeria.

MATERIALS AND METHODS

The study employed a comparative descriptive survey research approach. The study was designed to find out the difference in the use of cyber security software for the protection of digital learning platforms among Computer Science undergraduates of public and private universities in Enugu State, Nigeria. Descriptive survey research designs are appropriate for studies that collect quantitative data to describe, compare and analyse patterns of behaviour, attitudes and practices in a population (Creswell & Creswell, 2018). The approach was chosen properly as it enabled the researcher to assess the use of cybersecurity applications among Computer Science undergraduates in public and private universities and find out the predictive influence of cybersecurity applications on secure digital learning . The study was carried out in Enugu State, South-East geopolitical zone, Nigeria. The state has a number of public and private universities which are actively incorporating digital learning technology in teaching, learning, assessment and academic administration. These universities are progressively employing Learning Management Systems (LMS), institutional portals, virtual classrooms, cloud-based learning technologies and internet-enabled communication platforms to assist academic activities. The study area, Enugu State, was a good place for the investigation of utilisation of cybersecurity applications in digital learning environments because of the increasing use of digital learning technologies in the institutions in Enugu State. The study population comprised 4,416 undergraduate students of Computer Science in the

universities in Enugu State. The reason why we chose undergraduate computer science students is because they are often users of digital learning platforms, Internet-based academic systems, cybersecurity technologies and online instructional materials. Their experience and knowledge of digital systems and technology positioned them well to provide informed answers concerning the usage of cybersecurity applications to protect digital learning platforms. The sample size for the study was 393 and a multi-stage sampling technique was adopted. In the first stage, simple random sampling was used to select four universities offering accredited Computer Science curricula. In the second stage, proportional selection was employed to choose 10% of the Computer Science undergraduate population of each selected university. The sampling procedure also contributed to increase the representativeness of the sample and to eliminate sampling bias. Data were collected with an instrument devised by the researchers called "Cybersecurity Application Utilisation for Safeguarding Digital Learning Platforms Questionnaire (CAUSDLPQ)". The instrument was prepared in line with the study objectives and the pertinent literature on cybersecurity applications and safe digital learning. The questionnaire was in two parts. Section A asked respondents to provide demographic data and Section B addressed questions related to antivirus software, firewalls, Virtual Private Networks (VPNs), and secure digital learning.

The instrument was face validated by three experts, two of whom were in Computer Science and one in Measurement and Evaluation. The first draft of the instrument, with 60 items, was submitted to the validators, along with the objectives of the study, the research questions and the hypotheses. The adequacy of coverage of topics, clarity of statements, suitability of items and their agreement with research objectives were evaluated by the experts. Comments, recommendations and revisions were incorporated into the final version of the instrument before administration.

The instrument reliability was established using a pilot study of 50 Computer Science undergraduates at a university outside the study area but with close characteristics to those of the target group but not included in the main study. Cronbach's Alpha statistical technique was used to assess the data from the pilot study since the instrument was not scored dichotomously. The cluster reliability values were 0.79, 0.74, 0.79, 0.71, and 0.73, respectively, and the overall reliability coefficient was 0.75. The reliability coefficients indicated that the instrument had an acceptable internal consistency and was suitable for data collection.

The researcher, assisted by competent research assistants, administered the questionnaire to the respondents. Before data collection, respondents were informed about the aim of the study and assured that all contributed information would be kept confidential and utilised for academic purposes only. Ethical approval was granted by the relevant institutional authority. All respondents participated voluntarily in the study and no personally identifiable information was collected. Out of 393 copies of the questionnaire distributed, 364 copies were successfully retrieved and found appropriate for analysis giving a response rate of 93%.

The data collected for the study were analysed using the Statistical Package for the Social Sciences (SPSS). The mean and standard deviation were used to answer the research questions. Differences between undergraduates from public and private universities were assessed using independent-samples t-test. Furthermore, multiple regression analysis was utilised to examine the predictive effect of cybersecurity software on safe digital learning. The usual criteria for interpretation was: 3.50-4.00 = Very Great Extent (VGE), 2.50-3.49 = Great Extent (GE), 1.50-2.49 = Low Extent (LE), 1.00-1.49 = Very Low Extent (VLE). All hypotheses were tested at the significance level of 0.05.

RESULTS AND DISCUSSION

Research Question One

What differences exist in the utilisation of antivirus software for safeguarding digital learning platforms between Computer Science undergraduates in public and private universities in Enugu State?

Table1: Mean and Standard Deviation Scores on Utilisation of Antivirus Software among Computer Science Undergraduates in Public and Private Universities

Items	Public Mean	SD	Remark	Private Mean	SD	Remark
Antivirus software is installed on devices used for safeguarding digital learning platform activities	2.22	0.81	LE	2.48	0.69	LE
Antivirus applications are regularly updated on academic devices	2.15	0.87	LE	2.40	0.71	LE
Antivirus software is used to scan downloaded academic files before opening them	2.10	0.89	LE	2.35	0.74	LE
Antivirus tools help prevent malicious attacks during online learning activities	2.20	0.84	LE	2.46	0.66	LE

Antivirus software contributes to the protection of academic documents and files	2.28	0.79	LE	2.49	0.63	LE
Malware protection systems improve safety during internet-based academic activities	2.24	0.82	LE	2.45	0.68	LE
Antivirus applications reduce exposure to malicious websites during digital learning	2.12	0.88	LE	2.38	0.72	LE
Devices used for academic purposes are protected against virus infections	2.18	0.85	LE	2.41	0.70	LE
Antivirus software enhances confidence while accessing digital learning platforms	2.20	0.81	LE	2.46	0.67	LE
Antivirus applications contribute to secure digital learning environments	2.27	0.79	LE	2.50	0.61	GE
Cluster Mean	**2.20**	**0.84**	**LE**	**2.44**	**0.68**	**LE**

Table 1 revealed that Computer Science undergraduates in both public and private universities utilised antivirus software for safeguarding digital learning platforms to a low extent. Public university Computer Science undergraduates obtained a cluster mean score of 2.20, while private university Computer Science undergraduates obtained a cluster mean score of 2.44. Since both cluster mean scores were below the criterion mean of 2.50, the results indicate that antivirus software were utilised to a low extent by undergraduates in both categories of universities. However, the higher cluster mean recorded by undergraduates in private universities suggests that they utilised antivirus software more than their counterparts in public universities. The standard deviation values indicate that respondents' ratings were not widely dispersed, suggesting relative homogeneity in their responses.

Research Question Two

What differences exist in the utilisation of firewalls for safeguarding digital learning platforms between Computer Science undergraduates in public and private universities in Enugu State?

Table 2: Mean and Standard Deviation Scores on Utilisation of Firewalls among Computer Science Undergraduates in Public and Private Universities

Items	Public Mean	SD	Remark	Private Mean	SD	Remark
Firewall protection is enabled on devices used for digital learning	2.12	0.86	LE	2.34	0.71	LE
Firewall systems help prevent unauthorised access to academic activities	2.18	0.83	LE	2.40	0.67	LE
Protected university networks improve safety during online learning	2.22	0.80	LE	2.44	0.65	LE
Firewall technologies contribute to secure internet access for academic purposes	2.10	0.85	LE	2.31	0.72	LE
Firewall technologies help detect suspicious online activities	2.00	0.89	LE	2.24	0.75	LE
Firewall protection enhances confidentiality during online academic communication	2.14	0.83	LE	2.38	0.69	LE
Secure institutional networks reduce cyber threats during digital learning	2.19	0.82	LE	2.42	0.67	LE

Firewall technologies contribute to uninterrupted online learning activities	2.05	0.87	LE	2.28	0.73	LE
Firewall systems improve the protection of digital learning platforms	2.12	0.84	LE	2.36	0.70	LE
Firewall technologies strengthen cybersecurity within university learning environments	2.25	0.80	LE	2.48	0.62	LE
Cluster Mean	**2.14**	**0.84**	**LE**	**2.37**	**0.69**	**LE**

Table 2 revealed that undergraduates in both public and private universities utilised firewall technologies for safeguarding digital learning platforms to a low extent. Public university Computer Science undergraduates obtained a cluster mean score of 2.14, while private university Computer Science undergraduates obtained a cluster mean score of 2.37. Since both cluster mean scores were below the criterion mean of 2.50, the results indicate that firewall technologies were utilised to a low extent by undergraduates in both categories of universities. However, the higher cluster mean recorded by undergraduates in private universities suggests that they utilised firewall technologies more than their counterparts in public universities. The standard deviation values showed low variability in responses, indicating that respondents' ratings were relatively homogeneous.

Research Question Three

What differences exist in the utilisation of Virtual Private Networks (VPNs) for safeguarding digital learning platforms between Computer Science undergraduates in public and private universities in Enugu State?

Table 3: Mean and Standard Deviation Scores on Utilisation of VPNs among Computer Science Undergraduates in Public and Private Universities

Items	Public Mean	SD	Remark	Private Mean	SD	Remark
VPN services improve privacy during online academic activities	2.14	0.86	LE	2.38	0.70	LE
VPN technologies help protect internet-based academic communication	2.18	0.83	LE	2.42	0.67	LE
VPN usage improves safety when accessing public networks for learning purposes	2.10	0.88	LE	2.34	0.71	LE
VPNs reduce exposure to cyber threats during online learning	2.16	0.85	LE	2.40	0.68	LE
VPN technologies contribute to secure remote access to academic resources	2.22	0.82	LE	2.48	0.64	LE
VPNs improve confidentiality during internet-based learning activities	2.12	0.87	LE	2.32	0.72	LE
VPN usage enhances secure participation in virtual classrooms	2.08	0.89	LE	2.30	0.73	LE
VPN technologies strengthen the protection of digital academic activities	2.15	0.84	LE	2.39	0.69	LE
VPNs contribute to safer access to institutional online platforms	2.20	0.82	LE	2.45	0.66	LE
VPN technologies enhance secure digital learning environments	2.24	0.81	LE	2.49	0.60	LE
Cluster Mean	**2.16**	**0.85**	**LE**	**2.40**	**0.68**	**LE**

Table 3 revealed that Computer Science undergraduates in both public and private universities utilised Virtual Private Network (VPN) technologies for safeguarding digital learning platforms to a low extent. Public university Computer Science undergraduates obtained a cluster mean score of 2.16, while private university Computer Science undergraduates obtained a cluster mean score of 2.40. Since both cluster mean scores were

below the criterion mean of 2.50, the results indicate that VPN technologies were utilised to a low extent by Computer Science undergraduates in both categories of universities. However, the higher cluster mean obtained by private university Computer Science undergraduates suggests that they utilised VPN technologies more than their counterparts in public universities. The standard deviation values indicated that respondents' ratings were not widely dispersed, suggesting relative consistency in their responses.

Research Question Four

To what extent do cybersecurity applications predict secure digital learning among Computer Science undergraduates in public and private universities in Enugu State?

Table 4: Cybersecurity Applications as Predictors of Secure Digital Learning among Computer Science Undergraduates in Public and Private Universities in Enugu State

Items	Public Mean	SD	Remark	Private Mean	SD	Remark
Digital learning platforms are protected against cyber threats	2.22	0.81	LE	2.48	0.63	LE
Academic information remains confidential during online learning activities	2.24	0.79	LE	2.49	0.60	LE
Online learning activities are conducted safely within university digital environments	2.18	0.84	LE	2.44	0.66	LE
Digital learning systems provide secure access to academic resources	2.23	0.80	LE	2.46	0.64	LE
Secure digital learning environments improve confidence in online education	2.16	0.85	LE	2.38	0.69	LE
Academic records are protected against unauthorised access	2.20	0.82	LE	2.45	0.65	LE
Digital learning systems ensure reliable and uninterrupted academic activities	2.12	0.86	LE	2.36	0.70	LE
Online academic communication remains secure within digital learning platforms	2.18	0.84	LE	2.42	0.67	LE
Secure digital learning environments reduce risks associated with cyberattacks	2.22	0.81	LE	2.48	0.62	LE
Cybersecurity applications contribute significantly to safe digital learning experiences	2.26	0.78	LE	2.49	0.58	LE
Cluster Mean	**2.20**	**0.82**	**LE**	**2.45**	**0.64**	**LE**

Table 4 revealed that undergraduates in both public and private universities experienced secure digital learning to a low extent. Public university Computer Science undergraduates obtained a cluster mean score of 2.20, while private university Computer Science undergraduates obtained a cluster mean score of 2.45. Since both cluster mean scores were below the criterion mean of 2.50, the results indicate that cybersecurity applications contributed to secure digital learning to a low extent in both categories of universities. However, the higher cluster mean recorded by Computer Science undergraduates in private universities suggests that they experienced relatively more secure digital learning environments than their counterparts in public universities. The standard deviation values were low, indicating that respondents' ratings were relatively homogeneous and that there was considerable agreement among the Computer Science undergraduates regarding the extent to which cybersecurity applications contributed to secure digital learning.

Test of Hypotheses

The hypotheses were tested using an independent-samples t-test at the 0.05 level of significance.

Hypothesis One

There is no significant difference in the utilisation of antivirus software for safeguarding digital learning platforms between Computer Science undergraduates in public and private universities in Enugu State.

Table5: Independent Samples t-test Analysis on Utilisation of Antivirus Software between Computer Science Undergraduates in Public and Private Universities

Variable	University Type	N	$\bar{X}$	SD	t	Df	p-value	Decision
Antivirus Software	Public Universities	257	2.20	0.84				
	Private Universities	107	2.44	0.68	4.96	362	0.000	Significant

Table 5 revealed a significant difference in the utilisation of antivirus software for safeguarding digital learning platforms between Computer Science undergraduates in public and private universities in Enugu State ($t = 4.96$, $df = 362$, $p < 0.05$). Since the p-value of 0.000 was less than the 0.05 level of significance, the null hypothesis was rejected. This implies that Computer Science undergraduates in private universities utilised antivirus software significantly more than their counterparts in public universities. However, the mean scores of both groups remained below the criterion mean of 2.50, indicating that utilisation of antivirus software was generally low among Computer Science undergraduates in both public and private universities.

Hypothesis Two

There is no significant difference in the utilisation of firewalls for safeguarding digital learning platforms between Computer Science undergraduates in public and private universities in Enugu State.

Table6: Independent Samples t-test Analysis on Utilisation of Firewall Technologies between Computer Science Undergraduates in Public and Private Universities

Variable	University Type	N	$\bar{X}$	SD	t	Df	p-value	Decision
Firewall Technologies	Public Universities	257	2.14	0.84				
	Private Universities	107	2.37	0.69	5.18	362	0.000	Significant

Table 6 showed a significant difference in the utilisation of firewall technologies for safeguarding digital learning platforms between Computer Science undergraduates in public and private universities in Enugu State ($t = 5.18$, $df = 362$, $p < 0.05$). Since the p-value of 0.000 was less than the 0.05 level of significance, the null hypothesis was rejected. This implies that Computer Science undergraduates in private universities utilised firewall technologies significantly more than their counterparts in public universities. However, the mean scores of both groups were below the criterion mean of 2.50, indicating that firewall technologies were utilised to a low extent by undergraduates in both public and private universities.

Hypothesis Three

There is no significant difference in the utilisation of Virtual Private Network (VPN) technologies for safeguarding digital learning platforms between Computer Science undergraduates in public and private universities in Enugu State.

Table 7: Independent Samples t-test Analysis on Utilisation of Virtual Private Network (VPN) Technologies between Computer Science Undergraduates in Public and Private Universities

Variable	University Type	N	$\bar{X}$	SD	t	Df	p-value	Decision
VPN Technologies	Public Universities	257	2.16	0.85				
	Private Universities	107	2.40	0.68	5.42	362	0.000	Significant

Table 7 revealed a significant difference in the utilisation of Virtual Private Network (VPN) technologies for safeguarding digital learning platforms between undergraduates in public and private universities in Enugu State ($t = 5.42$, $df = 362$, $p < 0.05$). Since the p-value of 0.000 was less than the 0.05 level of significance, the null hypothesis was rejected. This implies that Computer Science undergraduates in private universities utilised VPN technologies significantly more than their counterparts in public universities. However, the mean scores of both groups were below the criterion mean of 2.50, indicating that VPN technologies were utilised to a low extent by Computer Science undergraduates in both public and private universities.

Hypothesis Four

Cybersecurity applications do not significantly predict secure digital learning among Computer Science undergraduates in public and private universities in Enugu State.

Table 8: Model Summary of Cybersecurity Applications as Predictors of Secure Digital Learning

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.586	0.343	0.337	0.547

Table 8 shows that the multiple correlation coefficient (R) for the relationship between cybersecurity applications and secure digital learning was 0.586. The coefficient of determination (R^2) was 0.343, indicating that antivirus software, firewall technologies, and VPN technologies jointly accounted for 34.3% of the variance in secure digital learning among Computer Science undergraduates in public and private universities in Enugu State. The adjusted R^2 value of 0.337 indicates that the model remained stable after adjustment for sample size and number of predictor variables.

Table 9: ANOVA for the Regression Model

Model	Sum of Squares	Df	Mean Square	F	p-value
Regression	56.432	3	18.811	62.754	0.000
Residual	107.908	360	0.300		
Total	164.340	363			

Table 9 shows that the regression model was statistically significant, $F(3, 360) = 62.754$, $p < 0.05$. Since the p-value of 0.000 was less than the 0.05 level of significance, the regression model significantly predicted secure digital learning among Computer Science undergraduates in public and private universities in Enugu State.

Table 10: Multiple Regression Analysis on Cybersecurity Applications as Predictors of Secure Digital Learning

Predictor Variables	B	Std. Error	Beta	t	p-value	Decision
(Constant)	0.914	0.227	—	4.026	0.000	
Antivirus Software	0.294	0.058	0.319	5.069	0.000	Significant
Firewall Technologies	0.216	0.052	0.232	4.154	0.000	Significant
VPN Technologies	0.201	0.049	0.221	4.102	0.000	Significant

Table 10 revealed that antivirus software ($\beta = 0.319$, $p < 0.05$), firewall technologies ($\beta = 0.232$, $p < 0.05$), and VPN technologies ($\beta = 0.221$, $p < 0.05$) significantly predicted secure digital learning among Computer Science undergraduates in public and private universities in Enugu State. Antivirus software emerged as the strongest predictor of secure digital learning, followed by firewall technologies and VPN technologies.

Since the p-values associated with all predictor variables were less than the 0.05 level of significance, the null hypothesis was rejected. The findings indicate that although undergraduates in both public and private universities utilised cybersecurity applications to a low extent, increased utilisation of antivirus software, firewall technologies, and VPN technologies significantly enhanced secure digital learning. Therefore, cybersecurity applications remain important determinants of secure digital learning among university undergraduates.

Discussion of Findings

The study's findings revealed that Computer Science undergraduates in both public and private universities in Enugu State had low utilisation of cybersecurity applications for the protection of digital learning platforms such as antivirus software, firewall technologies and Virtual Private Network (VPN) technologies. However, in all categories of cybersecurity applications, the undergraduates in Computer Science from private universities consistently reported higher levels of utilisation than their peers in public universities. The differences noted between the two groups were statistically significant, demonstrating that institutional ownership and disparities in technology infrastructure may influence cybersecurity use among university undergraduates.

In particular, the results indicated that Computer Science undergraduates in private institutions used antivirus software substantially more than Computer Science

undergraduates in public universities. Both groups exhibited low levels of utilisation but private university Computer Science undergraduates had a higher mean score indicating considerably better involvement with endpoint protection technology. The poor use in both groups may be due to low cybersecurity awareness, irregular software upgrades, lack of access to licensed security apps, and minimal institutional interest in the security of personal devices. However, the much higher usage by Computer Science undergraduates at private universities may be due to better access to technology resources and more institutional support for digital learning. This decision is in line with the position of the National Institute of Standards and Technology (2020) that acknowledged antivirus technology as vital methods for securing digital systems against malware attacks and unlawful compromise. The research also corroborates Eze, Chinedu-Eze and Bello (2018) who found that institutional technological infrastructure and access to digital resources had considerable impact on technology utilisation in higher education institutions.

The study also found that the computer science undergraduates in the private institutions used the firewall technologies substantially more than the computer science undergraduates in the public universities. Despite this disparity, the use of firewall technology was low for Computer Science undergraduates in both types of universities. This indicates that many undergraduates may lack knowledge about the significance of firewall technology in blocking unauthorised access, identifying suspicious activities, and safeguarding digital learning environments from cyber dangers. The low level of usage may also be a reflection of limited exposure to advanced cybersecurity techniques and lack of adequate cybersecurity training of the undergraduates. This result is similar with Scarfone and Mell (2012) who stressed the relevance of firewall solutions in securing network infrastructure and preventing cyber assaults. Results also show that Computer Science undergraduates studying at universities with better digital infrastructures are more likely to use cybersecurity tools than those studying at less technologically sophisticated environments.

Similarly, the results showed that the Computer Science undergraduates in private universities used the Virtual Private Network (VPN) technology substantially more than the Computer Science undergraduates in public institutions. However, the use of VPN was generally low by both groups of Computer Science undergraduates. The conclusion could suggest a lack of awareness regarding the security benefits of VPN technologies, especially in terms of preserving online communication, ensuring privacy and securing access to academic resources over public networks. This substantially higher utilisation among private university Computer Science undergraduates may be linked to better internet infrastructure, better support services for cybersecurity, and more institutional advocacy of secure internet behaviours. This finding is consistent with the report of the European Union Agency for Cybersecurity (2021) that VPN technologies are vital instruments to secure online communication and enhance the security of remote digital activities.

The results also indicated a poor amount of secure digital learning among the Computer Science undergraduates in both public and private universities. However, undergraduates in private universities in Computer Science reported relatively higher levels of safe digital learning compared to undergraduates in Computer Science in public universities across all metrics examined. "The low ratings of both groups indicate that current cybersecurity practices and technologies might not be properly applied to create highly secure digital learning environments. However, the relatively higher ratings given by private university undergraduates suggest that increased use of cybersecurity applications may help to improve protection against cyber threats, increase confidentiality of academic information and provide safer access to digital learning resources.

In addition, the regression analysis established that the cybersecurity applications strongly predicted secure digital learning among Computer Science undergraduates at public and private universities. The highest predictor of safe digital learning was the use of antivirus software ($\beta = 0.319$), followed by the use of firewall technologies ($\beta = 0.232$) and VPN technologies ($\beta = 0.221$). The model explained 34.3% of the variance in secure digital learning, demonstrating that cybersecurity applications are crucial for the promotion of secure digital learning environments. While levels of use were often modest, the important predictive linkages show that improvement in the use of cybersecurity apps might greatly improve security, confidentiality, dependability and resilience of digital learning systems.

The findings support the work of Ulven and Wangen (2021) that institutional cyber resilience depends primarily on users' cyber practices and the effective implementation of cyber measures. Findings add support to UNESCO (2021) that sustainable digital learning systems need to be built on safe technological infrastructures to protect educational activities from cyber threats. More importantly, the findings offer empirical evidence that variances in the use of cybersecurity applications among institutions have significant implications for the security and sustainability of digital learning environments.

The results showed that the practice of cyber security among university undergraduates in the field of computer science is still unsatisfactory, despite the rising reliance on digital learning tools. The undergraduates in private institutions who studied Computer Science had a little higher level of utilisation than those in public universities but both are below the expected level of utilisation. Therefore, universities need to strengthen cybersecurity awareness programs, provide access to cybersecurity technologies, offer hands-on cybersecurity training and build institutional norms that support the efficient use of cybersecurity applications. This would result in safer, more robust and sustainable digital learning environments

at higher education institutions.

CONCLUSION

The study investigated the use of cybersecurity apps in securing digital learning platforms among the Computer Science undergraduates of public and private universities in Enugu State, Nigeria. The findings showed that Computer Science undergraduates in public and private universities used antivirus software, firewall technologies, and Virtual Private Network (VPN) technologies to a limited extent. However, freshmen from private colleges consistently reported much higher levels of utilisation than their public university peers across all categories of cybersecurity applications. The study also identified antivirus software, firewall technologies and VPN technologies as important predictors of secure digital learning with antivirus software being the highest predictor. These findings imply that the use of cybersecurity software in university undergraduates is still inadequate despite the essential role they play in fostering secure digital learning.

The study indicates that there is a need to improve the use of cybersecurity apps to improve the security, confidentiality, dependability and resilience of digital learning environments in higher education institutions . It therefore recommends that universities should invest in modern cyber security infrastructure, strengthen institutional cyber security policies, provide regular cyber security awareness programmes and practical training, integrate cyber security education into university curricula and promote the routine use of anti-virus software, firewall technologies and VPNs. There is also a need for increased government support to develop ICT infrastructure and cybersecurity capacity in public universities.

The study was limited to Computer Science undergraduates in selected public and private universities in Enugu State. The study only focused on antivirus software, firewall technologies and VPN technologies. Thus, the results may not be generalisable to other disciplines or places. Future research should incorporate more cybersecurity apps, a broader coverage of institutions, and a more diverse student population for improving the generalisability of the findings.

REFERENCES

Alharbi, F., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among university undergraduates: An empirical study. *Education and Information Technologies, 26*(5), 5615–5635. https://doi.org/10.1007/s10639-021-10551-2

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behaviour: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*. Retrieved from https://arxiv.org/abs/1901.02672

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.

Dhawan, S. (2020). Online learning: A panacea in the time of the COVID-19 crisis. *Journal of Educational Technology Systems, 49*(1), 5–22. https://doi.org/10.1177/0047239520934018

Cybersecurity and Infrastructure Security Agency. (2023). *Implementing phishing-resistant MFA*. Retrieved fromhttps ://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

European Union Agency for Cybersecurity. (2021). *Cybersecurity guidelines for remote learning and education systems*. Retrieved from https://www.enisa.europa.eu/sites/default/files/publications/ENISA_Cybersecurity%20education%20initiatives%20in%20MS.pdf

European Union Agency for Cybersecurity. (2023). *Threat landscape for the education sector*. Retrieved from https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

Eze, S. C., Chinedu-Eze, V. C., & Bello, A. O. (2018). The utilisation of e-learning facilities in the educational delivery system of Nigeria: A study of M-University. *International Journal of Educational Technology in Higher Education, 15*(1), 34. Retreived from https://doi.org/10.1186/s41239-018-0116-z

Hadlington, L. (2017). Human factors in cybersecurity: examining the linkages among Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organisations (SP 800-53 Rev. 5)*. Retrieved from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *Journal of Engineering and Technology Research, 8*(3), 37–42.

Osijirin, A. N., Anigbo, L. C., & Okechukwu, O. (2026). Gender disparities in cybersecurity application usage among Computer Science undergraduates in Nigerian universities. *Asian Journal of Information Science and Technology, 16*(1). https://doi.org/10.70112/ajist-2026.16.1.4438

Osijirin, A. N., Sada, S. M., Edmond, V. U., Anigbo, L. C., & Okechukwu, O. (2026). AI-powered scams and deepfakes in tertiary institutions in Enugu State, Nigeria: The roles of cybersecurity awareness, digital

literacy, and media literacy in undergraduates' fraud detection preparedness. *Saudi Journal of Engineering and Technology, 11*(4). https://doi.org/10.36348/sjet.2026.v11i04.021

Scarfone, K., & Mell, P. (2012). *Guide to intrusion detection and prevention systems (IDPS)*—National Institute of Standards and Technology.

Teo, T. (2019). Undergraduates and teachers' intention to use technology: Assessing their measurement equivalence and structural invariance. *Journal of Educational Computing Research, 57*(1), 201–225.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviours: A protection motivation theory perspective. *Computers & Security, 59,* 138–150.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39.

UNESCO. (2021). *Education during COVID-19 and beyond.* Retrieved from https://www.unesco.org/en/covid-19/education-response

Viswanath Venkatesh, Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.