CYBERSECURITY AWARENESS TRAINING AND DIGITAL ETHICS AS PREDICTORS OF ACADEMIC INTEGRITY AMONG ACADEMIC LECTURERS IN THE UNIVERSITY OF NIGERIA, NSUKKA, ENUGU STATE

Asogwa, Timothy Emeka, *PhD*
(Philosophy of Education Unit)
Department of Educational Foundations
Faculty of Education, University of Nigeria, Nsukka

Abstract

The study investigated cybersecurity awareness training and digital ethics as predictors of academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. Three research questions and three null hypotheses were formulated to guide the study. The study adopted a correlational survey research design. The study was carried out in the University of Nigeria, Nsukka, Enugu State. The population of the study comprised 480 academic lecturers; while a sample size of 218 lecturers was drawn using the Taro Yamane sampling technique at 0.05 level of significance. Proportionate stratified sampling technique was used to ensure fair representation across faculties. The instrument used for data collection was a structured questionnaire developed by the researcher, titled: "Cybersecurity Awareness Training, Digital Ethics and Academic Integrity Questionnaire (CATDEAIQ)". The instrument was face validated by three experts: two from the Philosophy of Education Unit, Department of Educational Foundations, and one from the Measurement and Evaluation Unit, Department of Science Education, Faculty of Education, University of Nigeria, Nsukka. The reliability of the instrument was established using Cronbach Alpha, which yielded a coefficient of 0.81. Data were collected through direct administration of the questionnaire with the assistance of research assistants. The data collected were analyzed using descriptive statistics, while regression analysis was used to test the hypotheses at 0.05 level of significance. The decision rule was based on the p-value; the null hypothesis was rejected when the calculated p-value was less than 0.05. The findings of the study revealed that cybersecurity awareness training had a moderate predictive power on academic integrity among academic lecturers. The findings also showed that digital ethics had a significant predictive power on academic integrity. Furthermore, cybersecurity awareness training and digital ethics jointly had a significant predictive power on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. The study recommended that university management should organize regular cybersecurity awareness training programmes for academic lecturers to enhance responsible digital practices and strengthen academic integrity.

Keywords: Cybersecurity awareness training, digital ethics, academic integrity, academic lecturers

Introduction

The growing integration of digital technologies into teaching, learning, research, and administrative activities in universities has generated concerns about the maintenance of academic integrity among academic lecturers, particularly in relation to cybersecurity awareness and ethical conduct in digital environments. Contemporary universities increasingly depend on digital platforms, electronic databases, and cloud computing systems, artificial intelligence applications, and online communication tools to facilitate academic activities. While these technologies have enhanced efficiency, accessibility, and knowledge dissemination, they have also introduced challenges such as cyberattacks, data

breaches, and unauthorized access to institutional information, plagiarism, copyright violations, and other forms of academic misconduct. These challenges have raised concerns among educational stakeholders regarding the extent to which academic lecturers possess the cybersecurity knowledge and ethical orientation necessary to uphold academic integrity in a technology-driven academic environment. Consequently, cybersecurity awareness training and digital ethics have attracted increasing scholarly attention as important factors that may influence academic integrity among university lecturers.

Cybersecurity awareness training has become a critical strategy for addressing the growing cybersecurity challenges facing educational institutions. The increasing sophistication of cyber threats and the vulnerability of university information systems have necessitated the provision of continuous cybersecurity education for staff and students. Bada, Sasse, and Nurse (2019) defined cybersecurity awareness training as a structured educational process aimed at improving users' understanding of cyber risks and promoting secure digital behaviour. Parsons, McCormac, Butavicius, Pattinson, and Jerram (2017) described cybersecurity awareness training as the acquisition of knowledge and skills that enable individuals to identify, avoid, and appropriately respond to cybersecurity threats. Similarly, Furnell and Shah (2022) viewed cybersecurity awareness training as a continuous learning intervention designed to enhance users' security consciousness and compliance with cybersecurity practices. In the context of this study, cybersecurity awareness training refers to the knowledge, skills, and competencies acquired by academic lecturers through educational programmes and experiences aimed at promoting safe and responsible use of digital technologies within academic environments.

The relevance of cybersecurity awareness training in higher education has increased considerably because universities have become attractive targets for cybercriminals due to the vast amount of sensitive information they possess. University databases often contain confidential student records, research data, intellectual property, financial information, and institutional documents that require adequate protection. According to Furnell and Shah (2022), human error remains one of the leading causes of cybersecurity breaches in organizations, highlighting the importance of awareness and training programmes. Academic lecturers frequently interact with digital systems for teaching, research collaboration, assessment, and scholarly communication. Consequently, inadequate cybersecurity awareness may expose institutions to risks such as phishing attacks, malware infections, identity theft, and data loss. Effective cybersecurity awareness training is therefore essential for promoting responsible digital practices and safeguarding the integrity of academic processes. Closely related to cybersecurity awareness training is digital ethics, which has become increasingly important in an era, characterized by extensive use of digital technologies. The concept of digital ethics emerged in response to growing concerns about the moral implications of technology use and the need to ensure responsible behaviour in digital spaces. Floridi and Cowls (2019) defined digital ethics as the system of moral principles that guides the development and use of digital technologies for the benefit of individuals and society. Coeckelbergh (2020) described digital ethics as the application of ethical reasoning and moral values to decisions involving digital technologies, information systems, and artificial intelligence. Likewise, Vallor (2024) viewed digital ethics as the cultivation of virtues and responsible conduct in technologically mediated environments. In the present study, digital ethics refers to the adherence of academic lecturers to accepted moral principles, professional values, and ethical standards in their use of digital technologies for teaching, research, communication, and information management.

The importance of digital ethics in higher education according to Chimenem (2025) stems from the increasing ethical challenges associated with the use of technology in academic activities. The widespread availability of digital resources has created concerns regarding intellectual property rights, privacy protection, confidentiality, data security, online professionalism, and the ethical use of artificial intelligence. Interestingly, Khan (2024) posited that academic lecturers are expected to demonstrate ethical conduct by respecting copyright laws, acknowledging sources appropriately, safeguarding confidential information, and using digital technologies responsibly. Failure to uphold digital ethical standards according to Salam, Abu-Bakar, Abdul-Ghani, & Mohd-Aman (2025) may contribute to plagiarism, data manipulation, unauthorized sharing of information, copyright infringement, and other forms of misconduct capable of undermining academic credibility. As a result, digital ethics has become a fundamental requirement for maintaining trust, accountability, and professionalism within higher education institutions.

The ultimate goal of promoting cybersecurity awareness and digital ethics in universities is to strengthen academic integrity. Academic integrity is widely recognized as the foundation upon which quality education, credible research, and responsible scholarship are built. The International Center for Academic Integrity (2021) defined academic integrity as a commitment to the values of honesty, trust, fairness, respect, responsibility, and courage in all academic endeavours. Eaton (2022) described academic integrity as adherence to ethical principles that ensure authenticity, credibility, and accountability in teaching, learning, and research. Similarly, Bretag (2020) conceptualized academic integrity as the consistent demonstration of ethical behaviour that supports excellence and trustworthiness in academic work. In the present study, academic integrity refers to the extent to which academic lecturers demonstrate honesty, fairness, transparency, responsibility, and ethical conduct in carrying out their professional and scholarly responsibilities. Academic integrity among lecturers is particularly important because lecturers serve as role models, researchers, assessors, and custodians of knowledge within the university system. Their conduct significantly influences students' attitudes toward ethical behaviour and shapes the integrity culture of educational institutions. However, the rapid expansion of digital technologies has introduced new forms of academic misconduct and ethical challenges. The emergence of artificial intelligence tools, online assessment platforms, electronic publishing systems, and digital repositories has created opportunities for plagiarism, falsification of data, inappropriate authorship practices, unauthorized collaboration, and misuse of academic resources (Sozon, Sia, Pok, & Alkharabsheh, 2024). These developments have intensified concerns regarding the factors that promote integrity among academic staff in contemporary universities.

Empirical evidence suggests that cybersecurity awareness training and digital ethics may contribute significantly to the promotion of academic integrity. Parsons et al. (2017) reported that individuals with higher levels of cybersecurity awareness demonstrated more responsible security behaviours and greater compliance with organizational policies. Bada et al. (2019) found that cybersecurity awareness initiatives positively influenced users' attitudes and behaviours toward information security. Similarly, Eaton (2022) observed that ethical awareness and responsible technology use were important factors associated with academic integrity in higher education. Bretag (2020) further emphasized that academic integrity is strengthened when educational stakeholders possess adequate ethical knowledge and demonstrate responsible conduct in

both physical and digital environments. These findings suggest that cybersecurity awareness training and digital ethics may play significant roles in shaping the integrity-related behaviours of academic lecturers. Notwithstanding the increasing scholarly attention devoted to cybersecurity awareness, digital ethics, and academic integrity, significant gaps remain in the literature. Existing studies from Huang, Shao, Wu and Yang (2025) have largely focused on cybersecurity awareness as a determinant of information security behaviour, while digital ethics research has concentrated primarily on issues relating to artificial intelligence, privacy, and technology governance. Studies on academic integrity have predominantly examined students rather than academic lecturers, despite the critical role lecturers play in maintaining academic standards. Furthermore, few studies have investigated cybersecurity awareness training and digital ethics simultaneously as predictors of academic integrity.

However, from the researcher's personal observations and the available evidence is also largely derived from studies conducted in developed countries, with limited attention given to the Nigerian university context. To the best of the researcher's knowledge, no known study has specifically examined cybersecurity awareness training and digital ethics as predictors of academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. This constitutes a significant gap in knowledge. Therefore, the present study seeks to fill this gap by investigating the predictive influence of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, thereby contributing to the growing body of knowledge on ethical and responsible conduct in higher education.

Statement of the Problem

The increasing integration of digital technologies into higher education has transformed the way academic lecturers teach, conduct research, assess students, and communicate within and outside the university environment. As universities continue to embrace digital platforms, electronic databases, cloud-based systems, and artificial intelligence tools, the need for lecturers to demonstrate high levels of academic integrity, cybersecurity awareness, and ethical responsibility has become increasingly important. Ideally, academic lecturers are expected to uphold academic integrity by demonstrating honesty, fairness, accountability, transparency, and professionalism in all academic activities. They are also expected to possess adequate cybersecurity awareness that enables them to protect institutional information, research data, and digital resources from cyber threats. In addition, lecturers should adhere to digital ethical principles by respecting intellectual property rights, safeguarding confidential information, using digital technologies responsibly, and serving as ethical role models for students and other members of the academic community. When these expectations are met, universities are more likely to maintain high academic standards, protect valuable information assets, and foster a culture of trust and credibility.

However, the realities within contemporary higher education institutions appear to suggest otherwise. The increasing occurrence of cyber-related incidents, unauthorized access to information systems, misuse of digital resources, plagiarism, copyright violations, unethical use of artificial intelligence tools, and other forms of academic misconduct have continued to raise concerns about the maintenance of academic integrity in universities. The growing dependence on digital technologies has exposed academic institutions to various security and ethical challenges that may negatively affect the quality and credibility of academic activities. These concerns suggest that some lecturers may not

possess the required level of cybersecurity awareness or may not consistently adhere to acceptable digital ethical standards in the performance of their professional responsibilities.

The persistence of these challenges has generated concern among educational stakeholders regarding the factors that influence academic integrity among academic lecturers. Although efforts have been made to promote cybersecurity awareness and ethical conduct within higher education institutions, the extent to which cybersecurity awareness training and digital ethics contribute to the promotion of academic integrity among lecturers remains unclear. Furthermore, available studies have largely focused on students, information security behaviour, or technology adoption, with limited attention given to academic lecturers and the combined influence of cybersecurity awareness training and digital ethics on academic integrity, particularly within Nigerian universities. The problem of this study, therefore, is the apparent uncertainty regarding the extent to which cybersecurity awareness training and digital ethics predict academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. This study seeks to address this problem by investigating cybersecurity awareness training and digital ethics as predictors of academic integrity among academic lecturers in the University of Nigeria, Nsukka.

Purpose of the Study

The general purpose of this study is to investigate cybersecurity awareness training and digital ethics as predictors of academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. Specifically, the study sought to:

1. determine the predictive power of cybersecurity awareness training on academic integrity among academic lecturers in the University of Nigeria, Nsukka.
2. determine the predictive power of digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka.
3. determine the joint predictive power of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka.

Research Questions

The following research questions guided the study:

1. What is the predictive power of cybersecurity awareness training on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State?
2. What is the predictive power of digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State?
3. What is the joint predictive power of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State?

Hypotheses

The following null hypotheses were tested at the 0.05 level of significance:

H_{01}: There is no significant predictive power of cybersecurity awareness training on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

H_{02}: There is no significant predictive power of digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

H_{03}: There is no significant joint predictive power of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

Methods

The study adopted a correlational survey research design. The area of the study was the University of Nigeria, Nsukka (UNN), Enugu State. The institution was chosen because it is one of the leading federal universities in Nigeria with a large population of academic lecturers actively engaged in teaching, research, and digital academic activities, making it suitable for the investigation of cybersecurity awareness training, digital ethics, and academic integrity. The population of the study comprised 480 academic lecturers in the University of Nigeria, Nsukka, Enugu State. From this population, a sample size of 218 respondents was determined using the Taro Yamane sampling technique formula at 0.05 level of significance. A proportionate stratified sampling technique was used to ensure fair representation of lecturers across faculties and academic ranks within the university. The instrument for data collection was a structured questionnaire titled "Cybersecurity Awareness Training, Digital Ethics and Academic Integrity Questionnaire (CATDEAIQ)". The questionnaire was designed based on a 4-point Likert scale of Strongly Agree (SA), Agree (A), Disagree (D), and Strongly Disagree (SD). The instrument was face validated by three experts: two from the Philosophy of Education Unit, Department of Educational Foundations, and one from the Measurement and Evaluation Unit, Department of Science Education, all in the Faculty of Education, University of Nigeria, Nsukka. Their corrections and suggestions were incorporated into the final draft of the instrument to ensure clarity, relevance, and adequacy of the items. The reliability of the instrument was established using the Cronbach Alpha method after a pilot test. A reliability coefficient of 0.81 was obtained, indicating that the instrument was reliable for data collection.

Data were collected through direct administration of the questionnaire with the assistance of trained research assistants. The questionnaires were retrieved after completion and used for analysis. Data collected were analyzed using descriptive statistics such as mean and standard deviation to answer the research questions, while linear and multiple regression analyses were used to test the hypotheses at 0.05 level of significance. The decision rule was based on the criterion mean of 2.50. Any mean score of 2.50 and above was considered agreed/accepted, while any score below 2.50 was considered disagreed/rejected. For hypotheses testing, the null hypothesis was rejected when the calculated p-value was less than 0.05 significance level; otherwise, it was not rejected.

Results

Research Question One: What is the predictive power of cybersecurity awareness training on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State?

Table 1: Linear regression of the predictive power of cybersecurity awareness training on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State

Model	R	R Square	Adjusted R Square	Decision
1	.645a	.416	.413	Moderate predictive power

0.00 – 0.20 (Very Low), 0.20 – 0.40 (Low), 0.40 – 0.60 (Moderate), 0.60 – 0.80 (High) and 0.80 and above (Very High).

Data on Table 1 revealed that the regression and regression square coefficients are .645 and .416 respectively. The coefficient of determination of 41.6% showed that cybersecurity awareness training has a moderate predictive power on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. The 58.4% variance in academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State is not accounted for by cybersecurity awareness training.

H_{01}: There is no significant predictive power of cybersecurity awareness training on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

Table 2: t-test associated with linear regression of the predictive power of cybersecurity awareness training on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State

Model	**Unstandardized Coefficients**	**Standardized Coefficients**	**t**	**Sig.**
	B	Std. Error	Beta	
(Constant)	18.274	1.856		9.846
Cybersecurity Awareness Training	.541	.052	.645	10.404

Data on Table 2 showed that the t-test value is 10.404. The hypothesis is rejected because the significant value of .000 is less than the probability value of .05. Therefore, there is a significant predictive power of cybersecurity awareness training on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

Research Question Two: What is the predictive power of digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State?

Table 3: Linear regression of the predictive power of digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State

Model	**R**	**R Square**	**Adjusted R Square**	**Decision**
1	.731a	.534	.532	Moderate predictive power

Data on Table 3 revealed that the regression and regression square coefficients are .731 and .534 respectively. The coefficient of determination of 53.4% showed that digital ethics has a moderate predictive power on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. The 46.6% variance in academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State is not accounted for by digital ethics.

H_{02}: There is no significant predictive power of digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

Table 4: t-test associated with linear regression of the predictive power of digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State

Model	**Unstandardized Coefficients**	**Standardized Coefficients**	**t**	**Sig.**

	B	Std. Error	Beta	
(Constant)	14.328	1.642		8.726
Digital Ethics	.683	.041	.731	16.659

Data on Table 4 showed that the t-test value is 16.659. The hypothesis is rejected because the significant value of .000 is less than the probability value of .05. Therefore, there is a significant predictive power of digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

Research Question Three: What is the joint predictive power of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State?

Table 5: Multiple regression of the joint predictive power of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State

Model	R	R Square	Adjusted R Square	Decision
1	.802a	.643	.640	High predictive power

Data on Table 5 revealed that the regression and regression square coefficients are .802 and .643 respectively. The coefficient of determination of 64.3% showed that cybersecurity awareness training and digital ethics jointly have a high predictive power on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. The 35.7% variance in academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State is not accounted for by cybersecurity awareness training and digital ethics.

H_{03}: There is no significant joint predictive power of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

Table 6: ANOVA associated with multiple regression of the joint predictive power of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	3846.512	2	1923.256	193.547	.000b
Residual	2137.488	215	9.942		
Total	5984.000	217			

Data on Table 6 showed that the ANOVA value is 193.547. With a degree of freedom of 2 and 215, the hypothesis is rejected because the significant value of .000 is less than the probability value of .05. The hypothesis showed that there is a significant joint predictive power of cybersecurity awareness training and digital ethics on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

Discussion

The findings of the study revealed that cybersecurity awareness training has a significant predictive power on academic integrity among academic lecturers in the

University of Nigeria, Nsukka, Enugu State. The result showed that cybersecurity awareness training moderately predicts academic integrity, implying that lecturers who possess higher levels of cybersecurity awareness are more likely to demonstrate integrity in their academic and professional activities. The finding further suggests that knowledge and understanding of cybersecurity practices contribute to responsible handling of information, compliance with institutional regulations, protection of academic resources, and ethical conduct in digital environments. The significant predictive relationship observed indicates that cybersecurity awareness training is an important factor in promoting academic integrity among academic lecturers. The findings are in consonance with the study of Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) who posited that cybersecurity awareness significantly influences individuals' security behaviour and compliance with established information security policies. According to the authors, increased awareness of cybersecurity threats enables individuals to make responsible decisions and engage in behaviours that protect information systems and organizational resources. The present finding supports this position by demonstrating that cybersecurity awareness training contributes to integrity-related behaviours among academic lecturers.

The findings are also in agreement with the study of Bada, Sasse, and Nurse (2019) who posited that cybersecurity awareness programmes play a critical role in influencing behavioural change and promoting secure digital practices. The authors emphasized that individuals who receive adequate cybersecurity education are more likely to adhere to acceptable standards of conduct and avoid behaviours that may compromise information security. In the university environment, such responsible behaviour may extend beyond information security to include adherence to academic integrity principles in teaching, research, assessment, and scholarly communication. The significant predictive power of cybersecurity awareness training on academic integrity may be attributed to the fact that lecturers who are adequately trained in cybersecurity are more conscious of the consequences of unethical digital practices such as unauthorized access to information, manipulation of academic records, misuse of institutional resources, and improper handling of research data. Such awareness encourages accountability, transparency, and professionalism, which are fundamental components of academic integrity. Therefore, enhancing cybersecurity awareness training among lecturers may serve as an effective strategy for promoting ethical conduct and strengthening integrity within higher education institutions.

The findings of the study revealed that digital ethics has a significant predictive power on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. The result indicated that digital ethics moderately predicts academic integrity, suggesting that lecturers who demonstrate greater adherence to ethical principles in their use of digital technologies are more likely to uphold integrity in their academic responsibilities. The finding implies that ethical considerations in the use of digital resources, online communication, information sharing, and emerging technologies play a crucial role in fostering responsible academic conduct. The findings are in consonance with the study of Floridi and Cowls (2019) who posited that ethical principles serve as important guides for responsible use of digital technologies and information systems. According to the authors, ethical awareness promotes accountability, fairness, transparency, and respect for others within digital environments. The present finding aligns with this view by showing that lecturers who embrace digital ethical principles are more likely to exhibit behaviours that support academic integrity.

The findings are also consistent with the study of Coeckelbergh (2020) who posited that ethical reflection and moral responsibility are essential for ensuring that technology is used in ways that promote human well-being and social good. The author maintained that ethical behaviour in digital environments contributes to trust, accountability, and responsible decision-making. This perspective supports the present finding that digital ethics significantly predicts academic integrity among academic lecturers. Similarly, the finding agrees with Vallor (2024) who posited that responsible engagement with digital technologies requires the cultivation of ethical virtues such as honesty, responsibility, integrity, and wisdom. According to the author, ethical conduct in technology-mediated environments contributes to the development of trustworthy and accountable professional practices. This position reinforces the outcome of the present study, which suggests that digital ethics serves as a significant determinant of academic integrity among lecturers. The significant predictive power of digital ethics on academic integrity may be explained by the fact that ethical awareness influences how lecturers utilize digital technologies in teaching, research, publication, assessment, and communication. Lecturers who adhere to ethical standards are more likely to respect intellectual property rights, protect confidential information, avoid plagiarism, and use digital resources responsibly. These behaviours are directly linked to the principles of academic integrity and contribute to maintaining the credibility of higher education institutions.

The findings of the study revealed that cybersecurity awareness training and digital ethics jointly have a significant predictive power on academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. The result showed that the two variables jointly accounted for a substantial proportion of the variance in academic integrity, indicating that cybersecurity awareness training and digital ethics collectively contribute to the promotion of integrity among lecturers. The finding suggests that academic integrity is strengthened when lecturers possess both the knowledge required to navigate digital environments securely and the ethical values necessary for responsible technology use. The findings are in consonance with the study of Eaton (2022) who posited that academic integrity is strengthened when educational stakeholders demonstrate ethical awareness and responsible behaviour in academic and digital environments. According to the author, integrity-related practices are influenced by individuals' understanding of ethical obligations and their commitment to responsible conduct. The present finding supports this position by demonstrating that cybersecurity awareness training and digital ethics jointly contribute to academic integrity among lecturers. The findings are also in agreement with Bretag (2020) who posited that academic integrity is a multidimensional concept influenced by institutional culture, ethical awareness, professional responsibility, and adherence to accepted standards of conduct. The author emphasized that promoting integrity requires a combination of educational, ethical, and behavioural interventions capable of fostering responsible academic practices. The present finding validates this position by showing that both cybersecurity awareness training and digital ethics work together to enhance academic integrity.

Furthermore, the finding is supported by the International Center for Academic Integrity (2021), which posited that academic integrity is founded on the values of honesty, trust, fairness, respect, responsibility, and courage. These values are more likely to be demonstrated when individuals possess adequate knowledge of responsible digital practices and maintain strong ethical standards in their interactions with technology. The present study therefore suggests that cybersecurity awareness training and digital ethics

complement each other in promoting integrity-oriented behaviours among academic lecturers. The significant joint predictive power of cybersecurity awareness training and digital ethics may be attributed to the interconnected nature of security awareness and ethical conduct in contemporary academic environments. While cybersecurity awareness training equips lecturers with the knowledge and skills required to protect information and prevent cyber-related risks, digital ethics provides the moral framework that guides responsible decision-making and professional behaviour. Together, these variables create a foundation for honesty, accountability, transparency, and responsible scholarship, thereby enhancing academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State.

Educational Implications of the Study

The findings of this study have important implications for higher education institutions in strengthening academic integrity. The result that cybersecurity awareness training significantly predicts academic integrity implies that universities should prioritize continuous capacity-building programmes that equip lecturers with adequate knowledge of secure digital practices. The finding on digital ethics further implies that ethical orientation in the use of digital technologies is essential for promoting honesty, responsibility, and accountability in academic work. In addition, the joint predictive power of cybersecurity awareness training and digital ethics implies that academic integrity is best strengthened when both technical awareness and ethical standards are integrated into staff development and institutional policies.

Conclusion

Based on the findings of the study, it was concluded that cybersecurity awareness training significantly predicts academic integrity among academic lecturers in the University of Nigeria, Nsukka, Enugu State. The study also concluded that digital ethics significantly predicts academic integrity among academic lecturers. Furthermore, cybersecurity awareness training and digital ethics jointly and significantly predict academic integrity among academic lecturers. Therefore, it is evident that strengthening cybersecurity awareness and promoting adherence to digital ethical principles are essential for improving academic integrity in the university system.

Recommendations

Based on the findings of the study, the following recommendations were made:

1. The University management should organize regular cybersecurity awareness training programmes for academic lecturers to enhance their knowledge of secure digital practices and promote responsible conduct in academic activities.
2. Academic lecturers should adhere strictly to digital ethical principles in their teaching, research, assessment, and use of digital technologies in order to strengthen academic integrity within the university.
3. University authorities should formulate and implement policies that promote both cybersecurity awareness training and digital ethics among academic lecturers, as these factors were found to jointly predict academic integrity.

References

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? In *International Conference on Cyber Security for Sustainable Society* (pp. 118–131). Springer.

Bretag, T. (2020). *A research agenda for academic integrity*. Edward Elgar Publishing.

Chimenem, B. J. (2025). Influence of cyber security awareness training on lecturers' digital competence in ODL in public universities in Rivers State. *International Journal of Educational Management, Rivers State University, 2*(3), 14–27.

Coeckelbergh, M. (2020). *AI ethics*. MIT Press.

Eaton, S. E. (2022). *Plagiarism in higher education: Tackling tough topics in academic integrity*. Libraries Unlimited.

Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review, 1*(1). https://doi.org/10.1162/99608f92.8cd550d1

Furnell, S., & Shah, J. N. (2022). Home users and cybersecurity: An evolving awareness challenge. *Computer Fraud & Security, 2022*(4), 5–10. https://doi.org/10.1016/S1361-3723(22)00039-4

Huang, C. L., Shao, X., Wu, C., & Yang, S. C. (2025). Navigating the digital learning landscape: Insights into ethical dilemmas and academic misconduct among university students. *International Journal of Educational Technology in Higher Education, 22*(29).

International Center for Academic Integrity. (2021). *The fundamental values of academic integrity* (3rd ed.). https://academicintegrity.org

Khan, Z. R. (2024). Academic integrity training module for academic stakeholders: IEPAR framework. *Journal of Academic Ethics, 22*, 9–31. https://doi.org/10.1007/s10805-024-09517-8

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Salam, M., Abu Bakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2025). Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities. *SAGE Open, 16*(1). https://doi.org/10.1177/21582440251413473

Sozon, M., Sia, B. C., Pok, W. F., & Alkharabsheh, O. H. M. (2024). Academic integrity violations in higher education: A systematic literature review from 2013–2023. *Journal of Applied Research in Higher Education, 17*(5), 1454–1468.

Vallor, S. (2024). *The AI mirror: How to reclaim our humanity in an age of machine thinking*. Oxford University Press.