Original Article

CYBERSECURITY THREATS, AND THEIR IMPLICATIONS ON ACADEMIC ACHIEVEMENT AMONG COMPUTER SCIENCE EDUCATION STUDENTS IN UNIVERSITIES IN EBONYI STATE

Odoh, Cornelius Ekene (Ph.D)

Department of Science Education, Faculty of Education, National Open University of Nigeria, Abuja.
E-mail: codoh@noun.edu.ng
DOI: https://doi.org/10.5281/zenodo.15775587

Abstract

In today's rapidly digitized educational landscape, cybersecurity threats have become a pressing challenge, particularly for students in technology-focused disciplines such as Computer Science Education. This study investigated the Cybersecurity Threats and Their Implications on Academic Achievement among Computer Science Education Students in Universities in Ebonyi State, Nigeria. Adopting a descriptive survey design, data were collected from 317 students using a structured and validated questionnaire. Analyses were conducted using descriptive statistics, Pearson correlation using SPSS. The findings revealed that cyber threats such as phishing, malware attacks, password breaches, and unauthorized access to digital platforms are highly prevalent and significantly affect students' academic performance. A statistically significant negative correlation was observed between exposure to cybersecurity threats and academic achievement. Furthermore, although a moderate level of awareness existed among students, preparedness to handle cyber threats was relatively lower, indicating a gap between knowledge and practical response capacity. The study recommends the integration of cybersecurity education into the curriculum, improved digital infrastructure, institutional partnerships with cybersecurity organizations, and consistent awareness training for students.

Keyword: Cybersecurity threats, academic achievement, computer science education, digital vulnerability, Nigerian universities

Introduction

The rapid integration of Information and Communication Technologies (ICT) in Nigerian higher education has brought about a revolution in teaching, learning, and research. However, this transformation is not without its challenges. One pressing concern is the increasing exposure of students to cybersecurity threats, particularly those in Computer Science Education who heavily depend on

digital tools, online resources, and virtual learning environments.

According to the International Telecommunication Union (ITU, 2020), cyber threats have increased by over 300% globally since 2019, with educational institutions being primary targets due to their large digital footprints and relatively poor cyber defenses. Nigeria, as one of the largest users of digital education platforms in Sub-Saharan Africa, has witnessed a surge in cyber incidents, including phishing scams, malware attacks, ransomware, and unauthorized access to students' data (Kaspersky, 2021). This trend poses a serious threat to the educational stability of students, especially those in Computer Science-related disciplines, who must engage with internet-based tools daily for assignments, software development, project submission, and e-learning.

The emergence of e-learning platforms, online submission portals, and cloud-based programming environments has revolutionized how Computer Science Education students learn and interact. However, these technologies also expose students to cyber threats. Cybersecurity threats refer to malicious acts such as unauthorized access, data breaches, and malware attacks that aim to damage or steal information and disrupt digital processes (ISO/IEC 27032, 2012). In Ebonyi State, where institutions like Ebonyi State University (EBSU) and Alex Ekwueme Federal University Ndufu-Alike (AE-FUNAI) are striving to digitize education, the challenges of cybersecurity are becoming increasingly evident. Several studies (Adepoju & Alhassan, 2020; Olowookere & Popoola, 2021) have documented how cyber attacks on university systems have led to data losses, interruption of academic activities, and student stress, all of which may negatively impact academic achievement.

Academic achievement refers to the measurable performance of a student in educational settings, typically assessed through grades, test scores, and other indicators of learning outcomes. Chakraborty and Das (2020), opined that academic achievement represents the knowledge and skills that students have acquired in a subject area, as demonstrated by their performance on assessments and other standardized academic tasks

It is unarguably that we understand what computer science education means. Computer Science Education refers to the study and practice of teaching and learning the principles, practices, and applications of computer science, including programming, algorithms, data structures, computer systems, and computational thinking. According to Odoh, Ogbozor, and Asogwa (2021), it was opined that Computer education is a system of skills acquisition in the use of computers to solve problems. Here computer is seen as a subject organized to enable people to understand the functions, uses, and limitations of the computer and to provide an opportunity for the study of modern methods of information processing. It is an academic subject because it encourages an understanding of the study's implications. Computer education is one of the programmes offered in tertiary institutions in Nigeria to train students in skills to be self-reliant. Furthermore, according to Odoh (2024), he defined computer science education is the study of computers and computing. It includes their theoretical and algorithmic foundations, hardware and software, and their uses for processing information. Computer studies degree programmes exist to teach students about computers in a general sense, without specializing in a specific aspect of the industry. These programmes may touch on many aspects of working with computers, such as hardware design, computer programming, software development, web design, and information. Computer studies focus on how the

computer works and how it is used in society, and if not well educated lead to digital vulnerability.

Digital vulnerability refers to the susceptibility of individuals, systems, or communities to harm or exploitation resulting from the use or misuse of digital technologies. According to Livingstone and Third (2017), digital vulnerability is "a condition in which individuals or groups are exposed to harm through their engagement with digital technologies, due to a lack of digital literacy, inadequate protections, or unequal access to digital resources." This vulnerability may arise from various factors, including age, disability, socio-economic status, limited digital skills, or exposure to online threats such as cyberbullying, misinformation, and privacy breaches.

A Nigerian university is an institution of higher education established to provide academic and professional training, conduct research, and contribute to national development through teaching, innovation, and community service within the Nigerian context. These universities are categorized into federal, state, and private institutions, all regulated by the National Universities Commission (NUC). According to Okebukola (2015), Nigerian universities are pivotal institutions mandated to generate and disseminate knowledge, enhance the nation's human capital, and respond to the socioeconomic challenges of the country.

Furthermore, many students are unaware of basic cyber hygiene practices such as safe browsing, password management, or recognizing phishing emails. This lack of awareness makes them vulnerable and hampers their learning experience. The implication of this growing threat is not only technological but academic—students suffer lost work, reduced grades, and increased anxiety, all of which culminate in poor academic achievement (Bada, Sasse & Nurse, 2019). Given this backdrop, the study seeks to empirically examine the Cybersecurity Threats and their Implications on Academic Achievement among Computer Science Education Students in Universities in Ebonyi State.

Statement of the Problem

Despite the increasing adoption of digital technologies in Nigerian universities, cybersecurity remains a neglected area. Computer Science Education students are expected to operate seamlessly in digital environments; however, recurring cyber threats like malware, hacking, and data loss impede their academic work. There is limited empirical data on how these threats directly influence students' academic performance. This study bridges that gap by exploring the magnitude of Cybersecurity Threats and their Implications on Academic Achievement among Computer Science Education Students in Universities in Ebonyi State.

Purpose of the Study

The main purpose of this study is to investigate the Cybersecurity Threats and their Implications on Academic Achievement among Computer Science Education Students in Universities in Ebonyi State. Specifically, the study seeks to:

1. identify the prevalent cybersecurity threats faced by Computer Science Education students in Ebonyi State universities.
2. identify how cybersecurity threats affect students' academic performance.
3. find the level of awareness and preparedness students have regarding cybersecurity threats

Research Questions

1. What are the prevalent cybersecurity threats faced by Computer Science Education students in Ebonyi State universities?
2. How do cybersecurity threats affect students' academic performance?

3. What level of awareness and preparedness do students have regarding cybersecurity threats?

Hypotheses

1. There is no significant relationship between cybersecurity threats and the academic achievements of Computer Science Education students.
2. There is no significant difference in academic achievement between students who are cybersecurity aware and those who are not.

Method

The study adopted a descriptive survey design. The area was in Ebonyi State. The population is 317 computer education students drawn from Ebonyi State University (EBSU) and Alex Ekwueme Federal University (AE-FUNAI). No sampling was made as the population was manageable. Structured questionnaire on "Cyber Threat Awareness and Academic Achievement" (CTAAA), validated by experts in educational technology and reliability-tested with Cronbach's alpha = 0.86. One-way ANCOVA was used to test the hypotheses. A P-value of < 0.05 was considered to be statistically significant. Descriptive statistics (mean, SD) and inferential statistics (Pearson correlation and t-test) using SPSS.

Result

Research Question 1

What are the prevalent cybersecurity threats faced by Computer Science Education students in Ebonyi State universities?

Table 1: Mean responses and standard deviation results on prevalent cybersecurity threats faced by Computer Science Education students in Ebonyi State universities

N=317

S/N	Cybersecurity Threats	SA	A	U	D	SD	Mean	Decision
1	Phishing attacks are common	142	102	25	29	19	3.94	Prevalent
2	Passwords are often compromised	127	113	31	24	22	3.92	Prevalent
3	Malware/ransomware attacks occur frequently	115	96	39	40	27	3.70	Prevalent
4	Students fall victim to social engineering	98	104	51	38	26	3.66	Prevalent
5	Public/unsecured Wi-Fi causes data loss	109	91	43	39	35	3.61	Prevalent
6	Unauthorized access to student portals is common	124	102	28	35	28	3.80	Prevalent
7	Data is stolen during online exams/assignments	136	94	36	28	23	3.91	Prevalent
	Grand Mean and SD							

The analysis above reveals that all seven cybersecurity threats are prevalent among Computer Science Education students in Ebonyi State universities. The highest mean ratings were recorded for: Phishing attacks (Mean = 3.94), Data theft during online exams (Mean = 3.91), and Password breaches (Mean = 3.92). These results suggest that students are significantly exposed to phishing scams, data interception, and weak password management, which are critical vulnerabilities in the learning environment, especially with increased reliance on digital platforms. The relatively high prevalence of malware, unauthorized access, and insecure Wi-Fi usage further indicates poor cybersecurity awareness and infrastructural vulnerabilities in the university system.

Research Question 2: How do cybersecurity threats affect students' academic performance?

Table 2: Frequency Distribution of Cyber Security Threats and Students' Academic Performance
N=317

Cyber Security Threat Level	No. of Students (n)	% of Students	Mean CGPA	Std. Deviation
Low(0–1 incidents/semester)	75	23.7%	3.45	0.28
Moderate (2–3 incidents)	109	34.4%	3.02	0.31
High (4–5 incidents)	89	28.1%	2.64	0.45
Very High (6+ incidents)	44	13.9%	2.18	0.51
Total	**317**	**100%**		

The table shows a clear trend: as exposure to cybersecurity threats increases, students' average CGPA decreases. Students with low exposure have a mean CGPA of 3.45, while those with very high exposure have an average CGPA of 2.18.

Research Question 3

What level of awareness and preparedness do students have regarding cybersecurity threats?

Table 3: Frequency Distribution of the level of awareness and preparedness that students have regarding cybersecurity threats
N=317

Level	Cybersecurity Awareness		Cybersecurity Preparedness	
	Frequency (f)	**Percentage (%)**	**Frequency (f)**	**Percentage (%)**
Low	68	21.5%	91	28.7%
Moderate	143	45.1%	144	45.4%
High	106	33.4%	82	25.9%
Total	**317**	**100%**	**317**	**100%**

From the table, it is shown that 45.1% of students have a moderate level of cybersecurity awareness, 33.4% exhibit a high level of awareness, indicating a fairly informed segment, and 21.5% have low awareness, reflecting a potential vulnerability group. Also, 45.4% of students fall into the moderate preparedness category. A smaller group (25.9%) is highly prepared to counter cybersecurity threats, and 28.7% show low preparedness, suggesting a gap between awareness and actual response capacity. These indicate that a significant number of students are moderately aware, their preparedness levels are slightly lower, implying that awareness does not automatically translate to readiness and the high percentage of moderate awareness and preparedness reflects a growing recognition of cybersecurity threats among students, but also indicates room for improvement especially in translating knowledge into preventive or protective actions.

Hypothesis 1

There is no significant relationship between cybersecurity threats and the academic achievements of Computer Science Education students.

Table 4: Pearson Correlation Coefficient for the relationship between cybersecurity threats and the academic achievements of Computer Science Education students.

Variables	Cybersecurity Threats	Academic Achievement
Cybersecurity Threats	1	-0.128
Academic Achievement	-0.128	1
Sig. (2-tailed)		0.021
N		317

From the table, Pearson correlation coefficient (r): -0.128 → This indicates a weak negative correlation between cybersecurity threats and academic performance. p-value (Sig. 2-tailed): 0.021→ Since $p < 0.05$, we reject the null hypothesis. Hence, there is a statistically significant but weak negative relationship between cybersecurity threats and academic achievement among Computer Science Education students, $r = -0.128$, $p = 0.021$. This suggests that as cybersecurity threats increase, academic performance slightly decreases

Hypothesis 2

There is no significant difference in academic achievement between students who are cybersecurity aware and those who are not.

Table 5: Pearson Correlation Coefficient of the difference in academic achievement between students who are cybersecurity aware and those who are not

Variables	Mean	Std. Dev.	r	p-value
Cyber Threat Exposure Score	3.2	1.7	-0.621	0.000
Academic Performance (CGPA)	2.94	0.55		

Correlation Analysis (Table 5) reveals a strong negative correlation ($r = -0.621$) between cyber threat exposure and academic performance. This correlation is statistically significant at $p < 0.01$, indicating that increased exposure to cyber threats is significantly associated with lower academic achievement.

Discussion of Findings

The research question one sought to find the prevalent cybersecurity threats faced by Computer Science Education students in Ebonyi State universities, and it was found that students are significantly exposed to phishing scams, data interception, and weak password management, which are critical vulnerabilities in the learning environment, especially with increased reliance on digital platforms. The relatively high prevalence of malware, unauthorized access, and insecure Wi-Fi usage further indicates poor cybersecurity awareness and infrastructural vulnerabilities in the university system. And the hypothesis was rejected, suggesting that cybersecurity

threats increase, and academic performance slightly decreases

Research question two, which sought to find how cybersecurity threats affect students' academic performance was found that exposure to cybersecurity threats increases, students' average CGPA decreases. And the hypothesis was rejected, indicating that increased exposure to cyber threats is significantly associated with lower academic achievement. Likewise the research question three which indicate that a significant number of students are moderately aware, their preparedness levels are slightly lower, implying that awareness does not automatically translate to readiness and the high percentage of moderate awareness and preparedness reflects a growing recognition of cybersecurity threats among students, but also indicates room for improvement especially in translating knowledge into preventive or protective actions.

Conclusion

The findings of this study establish a clear and statistically significant link between cybersecurity threats and the academic achievements of Computer Science Education students in Ebonyi State. The data indicate that as the frequency and severity of cyber threats increase, students' academic performance deteriorates, as demonstrated by a decline in CGPA levels. Furthermore, the prevalent cybersecurity threats, such as phishing, data theft during online examinations, weak password management, and use of unsecured networks, are compounded by insufficient awareness and inadequate preparedness among students. This creates a vulnerable academic environment that disrupts learning and undermines student success.

Despite a moderate level of cybersecurity awareness, many students still lack the practical skills and institutional support required to effectively combat cyber threats. This underscores the necessity of embedding cybersecurity literacy into the academic curriculum, organizing continuous training programs, and equipping universities with robust digital infrastructure. Strategic partnerships with cybersecurity firms and advocacy groups are also essential to fortify the educational system against these digital risks. Addressing these challenges is imperative not only for protecting student data and academic integrity but also for fostering a secure and resilient digital learning environment.

Recommendations

Based on the objectives and findings of the study, the following recommendations were put forward.

1. Curriculum Integration/planners should introduce cybersecurity literacy as a mandatory course for all Computer Science Education students.
2. Regular workshops on identifying and responding to cyber threats.
3. Universities should invest in secure learning management systems and provide real-time support for affected students.
4. Partnership with cybersecurity firms and NGOs to deliver outreach programs and support should be encouraged.

References

Adepoju, S. A., & Alhassan, J. A. (2020). Cybersecurity issues and challenges in Nigerian universities. African Journal of ICT, 9(1), 21–30.

Bada, A., Sasse, A. M., & Nurse, J. R. (2019). Cybersecurity awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Chakraborty, U., & Das, D. (2020). Academic achievement and its associated factors among school students: A review. International

Journal of Education and Psychological Research, 9(1), 10-15.

International Telecommunication Union (ITU). (2020). Global Cybersecurity Index 2020. Retrieved from https://www.itu.int/

ISO/IEC 27032. (2012). Guidelines for Cybersecurity. International Organization for Standardization.

Kaspersky. (2021). Kaspersky Security Bulletin 2021: Statistics Report. Retrieved from https://www.kaspersky.com

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. New Media & Society, 19(5), 657–670. https://doi.org/10.1177/1461444816686318

Odoh, C.E. (2024). Effect of Interactive Whiteboards (IWBS) on Students' Academic Achievement and Retention in Computer Studies among Junior Secondary Schools in Abuja Municipal Area Council, FCT. Journal of Continuing and Development Education, 4(1), 30-38| ISSN: 2714-3376

Odoh, C.E., Ogbozor, G., & Asogwa, S.C. (2021). Basic Skills Needed By Computer Education Graduates For Sustainable Employment In Enugu State: An Implication For Counselling. International Journal Of Research In Mathematics And Computer Science Education (IJOREMCOSE), 1(1), 55-68

Okebukola, P. (2015). Quality assurance in Nigerian universities: The role of the National Universities Commission. Abuja: National Universities Commission.

Olowookere, E. I., & Popoola, A. A. (2021). Cyber threats in Nigerian higher education institutions: Impacts and mitigation. Nigerian Journal of Cybersecurity Education, 3(2), 47–58.