CYBER-SECURITY AWARENESS AND PRACTICES AMONG UNDERGRADUATE STUDENTS: A STUDY ON ARTIFICIAL INTELLIGENCE, PRIVACY CONCERN, AND DATA PROTECTION

SULYMAN Bola Mariam & MAKINDE Semiu Olawale
Department of Science Education**,** Al-Hikmah University, Ilorin, Nigeria
bolasulyman01@gmail.com

Abstract

Education has been completely transformed by the swift assimilation of Artificial Intelligence (AI) across multiple domains. With an emphasis on data protection, fraud prevention, and education privacy, this study investigates the impact of AI on undergraduates' understanding of cyber-security. The study looks at how AI-powered resources and methods improve students' comprehension and application of cyber-security protocols. This paper investigates the relationship between undergraduate students at Al-Hikmah University in Ilorin, Nigeria, and their understanding of cyber-security. Using a descriptive survey approach, the results show that students have a moderate to good grasp of cyber-security procedures, with privacy concerns and proactive adoption of protective measures standing out. The study underscores the importance of integrating robust cyber-security education to mitigate risks and enhance preparedness in the digital age.

Keywords: Artificial Intelligence; Cyber-security Awareness; Education; Fraud Prevention; Data Protection.

Introduction

One important breakthrough that has significantly improved educational systems worldwide is artificial intelligence. The creation of computer systems that are capable of tasks that normally require human intelligence is known as artificial intelligence (AI) (Collins et al., 2021). Using algorithms, data, and computing power, they are made to mimic human cognitive functions including reasoning, problem-solving, perception, and language understanding. As a result, they can carry out tasks including decision-making, pattern recognition, experience-based learning, and natural language comprehension. The integration of AI technologies and methodologies to improve teaching, learning, administration, and student support services in educational institutions is known as artificial intelligence (AI) in the educational system (Olatunde-Aiyedun, 2024). Therefore, Artificial Intelligence (AI) in education basically refers to the application of technologies like machine learning and natural language processing to enhance learning processes, teaching methodologies, and administrative tasks (Chen et al., 2020). Using AI in education may personalize educational content for the learners, can also automate repetitive tasks, as well as provide insights into student performance (Harry, 2023). The integration of AI in education is changing traditional teaching paradigms and learning experiences, by creating adaptive and responsive educational environments (Young, 2024).

Personalized learning experiences, administrative work automation, data analytics insights, and adaptive assessment facilitation are just a few of the ways artificial intelligence (AI) has the potential to completely transform the education industry (Igbokwe, 2023). Personalization of learning, which analyzes each student's learning style, interests, and performance to deliver them a tailored learning experience, is one of the other crucial uses of AI in the educational system (Seo et al., 2021). To ensure its responsible and equitable use, however, the ethical ramifications, privacy issues, and difficulties associated with the adoption and implementation of AI in education must be thoroughly evaluated and addressed. AI brings up moral concerns about algorithmic unfairness, data privacy, and the appropriate application of technology in the classroom (Huang, 2023; Akgun & Greenhow, 2022).

To ensure equity, fairness, and transparency in AI-powered systems, educators need to address these concerns. Additionally, a "one-size-fits-all" approach to learning and teaching may result from an overreliance on AI technologies, which may also reduce human interaction, critical thinking abilities, and creativity (Chen & Lin, 2024). Finally, cost and accessibility to AI technologies need to be considered. Cyber security is the practice of safeguarding computer systems, networks, programs, and data from digital attacks, unauthorized access, damage, or theft (Li & Liu, 2021). It encompasses various technologies, processes, and practices designed to safeguard information and systems from cyber threats (Jimmy, 2024). Adequate implementation of cyber security is necessary to protect AI against the detrimental effects of data breaches, theft, privacy, and other concerns. Protecting networks, devices, apps, and sensitive data from cyber threats and unauthorized access is what is meant by cyber security in the educational system, which is the application of policies and procedures to secure digital assets, information systems, and data within educational institutions (Jimmy, 2024). The protection of student data is one aspect of cyber security in educational systems. Large volumes of sensitive student data, such as financial, academic, and personal information, are stored by educational institutions; cyber security measures are crucial to keep this data safe from theft, breaches, and unauthorized access (Djeki, et al., 2024).

The vast and intricate network infrastructures that link different devices and systems are characteristic of educational institutions. Protecting these networks from cyber-attacks is facilitated by the implementation of firewalls, intrusion detection/prevention systems, and network seg mentation. They also need to protect various laptops, tablets, and smartphones in educational settings which is considered an endpoint. Installation of antivirus software, enforcing device encryption, and implementing remote device management solutions to help protect endpoints from malware and other cyber threats are essential (Chin et al., 2020). Students and Staff need to be trained on cyber security awareness. To avoid cyber incidents, they must be instructed in safe online conduct, how to spot phishing attempts, and the value of strong passwords. As more educational institutions begin to use digital tools and online learning platforms, it is imperative that these platforms be secure. This can be done by implementing secure authentication mechanisms, encrypting communication channels, and regularly updating their software to reduce the risk (Li & Liu, 2021).

Educational institutions are subject to data protection regulations such as the Family Educational Rights and Privacy Act (FERPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union (Frank & Wagner, 2018; Hoofnagle et al., 2019). Compliance with these regulations requires the implementation of appropriate cybersecurity measures to protect student and staff data. It is important to emphasize that cyber incidents may still occur notwithstanding precautionary measures. However, establishing incident response plans and procedures enables educational institutions to detect, contain, and mitigate the impact of cyber incidents swiftly. Regular data backups and disaster recovery plans help to minimize downtime and data loss (Kesa, 2023). Overall, cyber security in the educational system is essential for protecting sensitive data, maintaining the integrity of educational processes, and ensuring a safe and secure learning environment for students and staff. Paying adequate attention to cyber security will ensure the protection of data, information (PII), while prevention of cyber-attacks, and maintenance of continuity of educational activity by minimizing the impact of cyber incidents, reducing downtime, and ensuring that critical systems and services remain operational. Some shortcomings may arise by utilizing cyber security which have been discussed by scholars. One of these is cost because having robust cyber security can be expensive because it involves investment in technology, personnel, training, and ongoing maintenance.

Advancement in the field of AI and cybersecurity in recent years is phenomenal; hence, it is now easy for AI to detect threats and preemptively treat them before serious harm is done. In other words, AI-powered systems have abilities to analyze vast amounts of data to identify patterns and anomalies that may indicate potential cyberattacks, enabling real-time threat detection and automated incident response (Shanthi et al., 2023; Rizvi, 2023). Machine learning algorithms and natural language processing techniques have been shown to be effective in detecting malicious intent in textual data and improving threat intelligence (Ismail, 2024). Rizvi (2023) also reported that AI's predictive modeling has the capability to prevent attacks by recognizing potential threats before they occur (Rizvi, 2023). With all these advantages, advances in AI technology as regards cybersecurity have their own shortcomings. It is a known fact that AI can be used to enable more sophisticated forms of cyber-attacks, such as AI-powered malware and phishing attempts (Shanthi et al., 2023). Attackers can manipulate AI models with adversarial inputs that cause misclassification so that the threats will be identified as normal data. These adversarial malwares may also bypass AI-based detection by altering benign features. It is, therefore, essential to carefully consider ethical implications whenever there is for the integration of AI in cybersecurity frameworks (Mamadaliev, 2023).

Awareness of social engineering techniques such as phishing emails, fake websites, and social media scams varies among undergraduate students. While some may recognize and avoid these threats, others may fall victim to social engineering attacks due to lack of awareness (Abdulla et al., 2023). Some undergraduate students may not always prioritize the protection of their personal data, such as sensitive documents, financial information, and personal identifiable some may share sensitive information online or store it insecurely, thereby increasing the risk of data exposure. Some students are also not conversant with some basic safe internet practices such as avoiding unsecured Wi-Fi networks, using virtual private networks (VPNs) for added security, and being cautious when downloading or sharing files online (Alkhalil et al., 2021).

It is, therefore, not an overstatement to emphasize that cybersecurity awareness and knowledge among undergraduate students are paramount in this digital age due to the exponential increase in cyber threats and cybercrimes brought about by technological advancements (Mohammed & Bamasoud, 2022). Peker et al. (2016) noted that effective cybersecurity awareness programs are crucial for improving cybersecurity not only for computer science majors but for all students. This is because studies have shown a significant difference in cybersecurity awareness between students of computer science and those from other fields of study, highlighting the need for targeted education (Subhani et al., 2023). Furthermore, it is necessary to note that students are particularly vulnerable to cyber-attacks due to their active internet usage in educational activities, underscoring the importance of assessing their awareness of threats such as phishing, malware, and ransomware (Verma & Pawar, 2024).

Statement of the Problem

The rapid advancement of Artificial Intelligence (AI) presents both opportunities and challenges for cyber security, especially in the educational sector. While AI has the potential to revolutionize cyber defense by automating threat detection and deactivation of same, at the same time, it can be exploited by cyber criminals to launch more specific and targeted cyber-attacks. There appears to be a knowledge gap, particularly among undergraduate students who make use of artificial intelligence for their study and need robust cyber security practices to avoid or prevent cyber-attacks. However, there is dearth of studies on cyber security concerns on the use of Artificial Intelligence in education among undergraduate students in this part of the world. This study will, therefore, attempt to find out how undergraduate students of Al-Hikma University, Ilorin, Nigeria, perceive the relationship among the use of AI in education, cyber security, cyber threats and measure to curb these threats. By addressing these concerns, this research work seeks to bridge the knowledge gap and provide baseline information for future researchers on how to navigate the complexities of AI and cyber security effectively.

Purpose of the study

The purpose of this study is to provide insights into the intersection of cyber security awareness, AI education, and key concerns such as privacy, internet fraud, and data protection among undergraduate students. Specifically to find out;

1. The level of knowledge and consciousness about cyber security threats from the use of Artificial intelligence among undergraduate students of Kwara State.
2. Determine the influence of knowledge about Artificial Intelligence on cyber security awareness and practices of undergraduate students of Kwara State.
3. Explore the extent of understanding of undergraduate students of Kwara State on cyber security practices.

Research Questions

The following Research Questions will be answered:

1. To what extent do undergraduate students possess knowledge about cyber security threats and best practices?
2. What are the privacy concerns among undergraduate students in the context of AI technologies, and how do these concerns influence their online behaviours and practices?
3. How aware are undergraduate students of the various forms of cybersecurity practices

Methodology

The researcher employed a descriptive survey research design to examine the level of cybersecurity awareness and practices among undergraduate students. The study's population included all undergraduate students at Al-Hikmah University, located in Ilorin, Kwara State, Nigeria. A structured questionnaire was designed by the researchers to assess participants' awareness and knowledge of cybersecurity concepts, threats, and practices. The instrument was validated by the experts in Educational Technology for content and reliability validity prior to been used. Two hundred students were randomly selected from the seven faculties in the school to ensure equal representation across all levels and among genders. The interview was conducted in-person to ensure high response rates and to allow for clarification of questions when necessary.

Results

Research question 1: To what extent do undergraduate students possess knowledge about cyber security threats and best practices?

TABLE 1: DO UNDERGRADUATE STUDENTS POSSESS KNOWLEDGE ABOUT CYBER SECURITY THREATS AND BEST PRACTICES?

Item	**EX** Frequency %	**G** Frequency %	**M** Frequency %	**P** Frequency %	**VP** Frequency %	**Mean**
1. I understand Artificial Intelligence (AI) and its applications in cybersecurity	48.3	33.9	17.8	0.0	0.0	3.31
2. I have basic knowledge of privacy concerns in the context of AI technologies	22.2	70.0	3.9	3.9	0.0	3.11
3. I understand internet fraud and common cyber threats	40.6	38.9	16.7	3.9	0.0	3.16
4. I have Familiarity with data protection practices and regulations	21.1	53.3	25.6	0.0	0.0	2.96
Average mean						**3.14**

The table provides insights into the knowledge levels of undergraduate students regarding various aspects of cybersecurity. Excellent (EX), Good (G), Moderate (M), Poor (P), and Very Poor (VP), along with their respective frequencies and percentages. Students have a relatively high understanding of Artificial Intelligence (AI) and its applications in cybersecurity, with 87 respondents (48.3%) indicating strong knowledge in this area and a mean score of 3.31. Basic knowledge of privacy concerns in AI technologies is also prevalent, with 70% of respondents rating their understanding as average and a mean score of 3.11. Understanding of internet fraud and common cyber threats is similarly strong, with 40.6% reporting a high level of knowledge and a mean score of 3.16. However, familiarity with data protection practices and regulations is less common, with a mean score of 2.96. Overall, the average mean score across all areas is 3.14, indicating a moderate to strong level of cybersecurity awareness among the students surveyed.

Research question 2: What are the privacy concerns among undergraduate students in the context of AI technologies, and how do these concerns influence their online behaviours and practices?

TABLE 2: PRIVACY CONCERNS AMONG UNDERGRADUATE

Item	**SA** Frequency %	**A** Frequency %	**N** Frequency %	**D** Frequency %	**SD** Frequency %	**Mean**
1. I am concerned about my privacy when using AI-powered services or devices	103 57.2%	63 35.0%	14 7.8%	0 0.0%	0 0.0%	3.49
2. I believe that internet fraud is a significant threat in today's digital age	100 55.6%	61 33.9%	19 10.6%	0 0.0%	0 0.0%	3.45
3. I take proactive measures to protect my personal information online	82 45.6%	79 43.9%	19 10.6%	0 0.0%	0 0.0%	3.35
Average mean						**3.43**

The table highlights an overview of responses to the items across five rating categories: Strongly Agree (SA), Agree (A), Neutral (N), Disagree (D), and Strongly Disagree (SD), with the mean scores reflecting the overall sentiment. A significant majority of students, 57.2%, express strong concern about their privacy when using AI-powered services or devices, resulting in a mean score of 3.49. Additionally, 55.6% of students believe that internet fraud is a significant threat in today's digital age, with a mean score of 3.45. Furthermore, 45.6% of students take proactive measures to protect their personal information online, contributing to a mean score of 3.35. The overall average mean score of 3.43 indicates that privacy concerns and proactive behaviours are notably high among the surveyed students.

Research question 3: How aware are undergraduate students of the various forms of cybersecurity practices

TABLE 3: UNDERGRADUATE STUDENTS ON THE VARIOUS FORMS OF CYBERSECURITY PRACTICES

Item	**A** Frequency %	**OFT** Frequency %	**O** Frequency %	**R** Frequency %	**N** Frequency %	**Mean**
1. I can Update software and security patches on my devices	80 44.4%	72 40.0%	28 15.6%	0 0.0%	0 0.0%	3.47
2. I am using strong, unique passwords for online accounts	105 58.3%	54 30.0%	21 11.7%	0 0.0%	0 0.0%	3.51
3. I can Avoid sharing sensitive information online	105 58.3%	68 37.8%	0 0.0%	7 3.9%	0 0.0%	3.41
4. I am Regular in backing up important data	101 56.1%	58 32.2%	14 7.8%	7 3.9%	0 0.0%	3.29
Average mean						**3.42**

The table assesses undergraduate students' engagement in various cybersecurity practices across five categories: Agree (A), Often (OFT), Occasionally (O), Rarely (R), and Never (N), with the mean scores reflecting the overall engagement with these practices. A significant portion of students, 44.4%, frequently update software and security patches on their devices, resulting in a mean score of 3.47. Using strong, unique passwords for online accounts is practised by 58.3% of students, yielding the highest mean score of 3.51. Avoiding the sharing of sensitive information online is also common, with 58.3% of students adhering to this practice and a mean score of 3.41. Additionally, 56.1% of students regularly back up important data, with a mean score of 3.29. The overall average mean score is 3.42, indicating a good level of adherence to essential cybersecurity practices among the surveyed students.

Discussion of Findings

The survey reveals a moderate to strong level of cyber-security knowledge among undergraduate students. Notably, students demonstrate a robust understanding of artificial intelligence (AI) applications in cybersecurity. However, familiarity with data protection practices and regulations scores lower, indicating an area that requires improvement. Overall, the average mean score across all areas is 3.14, suggesting a solid foundation in cyber-security awareness among the surveyed students. Recent studies emphasize the importance of integrating practical cyber-security education into academic curricula to enhance students' preparedness for cyber threats (Smith, 2023).

The study also reveals that privacy concerns among students regarding AI technologies is considered to be important. The majority express strong concerns about their privacy when using AI-powered services or devices and perceive internet fraud as a substantial threat in the digital age. A significant proportion of undergraduate students take proactive measures to protect personal information online, such as regularly updating their software, using strong and unique passwords, and avoiding sharing sensitive information online. This is consistent with research by Lee and Ahmed (2021), which found that heightened privacy concerns often lead to more cautious online behaviors. When issues of privacy in technology are raised, it is often seen from security interests rather than privacy itself, though privacy remains crucial for autonomy and identity development (Elliott & Soifer, 2022). These privacy concerns include unauthorized access to sensitive personal data and a lack of transparency on how they are stored, as well as sharing this sensitive information with unauthorized third parties. Overzealousness in surveillance and inadvertently targeting certain individuals and groups as threats based on some common data with dangerous groups are another important area of concern when discussing privacy issues.

Conclusion

In conclusion, the findings underscore a promising level of cyber-security knowledge, awareness of privacy concerns, and engagement in best practices among undergraduate students. However, gaps in understanding data protection regulations highlight areas for targeted educational interventions. Moving forward, integrating practical learning and real-world case studies into cyber-security education can further enhance students' readiness to navigate cyber threats effectively.

Recommendations

1. Universities should incorporate cybersecurity education into their undergraduate curricula.
2. Practical sections in form of workshops focusing on AI privacy risks, such as unauthorized data access and surveillance should be organized regularly.
3. Students should be educated on ethical use of AI with emphasis on its potential vulnerabilities.
4. Schools should enforce online safety practices such as regular software updates, strong passwords, and cautious online interactions among students.
5. University can collaborate with AI developers to mitigate over-surveillance and biases that might target individuals unfairly.
6. Regulators should ensure that AI applications comply with privacy and ethical standards to protect against data from misuse.
7. There should be regular surveys and researches to assess students’ evolving knowledge, behaviours, and concerns related to cybersecurity and privacy.

References

Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., & Rashid, T. A. (2023). Analysis of Social Engineering Awareness among Students and Lecturers. *IEEE Access*. *doi:* 10.1109/*ACCESS*.2023.3311708

Akgun, S., & Greenhow, C. (2022). Artificial intelligence in education: *Addressing ethical challenges in K-12 settings*. *AI and Ethics*, *2*(3), 431-440. https://doi.org/10.1007/s43681-021-00096

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 563060.*doi*:10.3389/fcomp.2021.563060

Chen, J. J., & Lin, J. C. (2024). Artificial intelligence as a double-edged sword: Wielding the POWER principles to maximize its positive effects and minimize its negative effects. *Contemporary Issues in Early Childhood*, *25*(1), 146-153. https://doi.org/10.1177/14639491231169813

Chin, A. G., Little, P., & Jones, B. H. (2020). An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University. *International Journal of Education and Development Using Information and Communication Technology*, *16*(1), 44-61.

Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management*, *60*, 102383. https://*doi*.org/10.1038/s41746-020-0288-5

Djeki, E., Dégila, J., Bondiombouy, C., & Alhassan, M. H. (2024, April). Data protection in digital learning space: An overview. In *AIP Conference Proceedings* (Vol. 3109, No. 1). AIP Publishing. https://*doi*.org/10.1063/5.0204895

Elliott, D., & Soifer, E. (2022). AI technologies, privacy, and security. *Frontiers in Artificial Intelligence*, *5*, 826737.

Frank, R., & Wagner, L. (2018). Understanding the Importance of FERPA & Data Protection in Higher Education. An Application: Website at La Salle University.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means*. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. *Science Insights Education Frontiers*, *16*(2), 2577-2587.doi: 10.15354/sief.23.re202

Igbokwe, I. C. (2023). Application of artificial intelligence (AI) in educational management. *International Journal of Scientific and Research Publications*, *13*(3), 300-307. https://*doi*.org/10.18034/ajtp

Ismail, W. S. Threat Detection and Response Using AI and NLP in Cybersecurity.

Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation through Cloud Security Tools. *Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023*, *3*(1), 196-233. http://dx.doi.org/10.60087/jaigs.vol03.issue01.p233.

Kesa, D. M. (2023). Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. *World Journal of Advanced Research and Reviews*, *18*(3), 970-992. https://doi.org/10.30574/wjarr.2023.18.3.1166

Lee, C., & Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1), 18-33. *doi*: 10.54489/*ijtim*.v1i1.12.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mamadaliev, R. (2023). Artificial intelligence in cybersecurity: enhancing threat detection and mitigation. *Scientific Collection «InterConf»*, (157), 360-366.

Mohammed, M. A. R. A. M., & Bamasoud, D. M. (2022). The impact of enhancing awareness of cybersecurity on universities students: a survey paper. *Journal of Theoretical and Applied Information Technology*, *100*(15), 4756-4766.

Olatunde-Aiyedun, T. G. (2024). Artificial Intelligence (AI) in Education: Integration of AI In to Science Education Curriculum in Nigerian Universities. *International Journal of Artificial Intelligence for Digital*, *1*(1). https://*doi*.org/10.61796/ijaifd.v1i1.13

Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., & Lamberson, C. (2016, October). Raising cybersecurity awareness among college students. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 4, No. 1, pp. 17-17).

Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, *10*(05).

Seo, K., Tang, J., Roll, I., Fels, S., & Yoon, D. (2021). The impact of artificial intelligence on learner–instructor interaction in online learning. *International journal of educational technology in higher education*, *18*, 1-23. *doi*:10.1186/S41239-021-00292-9

Shanthi, R. R., Sasi, N. K., & Gouthaman, P. (2023, April). A New Era of Cybersecurity: The Influence of Artificial Intelligence. In *2023 International Conference on Networking and Communications (ICNWC)* (pp. 1-4). IEEE.

Smith, S. (2023). Investigating Factors that Increase Vulnerability to Cyber-Attacks during the First Year College Transition (Doctoral dissertation, Purdue University).

Subhani, A., Khan, I. A., & Ahmad, U. (2023). Importance of Conducting Cyber Security Awareness Sessions among Undergraduate Students. *Journal of Advanced Research in Social Sciences and Humanities*, *8*(2), 59-68.

Verma, V., & Pawar, J. (2024). Assessment Of Students Cybersecurity Awareness And Strategies To Safeguard Against Cyber Threats. *Journal of Advanced Zoology*, *45*.