

CYBERSECURITY THREATS EXPERIENCED BY COMPUTER AND BUSINESS EDUCATION STUDENTS AND THEIR EFFORTS TO SOLVE THEM

¹Uba, Mabel Obianuju and ²Dr. Chinenye Clara Akpa

Department of Computer and Robotics Education, University of Nigeria, Nsukka

Department of Business Education, Federal College of Education Ofeme, Ohuhu
Umuahia Abia State

Email: mabel.nnacheta@unn.edu.ng

ABSTRACT

Internet usage has grown exponentially, with individuals and companies performing multiple daily transactions in the Cyberspace rather than in the real world. This study investigated the Cybersecurity threats experienced by Computer and Business Education Students and their efforts to solve them. Two specific purposes and two research questions were raised to guide the study. The study adopted a descriptive survey research design in Cybersecurity threats experienced by Computer and Business Education Students and their subsequent mitigation efforts. The population for the study was 250 Undergraduate Students from Computer and Business Education second year students in Federal Universities in South East Nigeria, the results of the study identified a high prevalence of social engineering attacks, particularly phishing (78%) and malware incidents (62%), often linked to software privacy and vulnerable personal projects. Based on these results, it was recommended among others that Universities should ensure that Students have affordable or free access to necessary commercial software through campus-wide licenses or academic partnerships, reducing the incentive for piracy.

Keywords: Cybersecurity, Phishing, Malware, Student Security, Self-Efficacy, Threat Mitigation

Introduction

In the digital age, cybersecurity has emerged as one of the most critical sectors for safeguarding national security, protecting personal data, and ensuring the stability of global economies and education sectors. Digital landscape of higher education is increasingly complex with students relying on a myriad of personal devices, cloud services, and online platforms for their academic and personal lives. Within this ecosystem, students enrolled in Computer and Business Education programmes represent a critical group. The students were not merely end-users; but were developers, network administrators, and system analysts in training. The coursework often requires students to engage with potentially vulnerable software, experiment with network configurations and access a wide array of online resources, including unofficial software repositories. This high level of engagement with technology

paradoxically increases their attack surface in cybersecurity (Maczak, Akdogan, & Ashmore, 2023).

Cybersecurity involves the application of technologies, processes, and controls to protect systems, networks, programmes, and data from cyberattacks (Li & Liu, 2021), as well as safeguarding digital assets against unauthorised access, use, disruption, modification, or disclosure (Wu & Wu, 2021). As one of the most in-demand skill areas for Information Systems graduates, cybersecurity has become central to contemporary computing curricula. However, there remains a substantial global shortage of skilled cybersecurity professionals (Vogel, 2016; John et al., 2020; Triplett, 2023), with an estimated workforce gap of nearly 3.5 million professionals worldwide (Matthew, 2021). This shortage underscores the urgent need for educational

institutions to strengthen cybersecurity training programmes.

Cybersecurity education broadly encompasses technical (hard) skills and soft skills. Technically, professionals require competencies in networking and system administration, including access management, intrusion detection, and incident response (Flin & O'Connor, 2017; Fauziyah et al., 2022). Proficiency across multiple operating systems, such as Windows, macOS, Linux, and Ubuntu, is also essential for safeguarding organisational data and networks (Akhtar, 2024). Given the regulatory diversity across sectors, cybersecurity professionals must also remain current with compliance requirements and emerging threats.

Beyond technical expertise, effective cybersecurity practice requires strong soft skills, including communication, collaboration, analytical thinking, problem-solving, adaptability, critical thinking, active listening, and lifelong learning (Graham & Lu, 2023; Pham et al., 2021; Tagarev, 2020; Alqurashi & Ahmad, 2024; Fathoni et al., 2024; Kwon et al., 2021; Dillon et al., 2021; Lewrick et al., 2020; Hussain et al., 2024; Uchendu et al., 2021). These competencies enable professionals to interpret complex data, respond creatively to incidents, and communicate solutions effectively in dynamic environments. Consequently, both Computer and Business Education students constitute credible sources for identifying the cybersecurity threats experienced by students for effective cybersecurity learning in universities.

University Students according to Drew, (2020) are frequent targets of cybercrime. Studies have highlighted phishing as the dominant threat, exploiting students trust in institutional communications. Ali et al., (2024) identified other common issues as malware from peer-to-peer file sharing, weak password practices and a general lack of awareness about data privacy on social

media. In a nutshell, existing literature adequately covers threats to the general students' body and promotes general security awareness campaigns, there is a lack of focused research on how technically-skilled students specifically experience, perceive and resolve threats. Understanding their organic, self-directed mitigation strategies is crucial for designing educational interventions that build upon, rather than terminate their existing skill sets. The consequences of security incidents include theft of private information, data tampering and data deletion. Attacks can disrupt work processes, damage a company's reputation and have a tangible cost (Saffady, 2020).

In other to avert these consequences, many organisations allocate funds for security to ensure that they are ready to detect, respond to and proactively prevent attacks such as fake links like: phishing, malware, viruses, malicious insiders and ransomware. The three principles of cybersecurity are the basic tenets of Confidentiality, Integrity and Availability (CIA) (Perwej et al., 2021). Every element of cybersecurity programme must be designed to implement one or more of these principles. Confidentiality measures are designed to prevent unauthorised disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organisational functions (Nissenbaum, 2020). Integrity consistency protects against unauthorised changes (additions, deletions, alterations, etc.) to data (Kulkarni & Kothari, 2024). The principle of integrity ensures that data is accurate and reliable. It is not modified incorrectly, whether accidentally or maliciously. Availability on its part is the protection of a system's ability to make software systems and data fully available when a user needs it at a specified time. The purpose of availability is to make the technology infrastructure, the applications

and the data available when they are needed for an organisational process.

These three principles are very essential in assuring Cybersecurity as the practice of protecting computers, networks, systems, and data from digital attacks, damage, or unauthorized access. Cybersecurity professionals implement preventive, detective, and responsive measures against cyber threats such as malware, phishing, and ransomware to safeguard digital assets and maintain business continuity.

Evidence from available literature has only shown the types of threats that exist. Haridas et al., (2025) and Dauti (2025) share the same idea on the common types of Cybersecurity threats and their solutions. Malware is any software intentionally designed to harm, disrupt, or gain unauthorized access to computer systems, networks, or data (Alenezi et al., 2020). It is a broad term that includes various threats such as viruses, worms, ransomware, and spyware, which can be used to steal information, disrupt operations, or extort money from victims. Malware, according to Akinde, et al., (2021) can infect devices through malicious websites, deceptive emails, infected downloads, and system vulnerabilities. It infiltrates systems to steal data, encrypt files for ransom, or spy on user activity. Viruses attach to legitimate files and spread when executed (Choi, Lee, & Merizalde, 2023). They can corrupt data, slow performance, or destroy systems entirely. Trojans disguise themselves as harmless software, tricking users into installation (Mlelwa, 2023). Once active, they create backdoors for hackers to exploit. Spyware silently monitors a person's activity, collecting sensitive information like passwords or credit card details. It is often bundled with free software. Worms, unlike viruses, worms self-replicate and spread across networks without user interaction. A single infected device can compromise an entire organization. A phishing attack is a

type of cybersecurity fraud where criminals impersonate legitimate entities to trick people into revealing sensitive information like passwords, credit card numbers, or bank details (Ali, & Mohd, 2024). These deceptive communications, often sent via email, text messages, or fake websites, exploit human psychology by creating a sense of urgency or fear to prompt users into clicking malicious links, opening infected attachments, or sharing private data. Denial-of-Service (DoS) Attacks is a cyberattack where a single malicious actor floods a target system, network, or server with excessive traffic or requests, overwhelming its capacity and making it unavailable to legitimate users (Adedeji, Abu-Mahfouz & Kurien, 2023). This disruption prevents normal operation and access to services like websites, email, or online accounts. DoS attacks overwhelm servers with traffic, crashing websites or services. Structured Query Language (SQL) Injection is an attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code. Hackers use SQL injection to manipulate database queries, accessing or deleting sensitive data. SQL Injection is a common security vulnerability that arises from letting attacker-supplied data become SQL code (Abi, 2024). This happens when programmers assemble SQL queries either by string interpolation or by concatenating SQL commands with user supplied data. Man-in-the-Middle (MitM) Attacks are the cyberattack where a hacker secretly intercepts and potentially alters communication between two parties without their knowledge (Aliyeva, 2025; Mitră, 2020). The attacker positions themselves in the middle of the conversation, allowing them to eavesdrop on data, steal credentials like login details and credit card numbers, and even impersonate one of the parties. These attacks often occur on public Wi-Fi networks or via other insecure connections. Zero-Day Exploits. A zero-day

exploit is a cyberattack that takes advantage of previously unknown security vulnerability before the software vendor or developer has a chance to fix it (Bompos, 2020). The name "zero-day" comes from the fact that the developers have had "zero days" to address the flaw before it's actively being exploited. This makes such attacks particularly dangerous, as they can be used to steal data, install malware, or disrupt systems while the target is unaware of the vulnerability. Zero-day attacks target unpatched software vulnerabilities before developers can fix them. According to Shukla, et al., (2022), these Cybersecurity threats can disrupt the operations or render devices unusable, compromise sensitive data and steal sensitive data which lead to data and financial losses. By understanding Students experiences and innate problem-solving approaches, educators and institutions can develop more targeted and effective Cybersecurity modules that bridge the gap between theoretical knowledge and practical self-defense.

Purpose of the Study

The main purpose of this study was to investigate the Cybersecurity threats experienced by Computer and Business Education Students and their efforts to solve them. Specifically, this study:

1. Ascertained the most prevalent types of cybersecurity threats experienced by Computer and Business Education Students in their academic and personal contexts.
2. Determined the strategies that Students employ to solve the Cybersecurity threats encountered.

Research Questions

In line with the two specific purposes of this study, the following research questions were raised that guided this study:

1. What are the most prevalent types of Cybersecurity threats experienced by Computer and Business Education students in their academic and personal contexts?

2. What strategies do these students employ to solve the Cybersecurity incidents encountered?

Methods

This study adopted a descriptive survey research design. The study was conducted in southeast Nigeria. The population for the study was 250 (second year) undergraduate Students across Five Universities in South-East States, Nigeria. Comprising 169 Computer and Business Education students drawn from the University of Nigeria, Nsukka (UNN), Enugu State; Nnamdi Azikiwe University, Awka (UNIZIK), Anambra State (11 students); Alvan Ikoku Federal University of Education, Owerri (AIFUE), Imo State (22 students); Michael Okpara University of Agriculture, Umudike (MOUAU), Abia State (18 students); and the Federal University of Ndufu-Alike Ikwo (FUNAI), Ebonyi State (50 students). Computer and Business Education second students were selected because of their expertise and professional experience, which qualify them to provide reliable information on the competencies required for effective cybersecurity instruction. A structured online questionnaire was design using Google Form and was distributed to 250 Undergraduate Students across Five Universities majoring in Computer and Business Education. One hundred and eight-seven complete responses were received (74.8% response rate). The instrument was validated by three experts. Two from department and Computer Robotics Education and one from department of Business Education. All from Faculty of Vocational and Technical Education, University of Nigeria, Nsukka. To ensure the reliability of the instrument, it was trial-tested on 10 computer and business education students from the University of Port Harcourt (UNIPORT) in Rivers State, which is located outside the South-Eastern States of Nigeria. The reliability of the instrument was determined using Cronbach's Alpha reliability index. The

overall reliability index stood at 0.93. Data collected from the respondents were analysed using frequency counts and

percentage statistics for research question 1 while mean and standard deviation was used to analysed research question 2.

Results

Research Question 1: What are the most prevalent types of Cybersecurity threats experienced by Computer and Business Education Students in their academic and personal contexts?

Table 1: The most prevalent types of Cybersecurity threats experienced by Computer and Business Education Students in their academic and personal contexts

S/No.	Incident Type	(f)	(%)	Common Contexts
1	Phishing / Social Engineering	146	78	Fake software license emails, compromised peer accounts on Discord/Slack, fake internship offers.
2	Malware Infection	116	62	Often bundled with "cracked" software, game mods, or from downloading tools from unofficial sources.
3	Credential Theft	66	35	Reuse of university credentials on third-party developer sites (e.g., GitLab, Stack Overflow).
4	Privacy Breach (Doxing)	53	28	Personal information exposed on public code repositories (e.g., accidentally committing API keys).
5	Hacked Personal Project	42	22	Vulnerable web applications or servers set up for coursework being compromised.

Key: (f) = Frequency Count, (%) Percentages

As shown in Table 1, Phishing/social engineering was the most common threat experienced by Computer and Business Education undergraduates studied include: credential theft, privacy breach and hacked

personal project, followed by malware infection. Other threats frequency.

Research Question 2: What strategies and resources Computer and Business Students employ to solve the cybersecurity incidents they encounter?

Table 2. Mean ($\bar{x}$) and Standard Deviation (SD) on the Strategies and resources Computer and Business Students employ to solve the Cybersecurity incidents they encounter

S/N	Item Statement	N	$\bar{x}$	SD	Remark
1	I Googled the error message and found a removal guide on a tech forum.	250	4.42	1.04	Agree
2	Ran Malware bytes and it cleaned the infection.	250	3.83	1.33	Agree
3	Posted in our course Discord channel; a classmate helped me.	250	3.96	1.27	Agree
4	I manually checked my running processes and deleted suspicious files.	250	3.65	1.36	Agree
5	It was faster to just wipe the VM and start over.	250	3.79	1.29	Agree

6	I had to get my account unlocked after the breach.	250	3.72	1.35	Agree
7	I googled fake software license emails and found a removal guide on a tech forum.	250	3.54	1.41	Agree
Cluster Mean		250	3.85	.754	Agree

Key: Mean ratings between 1.00-2.33 = Disagreed; 2.34-3.66 = Somewhat Agreed; 3.67-5.00 = Agreed; and N = Number of Respondent)

Results in Table 2 showed that all the items in the cluster had their *mean* between 3.54-4.42, which means that the subjects used for this study agreed that these statements represent strategies and resources computer and business education students employ to solve the cybersecurity incidents they encounter.

Discussion of the Findings

The study revealed a strong culture of peer support, but a notable unwillingness to engage formal university IT services. Students perceived IT support as being for "general user problems, not for the complex material we confusion with". This indicates a potential disconnect between student needs and the perceived scope of institutional support. The study further showed that social engineering was the most common threat. Students could easily spot crude phishing attempts, they were often deceived by highly targeted "spear-phishing" related to their field, such as emails mimicking Adobe or JetBrains offering "student licenses. According to Van and Nguyen, (2023) who stated, it looked exactly like the real JetBrains email they got the year before. They only realized it was fake when the 'activation link' asked for their university password. Also, Malware was frequently an unintended consequence of seeking out expensive software for course projects. In addition, Students demonstrated high agency and technical competence in resolving incidents, primarily relying on independent methods (Table 2). Online forums (e.g., Stack Overflow, Reddit's r/techsupport) were the first line of defense. Students' knowledge of steps like password auditing across multiple sites, checking or reporting the incident was low. The "destroy and pave" approach for fully reinstalling an

operating system or development environment was a common solution adopted by students in overcoming threats, although it was considered a drastic, solution. It was praised for its effectiveness. The study revealed that Students are extremely targeted by and exposed to sophisticated threats like targeted phishing and malware from unofficial software sources and that their problem-solving is characterized by technical self-reliance but lacks formal structure and fails in the face of privacy and social engineering attacks. The findings of this study are in line with the findings of Alenezi al et. (2020) who, identified Malware as a broad term that includes various threats such as viruses, worms, ransomware, and spyware, which can be used to steal information, disrupt operations, or extort money from victims. In support of the findings, Van and Nguyen, (2023) stated that, it looked exactly like the real JetBrains email they got the year before, they only realized it was fake when the 'activation link' asked for their university password.

These findings confirm the "Computer and Business Education Student Paradox." Their technical proficiency is a double-edged sword, which enables them to independently solve complex technical problems like malware removal, but also leads to engagement in high-risk activities and a blind spot for sophisticated social threats. These findings are in line with the findings of Perweij et al (2021), who stated that many web applications are business-critical and contain sensitive customer data making them valuable targets for attackers and high priority for any cybersecurity programme. In a nutshell, AlDaajehet al., (2022), also mentioned three major cybersecurity

strategic goals: Development of secure digital and information technology infrastructure and services, defending from sophisticated cyber threats, and enrichment of individuals' cybersecurity maturity and awareness which are some of the strategies and resources that Students employ to solve the Cybersecurity incidents they encounter. Also, heavy reliance on informal, online resources suggests that Students are building practical knowledge outside the formal curriculum. While this demonstrates resourcefulness, it also means their security knowledge is fragmented and potentially based on inaccurate or incomplete information from unvetted sources. Also, Vasileiou (2020) discussed challenges such as misalignment between academia and Industry, Lack of standardisation, Limited Focus on Lifelong Learning, and Employer Engagement Barriers.

In addition, the low utilization of institutional IT support is a concern. It suggests that universities are missing a key opportunity to provide guided, expert-led security education in a "teachable moment" that is when a student is motivated to learn. These findings are in line with the findings of Haney and Lutters (2021), suggesting improvements for professional development that encourage greater security workforce diversity.

Recommendations

It was, therefore, recommended that Universities offering course in Computer and Business Education should:

1. Core computing courses should include modules with real-world scenarios, such as identifying spear-phishing emails related to software tools, securing API keys in code, and practicing incident response for a compromised server.
2. Universities should ensure that Students have affordable or free access to necessary commercial software through campus-wide licenses or

academic partnerships, reducing the incentive for piracy.

3. IT Departments should actively market themselves as partners for advanced security issues, by offering "security clinic" hours where students can bring compromised personal projects for analysis and guided recovery.

REFERENCES

- Abi, B. A. (2024). *Web sql injection attack detection algorithm using deep learning* (Doctoral dissertation, Marymount University).
- Adedeji, K. B., Abu-Mahfouz, A. M., & Kurien, A. M. (2023). DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. *Journal of Sensor and Actuator Networks*, 12(4), 51-60
- Akinde, O. K., Ilori, A. O., Afolayan, A. O., & Adewuyi, O. B. (2021). Review of computer malware: detection and preventive strategies. *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)*, 19, 49. 143-156.
- Alenezi, M. N., Alabdulrazzaq, H., Alshafer, A. A., & Alkharang, M. M. (2020). Evolution of malware threats and techniques: A review. *International journal of communication networks and information security*, 12(3), 326-337.
- AlDaajeh, S., Saleous, H., Alrabae, S., Barka, E., Breiting, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119, 1027-1054. <https://doi.org/10.1016/j.comnet.2024.110446>.
- Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform*, 33(1), 101-121.
- Ali, M., Chauhan, R., Kalyan, A., Devliyal, S., & Chanti, Y. (2024). Peer To Peer Confidentiality in Social Applications. In *2024 3rd International Conference for Innovation in Technology (INOCON)* (pp. 1-11). IEEE.
- Aliyeva, T. (2025). Investigation of Cyberattack and Intrusion: Methods and Tool.
- Bompos, K. (2020). *Development time of Zero-Day cyber exploits in support of offensive cyber operations* (Unpublished Doctoral dissertation, Monterey, CA; Naval Postgraduate School).
- Choi, K. S., Lee, C. S., & Merizalde, J. (2023). Spreading viruses and malicious codes. In *Handbook on Crime and Technology* (pp. 232-250). Edward Elgar Publishing.
- Dauti, B. (2025). *Windows Server 2025 Administration Fundamentals: A beginner's guide to managing and administering Windows Server environments*. Packt Publishing Ltd.
- Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17-33.
- Haney, J. M., & Lutters, W. G. (2021). Cybersecurity advocates: discovering the characteristics and skills of an emergent role. *Information & Computer Security*, 29(3), 485-499. <https://doi.org/10.1108/ICS-08-2020-0131>.
- Haridas, R., Sharma, S., Bhakar, R., & Gu, C. (2025). Cybersecurity Threats to Critical Energy Infrastructure in India: Challenges, Opportunities and Insights for Developing Nations. *The Commonwealth Cyber Journal (CCJ)*, 3, 53-78.
- Kulkarni, P., & Kothari, C. (2024). Documentation and Data Integrity in

- Pharmaceutical Industry. In *Modern Aspects of Pharmaceutical Quality Assurance: Developing & Proposing Application models, SOPs, practical audit systems for Pharma Industry* (pp. 381-403). Singapore: Springer Nature Singapore.
- Matczak, A., Akdogan, H., & Ashmore, D. (2023). The paradox of technology in online education during the COVID-19 pandemic: the experiences of safety and security students in a Dutch university. *Higher Education*, 86(6), 1269-1292.
- Mitră, S. E. (2020). The Structure of Cyber Attacks. *International Journal of Information Security and Cybercrime (IJISC)*, 9(1), 43-52.
- Mlelwa, K. (2023). Investigate trojans, wireless concepts and their attacks.
- Nissenbaum, H. (2020). *Protecting privacy in an information age: The problem of privacy in public*. In *The ethics of information technologies* (pp. 141-178). Routledge. <https://www.taylorfrancis.com/chapters/edit/10.4324/9781003075011-12/protecting-privacy-information-age-problem-privacy-public-helen-nissenbaum>.
- Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, 9(12), 669-710. DOI: 10.18535/ijssrm/v9i12.ec04.
- Pinjarkar, L., Hete, P. R., Mattada, M., Nejekar, S., Agrawal, P., & Kaur, G. (2024). An Examination of Prevalent Online Scams: Phishing Attacks, Banking Frauds, and E-Commerce Deceptions. In *2024 Second International Conference on Advances in Information Technology (ICAIT)* 1(1), 1-6). IEEE.
- Saffady, W. (2020). *Managing information risks: threats, vulnerabilities, and responses*. New York: Bloomsbury Publishing PLC.
- Shukla, S., George, J. P., Tiwari, K., & Kureethara, J. V. (2022). Data security. *Data ethics and challenges* (41-59). Singapore: Springer Singapore.
- Unigwe, M. (2022). *The views of information security professionals toward information security objectives: Confidentiality, integrity, and availability triad*. Trident University International Journal. 46(5), 351-361.
- Van Horn II, B. M., & Nguyen, Q. (2023). *Hands-on application development with PyCharm: Build applications like a Pro with the ultimate Python development tool*. Singapore: Packt Publishing Ltd.
- Vasileiou, I. (2020). Cyber security education and training delivering industry relevant education and skills via degree apprenticeships: In *human aspects of information security and assurance. International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020, Proceedings 14* (175-185). Springer International Publishing.