Asian Journal of Information Science and Technology, 16(1), 56–65, 2026

Asian Journal of Information Science and Technology
ISSN: 2231-6108 (Print) | 3049-2661 (Online)
Journal Homepage: https://ajist.co
DOI: https://doi.org/10.70112/ajist-2026.16.1.4438

Research Article

# Gender Disparities in Cybersecurity Application Usage among Computer Science Undergraduates in Nigerian Universities

**Adesegun Nurudeen Osijirin[1*], Leonard C. Anigbo[2] and Oliver Okechukwu[3]**
[1]Department of Healthcare Management, Federal University of Allied Health Sciences, Enugu State, Nigeria
[2,3]Department of Mathematics and Computer Science Education, Enugu State University of Science and Technology, Enugu State, Nigeria

## Article Information

Article History
Received: 23 February 2026
Revised: 16 March 2026
Accepted: 31 March 2026
Published online: 10 April 2026

Keywords
Cybersecurity Applications
Gender Disparities
Antivirus and Antimalware Software
Firewalls and IDS/IPS
Multi-Factor Authentication
Virtual Private Networks

Correspondence*
adesegunosijirin@fuahse.edu.ng

ORCID
Adesegun Nurudeen Osijirin
https://orcid.org/0009-0002-1053-0913
Leonard C. Anigbo
https://orcid.org/0009-0000-4980-8850
Oliver Okechukwu
https://orcid.org/0009-0009-7404-1431

## Abstract

This study explored gender differences in the use of cybersecurity applications among computer science undergraduates in universities in Enugu State, Nigeria. The use of antivirus and anti-malware software, firewalls, intrusion detection/prevention systems (IDS/IPS), encryption tools, Multi-Factor Authentication/Two-Factor Authentication (MFA/2FA), and Virtual Private Networks (VPNs) in digital learning environments was examined. A descriptive survey research design was adopted. The population comprised 5,351 computer science undergraduates, from which a sample of 486 respondents was selected using a multi-stage proportionate stratified random sampling technique. The sample consisted of 295 males and 191 females. Data were collected using the Utilisation of Cybersecurity Applications for Digital Learning Questionnaire (UCADLQ). Statistical analyses were conducted using means, standard deviations, and independent-samples t-tests. The findings revealed significant gender differences in the use of antivirus software, firewalls, IDS/IPS, encryption tools, MFA/2FA, and VPN technologies, with male students demonstrating relatively higher usage rates than female students. The study confirmed that gender has a significant influence on the utilisation of cybersecurity applications in digital learning environments. The study recommended practical cybersecurity education, comprehensive digital safety programmes, and institutional cybersecurity support frameworks to enhance student engagement with cybersecurity practices in universities.



## I.INTRODUCTION

Information and communication technology has developed rapidly and has had a significant impact on educational systems around the world. Digital technologies are becoming increasingly important in teaching and learning, assessment, research, communication, and academic administration in universities. With the advent of internet-enabled systems, virtual classrooms, institutional portals, cloud-based learning platforms, video conferencing technologies, and Learning Management Systems (LMS), digital learning environments have revolutionized the traditional delivery of education. Through digital technologies, education has become more accessible, collaboration between students and lecturers has been enhanced, flexible learning has become possible, and academic resources are now available beyond the traditional classroom. The COVID-19 pandemic disrupted traditional face-to-face education systems in many countries and accelerated the growth of digital education worldwide. During this period, universities rapidly adopted online learning technologies to maintain academic operations and sustain educational delivery. As noted by UNESCO (2021), educational institutions worldwide increasingly employed digital learning tools as alternative means of continuing teaching and learning activities during the pandemic. Consequently, universities became more dependent on internet-based systems and other digital infrastructures for academic communication, online assessments, assignment submissions, virtual interactions, and cloud-based educational activities. Although digital learning systems offer numerous advantages, their increasing reliance on digital technologies exposes universities to a wide range of cybersecurity threats. Educational institutions are increasingly targeted by cyberattacks such as phishing,

malware infections, ransomware, stolen login credentials, identity theft, unauthorized access to institutional systems, and the unauthorized dissemination of digital content. Cybersecurity concerns pose significant risks to students, academics, institutional infrastructures, online learning platforms, academic databases, and sensitive educational data. The growing sophistication of cyber threats in higher education has made cybersecurity an essential component of sustainable digital learning systems.

The open and interconnected nature of digital environments, coupled with thousands of users possessing varying levels of digital literacy and cybersecurity knowledge, makes higher education institutions attractive targets for cybercriminals. The effectiveness of cybersecurity systems in digital learning environments depends largely on users' cybersecurity practices and usage behaviors. Research has shown that merely possessing appropriate cybersecurity technologies does not guarantee online security for individuals or organizations. Rather, it is the proper and consistent use of such technologies that makes the difference. Therefore, human behavior is a key determinant of cybersecurity success in educational institutions. Although institutions may have cybersecurity infrastructures in place, students may lack adequate cybersecurity practices, making them vulnerable to cyber threats. Gender is one factor that may influence cybersecurity usage behavior. Understanding these differences can help stakeholders develop strategies to enhance digital safety and encourage more effective cybersecurity practices among students. Many studies have demonstrated that male students tend to be more confident in using technology, experiment more with digital systems, and engage more frequently with cybersecurity technologies than female students. Conversely, other studies suggest that female students may exhibit greater online caution, safer online behaviors, and heightened sensitivity to privacy concerns, despite possessing lower levels of technological competence. The literature on gender differences in cybersecurity usage behavior has produced inconsistent findings, highlighting the need for further empirical investigation, particularly within higher education environments.

Computer science undergraduates represent an important population for examining the use of cybersecurity applications due to their regular interaction with computing systems, internet technologies, software environments, and digital platforms. These students are generally expected to possess a greater understanding of digital systems and cybersecurity concepts than students in many other disciplines. Nevertheless, despite their technological exposure, variations exist in the practical application of cybersecurity tools during digital learning activities. The Nigerian context presents unique cybersecurity challenges, and there is a paucity of empirical studies examining gender differences in the use of cybersecurity applications among university students. Most studies conducted in Nigeria have focused on cybersecurity knowledge, digital literacy, internet usage, e-learning adoption, or general online behavior without explicitly investigating gender-related differences in the actual use of cybersecurity applications within digital learning environments. Furthermore, there is a dearth of empirical studies on cybersecurity usage behavior among computer science undergraduates in universities in Enugu State, Nigeria. This represents a significant empirical and contextual gap, as understanding gender-specific cybersecurity usage behaviors is essential for developing targeted cybersecurity strategies, promoting secure digital learning environments, advancing inclusive cybersecurity education, and enhancing digital resilience within universities. Failure to address these gender-related cybersecurity disparities may leave educational institutions vulnerable to unsafe cybersecurity practices among students. Therefore, this study investigated gender differences in the use of cybersecurity applications among computer science undergraduates in universities in Enugu State, Nigeria.

## II. METHODOLOGY

This research employed a descriptive survey design to investigate gender disparities in the utilisation of cybersecurity applications among computer science undergraduates at universities in Enugu State, Nigeria. The descriptive survey design was deemed suitable because the study involved gathering quantitative data from participants regarding their cybersecurity usage behaviour in digital learning settings. Creswell and Creswell (2018) assert that descriptive survey research designs are appropriate for investigations aimed at describing behavioural patterns, attitudes, views, and practices within a specified population. The design enabled the researcher to collect relevant information on students' use of cybersecurity applications and comparatively analyse gender-related differences in cybersecurity utilisation behaviour. The research was carried out in Enugu State, Nigeria. Enugu State, located in Nigeria’s South-East geopolitical zone, has several federal, state, and private universities that currently utilise digital learning systems and internet-enabled educational technologies.

The study population comprised 5,351 computer science undergraduates, consisting of 3,544 males and 1,807 females, from selected universities in Enugu State, Nigeria. Computer science undergraduates were selected because they frequently use digital systems, internet technologies, online learning platforms, and cybersecurity applications in academic contexts. Their technological proficiency enabled them to provide informed perspectives on the utilisation of cybersecurity applications in digital learning environments. The sample for the study consisted of 486 respondents, including 295 males and 191 females. The study adopted a multi-stage proportionate stratified random sampling technique. Initially, universities in Enugu State were categorised by ownership as federal, state, and private institutions. To ensure adequate representation across ownership categories, a proportionate stratified sampling procedure was used to select the participating universities. This process resulted in the selection of one federal university, one state university, and two private universities. The second stage involved a proportionate stratified sampling process within the selected universities to choose respondents

from the Department of Computer Science. The study randomly selected 10% of the total population of computer science undergraduates from the selected universities. Simple random sampling was then used to select respondents from each institution. Data for the study were collected using a structured questionnaire titled *Utilisation of Cybersecurity Applications for Digital Learning Questionnaire (UCADLQ)*. The instrument was developed by the researcher based on the objectives of the study and related literature on the application of cybersecurity in digital learning environments. The questionnaire consisted of two sections. Section A collected data on the demographic characteristics of the respondents, such as gender, institution, and academic level. Section B contained questionnaire items designed to measure students' use of antivirus and antimalware software, firewalls and IDS/IPS, encryption tools, MFA/2FA, and VPN technologies. The questionnaire items were organised using a four-point Likert rating scale comprising: Very Great Extent (VGE), Great Extent (GE), Low Extent (LE), and Very Low Extent (VLE).

The instrument underwent face and content validation by three experts. Two experts were selected from the Department of Computer and Robotics Education, while one was selected from the Department of Measurement and Evaluation. The validators carefully assessed the instrument for linguistic clarity, relevance of the questionnaire items, adequacy of content coverage, appropriateness of the measurement scale, and alignment with the study objectives. The experts' suggestions and corrections were incorporated before the final administration of the instrument. The reliability of the instrument was determined using Cronbach's alpha. The instrument was pilot-tested with 30 computer science undergraduates from universities outside the study area who possessed characteristics similar to those of the target population. Data obtained from the pilot study were analysed using the Statistical Package for the Social Sciences (SPSS). The reliability coefficients for the various clusters ranged from 0.81 to 0.88, while the overall reliability coefficient of the instrument was 0.84. Nunnally and Bernstein (1994) stated that reliability coefficients above 0.70 are considered acceptable for educational and social science research. The researcher administered the questionnaire directly to the participants with the assistance of trained research assistants. The participants were informed of the purpose of the study and assured that all information provided would be treated confidentially and used solely for academic purposes. Completed questionnaire copies were collected immediately after completion to minimise loss and ensure a high response rate. The data collected for the study were analysed using the Statistical Package for the Social Sciences (SPSS). Mean and standard deviation were used to answer the research questions, while an independent-samples t-test was employed to test the hypotheses at a 0.05 level of significance. The criterion mean used for interpretation was as follows:

3.50–4.00 = Very Great Extent; 2.50–3.49 = Great Extent; 1.50–2.49 = Low Extent; 1.00–1.49 = Very Low Extent.

## III. RESULTS

This section presents an analysis of the data obtained for the study, together with the research questions and hypotheses that guided the investigation. Mean and standard deviation were used to answer the research questions, while an independent-samples t-test was employed to test the hypotheses at a 0.05 level of significance.

### *A. Research Question One*

What gender disparities exist in the use of antivirus and antimalware software among computer science undergraduates in universities in Enugu State?

TABLE I AVERAGE AND STANDARD DEVIATION SCORES ON GENDER DISPARITIES IN THE UTILISATION OF ANTIVIRUS AND ANTIMALWARE SOFTWARE

| S.No. | Items | Male Mean | SD | Remark | Female Mean | SD | Remark |
|---|---|---|---|---|---|---|---|
| 1 | Antivirus software is installed on devices used for digital learning activities | 2.48 | 0.83 | LE | 2.22 | 0.91 | LE |
| 2 | Antivirus applications are regularly updated on academic devices | 2.41 | 0.86 | LE | 2.15 | 0.94 | LE |
| 3 | Antivirus software is used to scan downloaded academic files before opening them | 2.45 | 0.82 | LE | 2.10 | 0.95 | LE |
| 4 | Antimalware tools help prevent malicious attacks during online learning activities | 2.52 | 0.79 | GE | 2.18 | 0.92 | LE |
| 5 | Antivirus software contributes to the protection of academic documents and files | 2.49 | 0.81 | LE | 2.16 | 0.93 | LE |
| 6 | Malware protection systems improve safety during internet-based academic activities | 2.46 | 0.84 | LE | 2.14 | 0.91 | LE |
| 7 | Antivirus applications reduce exposure to malicious websites during digital learning | 2.40 | 0.87 | LE | 2.11 | 0.95 | LE |
| 8 | Devices used for academic purposes are protected against virus infections | 2.44 | 0.83 | LE | 2.17 | 0.92 | LE |
| 9 | Antivirus software enhances confidence while accessing digital learning platforms | 2.50 | 0.80 | GE | 2.19 | 0.90 | LE |
| 10 | Antivirus and antimalware applications contribute to secure digital learning environments | 2.53 | 0.78 | GE | 2.20 | 0.89 | LE |
| | GRAND | 2.47 | 0.82 | LE | 2.16 | 0.92 | LE |

Table I indicates that male students exhibited a comparatively higher utilisation of antivirus and antimalware software than female students. The grand mean of 2.47 for male respondents exceeded the cluster mean of 2.16 for female respondents, indicating greater use of antivirus technologies among male students.

### *B. Research Question Two*

What gender disparities exist in the utilisation of firewalls and IDS/IPS among computer science undergraduates in universities in Enugu State?

TABLE II AVERAGE AND STANDARD DEVIATION SCORES ON GENDER DISPARITIES IN THE UTILISATION OF FIREWALLS AND IDS/IPS

| S.No. | Items | Male Mean | SD | Remark | Female Mean | SD | Remark |
|---|---|---|---|---|---|---|---|
| 11 | Firewall protection is enabled on devices used for digital learning | 2.46 | 0.84 | LE | 2.12 | 0.93 | LE |
| 12 | Firewall systems help prevent unauthorised access to academic activities | 2.51 | 0.80 | GE | 2.18 | 0.90 | LE |
| 13 | Protected university networks improve safety during online learning | 2.49 | 0.81 | LE | 2.16 | 0.92 | LE |
| 14 | Firewalls contribute to secure internet access for academic purposes | 2.44 | 0.85 | LE | 2.10 | 0.95 | LE |
| 15 | IDS/IPS technologies help detect suspicious online activities | 2.40 | 0.88 | LE | 2.08 | 0.96 | LE |
| 16 | Firewall protection enhances confidentiality during online academic communication | 2.48 | 0.82 | LE | 2.14 | 0.91 | LE |
| 17 | Secure institutional networks reduce cyber threats during digital learning | 2.50 | 0.80 | GE | 2.17 | 0.89 | LE |
| 18 | IDS/IPS technologies contribute to uninterrupted online learning activities | 2.43 | 0.86 | LE | 2.11 | 0.94 | LE |
| 19 | Firewall systems improve the protection of digital learning platforms | 2.47 | 0.83 | LE | 2.13 | 0.92 | LE |
| 20 | Firewalls and IDS/IPS strengthen cybersecurity within university learning environments | 2.55 | 0.77 | GE | 2.20 | 0.88 | LE |

Table II indicates that male students utilised firewall and IDS/IPS technologies more frequently than female students. The cluster mean of 2.47 for male respondents exceeded the corresponding cluster mean of 2.14 for female respondents.

### *C. Research Question Three*

What gender disparities exist in the use of encryption technologies among computer science undergraduates in universities in Enugu State?

TABLE III AVERAGE AND STANDARD DEVIATION SCORES ON GENDER DISPARITIES IN THE USE OF ENCRYPTION TOOLS

| S.No. | Items | Male Mean | SD | Remark | Female Mean | SD | Remark |
|---|---|---|---|---|---|---|---|
| 21 | Encrypted academic websites improve confidentiality during digital learning | 2.49 | 0.81 | LE | 2.17 | 0.91 | LE |
| 22 | Encryption tools help protect academic information from unauthorised access | 2.54 | 0.78 | GE | 2.19 | 0.89 | LE |
| 23 | Password-protected academic files improve digital learning security | 2.46 | 0.83 | LE | 2.13 | 0.93 | LE |
| 24 | Encrypted communication enhances trust in online academic interactions | 2.48 | 0.82 | LE | 2.15 | 0.91 | LE |
| 25 | Encryption technologies contribute to the secure submission of academic assignments | 2.44 | 0.85 | LE | 2.10 | 0.95 | LE |
| 26 | Secure, encrypted platforms improve safety during online learning | 2.50 | 0.80 | GE | 2.18 | 0.90 | LE |
| 27 | Encryption tools reduce the risk of academic data interception | 2.45 | 0.84 | LE | 2.12 | 0.93 | LE |
| 28 | Digital learning activities are safer on encrypted platforms | 2.47 | 0.82 | LE | 2.14 | 0.91 | LE |
| 29 | Encryption mechanisms enhance privacy during online academic communication | 2.51 | 0.79 | GE | 2.16 | 0.90 | LE |
| 30 | Encryption tools contribute significantly to secure digital learning environments | 2.55 | 0.77 | GE | 2.20 | 0.88 | LE |
| | GRAND | 2.49 | 0.81 | LE | 2.15 | 0.91 | LE |

Table III indicates that male students utilised encryption technologies to a greater extent than their female counterparts. The cluster mean for male respondents exceeded that of female respondents.

### *D. Research Question Four*

What gender disparities exist in the use of MFA/2FA among computer science undergraduates in universities in Enugu State?

TABLE IV AVERAGE AND STANDARD DEVIATION SCORES ON GENDER DISPARITIES IN THE UTILISATION OF MFA/2FA

| S.No. | Items | Male Mean | SD | Remark | Female Mean | SD | Remark |
|---|---|---|---|---|---|---|---|
| 31 | MFA/2FA improves the protection of academic accounts | 2.60 | 0.75 | GE | 2.24 | 0.87 | LE |
| 32 | Secure authentication mechanisms reduce unauthorised access to digital learning platforms | 2.56 | 0.77 | GE | 2.20 | 0.89 | LE |
| 33 | MFA/2FA enhances security during online academic activities | 2.58 | 0.76 | GE | 2.22 | 0.88 | LE |
| 34 | Digital learning systems protected by MFA/2FA are safer to use | 2.50 | 0.80 | GE | 2.18 | 0.90 | LE |
| 35 | MFA/2FA reduces the risk of account compromise in online learning environments | 2.57 | 0.77 | GE | 2.21 | 0.88 | LE |
| 36 | Authentication mechanisms improve the confidentiality of academic information | 2.49 | 0.81 | LE | 2.16 | 0.92 | LE |
| 37 | Secure login systems contribute to safe participation in online learning | 2.54 | 0.78 | GE | 2.20 | 0.89 | LE |
| 38 | MFA/2FA enhances trust in institutional digital learning platforms | 2.48 | 0.82 | LE | 2.15 | 0.91 | LE |
| 39 | SeCure authentication systems strengthen the protection of academic records | 2.55 | 0.77 | GE | 2.18 | 0.89 | LE |
| 40 | MFA/2FA contributes significantly to securing digital learning | 2.62 | 0.74 | GE | 2.24 | 0.86 | LE |
| | GRAND | 2.55 | 0.78 | GE | 2.20 | 0.89 | LE |

Table IV indicates that male students exhibited a comparatively higher utilisation of MFA/2FA technologies than female students. The overall mean for male respondents indicated a high level of usage, whereas female respondents demonstrated a low level of utilisation.

### *E. Research Question Five*

What gender disparities exist in the utilisation of VPN technology among computer science undergraduates in universities in Enugu State?

TABLE V AVERAGE AND STANDARD DEVIATION SCORES ON GENDER DISPARITIES IN THE UTILISATION OF VPN TECHNOLOGIES

| S.No. | Items | Male Mean | SD | Remark | Female Mean | SD | Remark |
|---|---|---|---|---|---|---|---|
| 41 | VPN services improve privacy during online academic activities | 2.46 | 0.83 | LE | 2.12 | 0.93 | LE |
| 42 | VPN technologies help protect internet-based academic communication | 2.50 | 0.80 | GE | 2.16 | 0.91 | LE |
| 43 | VPN usage improves safety when accessing public networks for learning purposes | 2.44 | 0.85 | LE | 2.10 | 0.95 | LE |
| 44 | VPNs reduce exposure to cyber threats during online learning | 2.48 | 0.82 | LE | 2.14 | 0.91 | LE |
| 45 | VPN technologies contribute to secure remote access to academic resources | 2.52 | 0.79 | GE | 2.18 | 0.90 | LE |
| 46 | VPNs improve confidentiality during internet-based learning activities | 2.45 | 0.84 | LE | 2.11 | 0.94 | LE |
| 47 | VPN usage enhances secure participation in virtual classrooms | 2.43 | 0.86 | LE | 2.09 | 0.95 | LE |
| 48 | VPN technologies strengthen the protection of digital academic activities | 2.47 | 0.82 | LE | 2.13 | 0.92 | LE |
| 49 | VPNs contribute to safer access to institutional online platforms | 2.50 | 0.80 | GE | 2.16 | 0.91 | LE |
| 50 | VPN technologies enhance secure digital learning environments | 2.54 | 0.78 | GE | 2.20 | 0.88 | LE |
| | GRAND | 2.48 | 0.82 | LE | 2.14 | 0.92 | LE |

Table V indicates that male students exhibited greater utilisation of VPN technology than female students across all questionnaire items. The cluster mean for male respondents exceeded that of female respondents, indicating greater VPN utilisation among male students.

### *F. Hypothesis One*

There is no significant gender disparity in the utilisation of antivirus and antimalware software among computer science undergraduates in universities in Enugu State.

TABLE VI INDEPENDENT-SAMPLES T-TEST ANALYSIS OF GENDER DISPARITIES IN THE UTILISATION OF ANTIVIRUS AND ANTIMALWARE SOFTWARE

| Variable | Gender | N | Mean | SD | t | Df | Sig. | Decision |
|---|---|---|---|---|---|---|---|---|
| Antivirus and Antimalware Software | Male | 295 | 2.47 | 0.82 | | | | |
| | Female | 191 | 2.16 | 0.92 | 3.86 | 484 | 0.000 | Significant |

Table VI indicates a significant gender disparity in the utilisation of antivirus and antimalware software among computer science undergraduates in universities in Enugu State ($t = 3.86$, $df = 484$, $p < 0.05$). The p-value of 0.000, being less than the 0.05 level of significance, led to the rejection of the null hypothesis. This indicates that gender significantly influenced students' utilisation of antivirus and antimalware software, with male students exhibiting comparatively higher usage than female students.

### *G. Hypothesis Two*

There is no significant gender disparity in the utilisation of firewalls and IDS/IPS among computer science undergraduates in universities in Enugu State.

TABLE VII INDEPENDENT SAMPLES T-TEST ANALYSIS OF GENDER DISPARITIES IN THE UTILISATION OF FIREWALLS AND IDS/IPS

| Variable | Gender | N | Mean | SD | t | df | Sig. | Decision |
|---|---|---|---|---|---|---|---|---|
| Firewalls and IDS/IPS | Male | 295 | 2.47 | 0.83 | | | | |
| | Female | 191 | 2.14 | 0.92 | 4.02 | 484 | 0.000 | Significant |

Table VII indicates a significant gender disparity in the utilisation of firewalls and IDS/IPS among computer science undergraduates in universities in Enugu State ($t = 4.02$, $df = 484$, $p < 0.05$). The p-value of 0.000, being less than the 0.05 level of significance, led to the rejection of the null hypothesis. This indicates that gender significantly influenced students' utilisation of firewalls and IDS/IPS technologies, with male students exhibiting comparatively higher utilisation than female students.

### *H. Hypothesis Three*

There is no significant gender disparity in the utilisation of encryption technologies among computer science undergraduates in universities in Enugu State.

TABLE VIII INDEPENDENT SAMPLES T-TEST ANALYSIS OF GENDER DISPARITIES IN THE UTILISATION OF ENCRYPTION TOOLS

| Variable | Gender | N | Mean | SD | t | df | Sig. | Decision |
|---|---|---|---|---|---|---|---|---|
| Encryption Tools | Male | 295 | 2.49 | 0.81 | | | | |
| | Female | 191 | 2.15 | 0.91 | 4.15 | 484 | 0.000 | Significant |

Table VIII indicates a significant gender disparity in the utilisation of encryption technologies among computer science undergraduates in universities in Enugu State ($t = 4.15$, $df = 484$, $p < 0.05$). Given that the p-value of 0.000 was below the 0.05 level of significance, the null hypothesis was rejected. This indicates that gender significantly influenced students' utilisation of encryption technologies, with male students exhibiting comparatively higher utilisation than female students.

### *I. Hypothesis Four*

There is no significant gender disparity in the utilisation of MFA/2FA among computer science undergraduates in universities in Enugu State.

TABLE IX INDEPENDENT SAMPLES T-TEST ANALYSIS OF GENDER DISPARITIES IN THE UTILISATION OF MFA/2FA

| Variable | Gender | N | Mean | SD | t | df | Sig. | Decision |
|---|---|---|---|---|---|---|---|---|
| MFA/2FA | Male | 295 | 2.55 | 0.78 | | | | |
| | Female | 191 | 2.20 | 0.89 | 4.38 | 484 | 0.000 | Significant |

Table IX demonstrates a significant gender disparity in the utilisation of MFA/2FA among computer science undergraduates in universities in Enugu State ($t = 4.38$, $df = 484$, $p < 0.05$). Given that the p-value of 0.000 was below the

0.05 level of significance, the null hypothesis was rejected. This indicates that gender significantly influenced students' utilisation of MFA/2FA technology, with male students exhibiting comparatively higher utilisation than female students.

### *J. Hypothesis Five*

There is no significant gender disparity in the utilisation of VPN technology among computer science undergraduates in universities in Enugu State.

TABLE X INDEPENDENT SAMPLES T-TEST ANALYSIS OF GENDER DISPARITIES IN VPN TECHNOLOGY UTILISATION

| Variable | Gender | N | Mean | SD | t | df | Sig. | Decision |
|---|---|---|---|---|---|---|---|---|
| VPN Technologies | Male | 295 | 2.48 | 0.82 | | | | |
| | Female | 191 | 2.14 | 0.92 | 4.11 | 484 | 0.000 | Significant |

Table X showed a significant gender difference in the utilisation of VPN technologies among computer science undergraduates in universities in Enugu State ($t = 4.11$, $df = 484$, $p < 0.05$). Since the p-value of 0.000 was less than the 0.05 level of significance, the null hypothesis was rejected. This implies that gender significantly influenced students' utilisation of VPN technologies, with male students demonstrating comparatively higher utilisation than female students.

## IV. DISCUSSION

The findings were discussed in relation to the research questions and hypotheses that guided the study.

### *A. Extent of Utilisation of Antivirus and Antimalware Software for Digital Learning*

Regarding the extent of utilisation of antivirus and antimalware software for digital learning among computer science undergraduates in universities in Enugu State, this study found that the undergraduates utilised antivirus and antimalware software to a low extent for digital learning. This finding agrees with that of Ani and Mogboh (2021), who found that ICT and digital protection facilities were not adequately utilised in universities in Enugu State. The finding also aligns with that of Bottyán (2023), who identified weaknesses in students' cybersecurity behaviour and online protection practices. However, the finding contradicts that of Santelices (2025), who reported that students demonstrated high levels of cybersecurity awareness and cybersecurity education.

Regarding the influence of gender, this study found that male and female computer science undergraduates differed significantly in their utilisation of antivirus and antimalware software for digital learning, with male students demonstrating comparatively higher utilisation than female students. This finding supports those of Alotaibi and Alshehri (2020), McGill and Thompson (2018), and Anwar et al. (2016), who found that male users demonstrated stronger cybersecurity behaviour and security management practices than female users. The finding further implies that inadequate utilisation of antivirus and antimalware software may expose students and university digital learning systems to malware attacks, spyware, ransomware, and unauthorised system access.

### *B. Extent of Utilisation of Firewalls and IDS/IPS for Digital Learning*

Regarding the extent of utilisation of firewalls and intrusion detection/prevention systems (IDS/IPS) for digital learning, this study found that computer science undergraduates utilised firewalls and IDS/IPS to a low extent within digital learning environments. This finding agrees with that of Ulven and Wangen (2021), who reported that weak cybersecurity practices and inadequate institutional cybersecurity measures contribute significantly to cybersecurity vulnerabilities in higher education institutions. The finding also aligns with that of Binuyo (2019), who found that universities experience several cyber threats despite the availability of institutional security technologies. However, the finding contradicts that of Bibangco and Villar (2025), who reported relatively stronger cybersecurity practices among students in some university environments.

Regarding the influence of gender, the study found significant gender differences in the utilisation of firewalls and IDS/IPS among undergraduates, with male students demonstrating comparatively higher utilisation than female students. This finding corroborates those of Alotaibi and Alshehri (2020) and Branley-Bell *et al.* (2022), who found that males demonstrated relatively stronger cybersecurity behaviour and online protection practices than females. The low utilisation of firewalls and IDS/IPS therefore suggests weak network protection practices among students within digital learning environments.

### *C. Extent of Utilisation of Encryption Tools for Digital Learning*

Regarding the extent of utilisation of encryption tools for digital learning among computer science undergraduates, this study found that students utilised encryption tools to a low extent in universities in Enugu State. This finding agrees with those of Bottyán (2023) and Alharbi and Tassaddiq (2021), who identified gaps in cybersecurity awareness, secure online behaviour, and digital protection practices among students. However, the finding contradicts that of Osijirin *et al.* (2026), who found that students demonstrated

cybersecurity awareness and preparedness to a great extent in detecting AI-powered scams and deepfakes. Regarding gender influence, the study revealed significant gender differences in the utilisation of encryption tools, with male undergraduates demonstrating comparatively higher utilisation than female students. This finding supports those of Anwar *et al.* (2016) and McGill and Thompson (2018), who found that males demonstrated stronger cybersecurity practices and higher cybersecurity self-efficacy than females. The finding implies that limited utilisation of encryption tools may expose students' academic data, passwords, and digital communications to interception and unauthorised access.

### *D. Extent of Utilisation of MFA/2FA for Digital Learning*

Regarding the extent of utilisation of Multi-Factor Authentication and Two-Factor Authentication (MFA/2FA) for digital learning, this study found that computer science undergraduates utilised MFA/2FA technologies to a low extent within digital learning environments. This finding agrees with that of Alharbi and Tassaddiq (2021), who identified gaps in students' cybersecurity awareness and compliance practices. The finding also supports that of Ulven and Wangen (2021), who identified weak password management and inadequate authentication practices as major cybersecurity vulnerabilities in higher education institutions. However, the finding contradicts that of Santelices (2025), who reported high cybersecurity awareness and positive cybersecurity practices among students.

Regarding the influence of gender, the study found that male and female undergraduates differed significantly in their utilisation of MFA/2FA technologies, with male students demonstrating comparatively higher utilisation. This finding agrees with those of Alotaibi and Alshehri (2020), McGill and Thompson (2018), and Anwar *et al*. (2016), who reported stronger cybersecurity practices among males. The finding therefore suggests that weak authentication practices may increase students' vulnerability to phishing attacks, account compromise, and identity theft within digital learning environments.

### *E. Extent of Utilisation of VPN Technologies for Digital Learning*

Regarding the extent of utilisation of Virtual Private Networks (VPNs) for digital learning, this study found that computer science undergraduates utilised VPN technologies to a low extent in universities in Enugu State. This finding agrees with that of Ani and Mogboh (2021), who found inadequate utilisation of several ICT and digital learning technologies within universities. The finding also aligns with that of Ulven and Wangen (2021), who identified inadequate digital protection mechanisms as major cybersecurity challenges in higher education institutions. However, the finding contradicts that of Bibangco and Villar (2025), who reported stronger cybersecurity practices among some university students. Regarding the influence of gender, this study found significant gender differences in the utilisation of VPN technologies, with male students demonstrating comparatively higher utilisation than female students. This finding corroborates those of Alotaibi and Alshehri (2020), McGill and Thompson (2018), and David-West and Akameze (2022), who found significant gender differences in technology utilisation and cybersecurity behaviour. The finding implies that inadequate utilisation of VPN technologies may expose students' online activities, browsing data, and digital communications to privacy risks and cyber threats within digital learning environments.

## V. CONCLUSION

The study examined the extent of utilisation of cybersecurity applications for safeguarding digital learning among computer science undergraduates in universities in Enugu State, with specific focus on antivirus and anti-malware software, firewalls and intrusion detection/prevention systems, encryption tools, secure authentication mechanisms, and virtual private networks. The findings of the study provide important insights into the current state of cybersecurity practices within digital learning environments in the study area. Based on the empirical evidence obtained, it is concluded that the utilisation of cybersecurity applications among computer science undergraduates in universities in Enugu State is generally low across all identified categories. This suggests that although students operate within technology-driven academic environments and possess foundational knowledge of computing, such knowledge does not sufficiently translate into practical cybersecurity behaviour. The implication is that the digital learning environment remains vulnerable to various forms of cyber threats due to inadequate user-level protection practices. The study further concludes that basic cybersecurity tools such as antivirus software, which are expected to be widely adopted, are still underutilised, while more advanced security measures such as encryption tools and virtual private networks receive even lower levels of utilisation. This indicates a pattern in which students demonstrate limited engagement with both fundamental and advanced cybersecurity mechanisms, thereby exposing digital learning systems to risks such as malware attacks, data breaches, and unauthorised access.

In addition, the findings revealed that the utilisation of secure authentication mechanisms, including multi-factor authentication and two-factor authentication, is also low despite global evidence of their effectiveness in preventing cyber intrusions. This suggests that the issue is not merely the availability of cybersecurity tools but also a lack of consistent adoption, enforcement, and behavioural compliance among students. Furthermore, the study established that there are significant differences between male and female students in their utilisation of cybersecurity applications. This indicates that gender plays a role in shaping cybersecurity behaviour, possibly due to differences in exposure, confidence, or engagement with technical tools. However, the existence of

such differences does not diminish the overall observation that utilisation levels remain low across both groups. Drawing from the theoretical frameworks underpinning the study, it can be concluded that factors such as perceived usefulness and perceived ease of use (Technology Acceptance Model), facilitating conditions (UTAUT), and threat perception and coping appraisal (Protection Motivation Theory) significantly influence the extent to which students utilise cybersecurity applications. The low level of utilisation observed in this study therefore reflects gaps in these constructs, particularly in terms of awareness, motivation, and institutional support. The study concludes that the effectiveness of cybersecurity in digital learning environments within universities in Enugu State is not solely dependent on the availability of technological tools but largely on the extent of their utilisation by students. Consequently, without deliberate efforts to improve awareness, enforcement, and practical engagement with cybersecurity applications, the digital learning ecosystem will continue to face significant security vulnerabilities.

### *A. Practical Implications*

The findings of this study have several practical implications for university administrators, instructors, cybersecurity experts, instructional technology developers, policymakers, and students in higher education institutions. The results showed a significant gender difference in the utilisation of cybersecurity applications among computer science students, with male students demonstrating higher utilisation than female students. These findings suggest that institutions should implement inclusive cybersecurity education programmes to enhance cybersecurity utilisation behaviour among all students, regardless of gender. As such, universities should consider designing practical cybersecurity awareness and digital safety programmes that specifically encourage the participation and engagement of female students in cybersecurity-related activities.

The results also indicated that the level of cybersecurity awareness may not be sufficient for students to demonstrate appropriate cybersecurity utilisation behaviour. In practice, there is a need to promote the effective use of cybersecurity technologies such as antivirus software, firewalls, encryption tools, MFA/2FA, and VPNs to enhance students' digital protection practices in online learning contexts. Therefore, universities should incorporate practical cybersecurity training into computer science curricula and other technology-related academic programmes to improve students' cybersecurity competence and digital safety skills.
The findings further underscore the importance of institutional support mechanisms and environments that facilitate the adoption of cybersecurity applications in universities. Educational institutions should strengthen their cybersecurity infrastructures by implementing secure internet systems, secure learning management systems, secure authentication systems, encrypted communication systems, and institution-wide cybersecurity policies. Robust institutional cybersecurity infrastructures can encourage better cybersecurity utilisation behaviour among students and support more secure digital learning environments. The results also highlight the importance of improving digital identity security within institutional learning systems through the implementation of mandatory Multi-Factor Authentication/Two-Factor Authentication (MFA/2FA) in institutional portals and digital learning environments. MFA/2FA technologies play a critical role in digital security, and universities should prioritise the adoption of secure authentication mechanisms to mitigate the risks of credential theft, phishing attacks, and unauthorised access to academic systems. The findings further suggest that educational policymakers should establish institutional cybersecurity frameworks and digital safety policies to promote cybersecurity preparedness in higher education institutions. Government agencies responsible for educational technology and digital transformation should support universities through cybersecurity capacity-building programmes, digital safety awareness campaigns, and investments in secure digital learning infrastructure.

The findings also indicate that educational technology developers and institutional ICT units should focus on developing user-friendly cybersecurity systems to enhance the adoption and utilisation of cybersecurity applications among students. Students may not consistently use cybersecurity solutions if they are perceived as complex or difficult to operate, particularly when technological trust is low. Therefore, universities should implement accessible, easy-to-use, user-centred, and adaptable cybersecurity tools to support students' digital learning activities. The findings additionally emphasise the importance of fostering a strong cybersecurity culture within universities. Educational institutions should organise regular cybersecurity workshops, seminars, digital safety campaigns, and practical online security training programmes to promote responsible digital behaviour and safe internet practices among students. Strengthening the institutional cybersecurity culture may be a critical factor in reducing the risks associated with unsafe user behaviours in digital learning environments. Finally, the results indicate that increasing the utilisation of cybersecurity applications among students can significantly contribute to securing digital learning environments, strengthening institutional cybersecurity resilience, protecting online privacy, supporting safer academic communication, and promoting sustainable digital transformation in higher education institutions.

### *B. Recommendations*

Based on the findings of the study, the following recommendations are proposed:

1. Universities should regularly organise cybersecurity awareness programmes, workshops, seminars, and practical digital safety training to increase students' utilisation of cybersecurity applications.
2. University management should strengthen institutional cybersecurity infrastructure by implementing effective

antivirus software, firewall systems, authentication technologies, secure communication systems, internet security services, and secure digital learning platforms.

3. Universities should mandate Multi-Factor Authentication/Two-Factor Authentication (MFA/2FA) for institutional portals, online learning platforms, and academic communication systems to enhance digital identity security.
4. Educational institutions should encourage greater participation of female students in cybersecurity-related activities, practical cybersecurity training, and digital protection programmes to bridge the gender gap in cybersecurity utilisation behaviour.
5. Undergraduate computer science programmes should incorporate practical instruction on the application of cybersecurity knowledge to enhance students' cybersecurity competencies and digital protection practices.

### Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

### Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

### Use of Artificial Intelligence (AI)-Assisted Technology for Manuscript Preparation

The authors confirm that no AI-assisted technologies were used in the preparation or writing of the manuscript, and no images were altered using AI.

## REFERENCES

[1] F. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among university students: Knowledge, attitudes, and online safety practices," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, pp. 623–631, 2021, doi: 10.14569/IJACSA.2021.0120476.

[2] F. Alotaibi and M. Alshehri, "Gender differences in cybersecurity behaviour and awareness among university students," *International Journal of Computer Science and Network Security*, vol. 20, no. 7, pp. 137–145, 2020.

[3] M. Alshaikh, "Developing cybersecurity culture to influence employee behaviour: A practice perspective," *Computers & Security*, vol. 98, p. 102003, 2020, doi: 10.1016/j.cose.2020.102003.

[4] V. A. Ani and C. N. Mogboh, "Utilisation of ICT facilities for teaching and learning in universities in Enugu State, Nigeria," *Library Philosophy and Practice*, pp. 1–17, 2021.

[5] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior*, vol. 69, pp. 437–443, 2017, doi: 10.1016/j.chb.2016.12.040.

[6] O. M. Awoleye, W. O. Siyanbola, and F. O. Oladipo, "Cybersecurity awareness and online safety practices among Nigerian university students," *International Journal of Cyber Criminology*, vol. 14, no. 2, pp. 455–470, 2020.

[7] E. Bibangco and R. Villar, "Cybersecurity practices and digital safety behaviour among university students," *International Journal of Information and Education Technology*, vol. 15, no. 2, pp. 110–121, 2025, doi: 10.18178/ijiet.2025.15.2.2035.

[8] O. Binuyo, "Cybersecurity threats and institutional security management in Nigerian universities," *African Journal of Computing & ICT*, vol. 12, no. 3, pp. 55–67, 2019.

[9] A. Bottyán, "Cybersecurity awareness and password management behaviour among university students," *Procedia Computer Science*, vol. 219, pp. 1256–1263, 2023, doi: 10.1016/j.procs.2023.01.401.

[10] A. Branley-Bell, L. Coventry, E. Sillence, A. Joinson, and P. Briggs, "Examining gender differences in online safety behaviour and cybersecurity practices," *Computers & Security*, vol. 112, p. 102519, 2022.

[11] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 5th ed. Thousand Oaks, CA, USA: Sage Publications, 2018.

[12] O. David-West and P. Akameze, "Gender and digital technology utilisation in higher education environments in Nigeria," *International Journal of Education and Development using ICT*, vol. 18, no. 1, pp. 45–61, 2022.

[13] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory," *Computers & Security*, vol. 31, no. 1, pp. 83–95, 2012, doi: 10.1016/j.cose.2011.10.007.

[14] T. McGill and N. Thompson, "Gender differences in information security perceptions and behaviour," in *Proc. Australasian Conference on Information Systems (ACIS)*, 2018, pp. 1–11.

[15] J. C. Nunnally and I. H. Bernstein, *Psychometric Theory*, 3rd ed. New York, NY, USA: McGraw-Hill, 1994.

[16] A. N. Osijirin, S. M. Sada, V. U. Edmond, L. C. Anigbo, and O. Okechukwu, "AI-powered scams and deepfakes in tertiary institutions in Enugu State, Nigeria: The roles of cybersecurity awareness, digital literacy, and media literacy in students' fraud detection preparedness," *Saudi Journal of Engineering and Technology*, vol. 11, no. 4, pp. 355–361, 2026.

[17] J. R. Santelices, "Students' perspectives on cybersecurity awareness and education among students of Catanduanes State University," *International Journal of Advanced Research in Computer Science and Technology*, vol. 13, no. 1, pp. 15–28, 2025.

[18] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, p. 39, 2021, doi: 10.3390/fi13020039.