GJR Publication
OPEN ACCESS

Global Journal of Research in Engineering & Computer Sciences
ISSN: 2583-2727 (Online)
Volume 04| Issue 06 | Nov.-Dec. | 2024
Journal homepage: https://gjrpublication.com/gjrecs/

Review Article

Educational Cybersecurity Awareness in the Digital Era: A Comprehensive Review

[1]Abubakar Surajo Imam, [2]Nurudeen Danladi Garba, [3]Muhammad Muneer Haruna, [4]Muhammad Ahmad Baballe*

[1, 2 ,3, 4]Department of Mechatronics Engineering, Nigerian Defence Academy (NDA), Kaduna, Nigeria.

DOI: 10.5281/zenodo.14488381 **Submission Date: 10 Nov. 2024 | Published Date: 15 Dec. 2024**

***Corresponding author: Muhammad Ahmad Baballe**
Department of Mechatronics Engineering, Nigerian Defence Academy (NDA), Kaduna, Nigeria.
ORCID: 0000-0001-9441-7023

Abstract

The escalating reliance on computer systems and interconnected digital landscape underscores the critical need for robust cybersecurity measures. Human error, stemming from careless or uninformed behaviour, poses a significant threat to information system security. This comprehensive literature review and expert analysis aims to investigate the impact of educational cybersecurity awareness on mitigating user-related vulnerabilities. The research objectives are to examine the relationship between cybersecurity awareness and user behaviour, evaluate the efficacy of educational interventions in reducing security breaches, and identify key factors influencing cybersecurity awareness among internet users. This study synthesises existing research, industry reports, and expert experiences to inform evidence-based cybersecurity awareness programs, enhancing information system security, protecting sensitive data, reducing cyber-attack risks, improving compliance with security protocols, and enhancing digital literacy. Cybersecurity measures in this digital era of the Fourth Industrial Revolution (4IR). In this digital world, there are about 5.45 billion people connected to the Internet. Which represents approximately 67.1% of the world population uses the Internet.

Keywords: *Cybersecurity, Education, Internet of Things (IoT), Security Awareness, Phishing, Cyber Attacks.*

I. INTRODUCTION

The internet has developed into a worldwide computer network that makes it simple and quick for people to connect and exchange information. There is a plethora of knowledge available online in almost every profession. Additionally, social media platforms make it simpler for non-experts to reach a wide audience with a variety of media. Not every user benefits equally from new media, even if technology has made it easier for everyone to interact, communicate, and trade information quickly. Cybercrime, including cyberbullying, is committed by some persons who abuse the internet. Communication methods like email, cell phones, instant messaging, online chat rooms, social networking websites, and webcams can all be used for cyberbullying. While cybersecurity focuses on protecting internet-connected devices and networks from online threats, information security generally deals with safeguarding all kinds of data [17–18].

Stopping cyberattacks, which are frequently conducted by outside threats like malware and hackers, is the primary objective of cybersecurity solutions. Information security measures, on the other hand, focus on preventing threats from both the inside and the outside and take into account different types of data storage, including physical storage like paper documents.

II. LITERATURE REVIEW

Cybersecurity has risen to the top of the priority list for organizations and governments worldwide. Unfortunately, many companies still do not have the tools and processes in place to protect themselves from cyberattacks. This article will cover the current challenges and issues confronting cybersecurity experts, as well as potential solutions to these issues. [8]. Overall, this survey gives a thorough review of computer cyber security, emphasizing the significance of proactive measures and ongoing adaptation to a shifting threat scenario [9].

Individuals and businesses may better defend themselves from cyberattacks and contribute to a safer digital world by knowing the current status of computers. Cybersecurity is the process of securing internet-connected systems, as well as the hardware, software, and data contained inside, against unwanted access, use, disclosure, modification, and destruction. Along with the restricted network infrastructure, sensitive data like financial and personal information, intellectual property, and trade secrets must be protected. Cybersecurity includes a variety of security measures that are aimed at defending the availability, confidentiality, and integrity of information from cyberattacks [3]. On the other hand, regardless of the medium used, information security includes measures to protect data from unauthorized access, unauthorized use, disclosure, alteration, and destruction. Information security versus computer security includes both computerized systems, such as file cabinets, and non-computerized systems, such as physical papers. In addition, information security is concerned with safeguarding all kinds of data, including financial and personal information, trade secrets, and intellectual property. It entails a variety of safeguards, including encryption, access control, firewalls, and security rules designed to protect data during its entire existence [10].

This paper examines the question of whether serious games and online quizzes can heighten cyber security awareness and motivate individual students to change their cybersecurity behavior. The paper reports on the findings based on written reflection notes from students belonging to both courses. The technique of examination and interpretation applied to the data was qualitative thematic content analysis supported by computer-assisted qualitative data analysis software NVivo. Theoretical analysis was guided by a social constructionist perspective on knowledge creation. While many advantages of the use of online quizzes and computer games were specified by students, challenges were identified as well. However, the findings show that the use of serious games and online quizzes can be an efficient approach to raising security awareness among participating students [1]. In this digital era, a person’s day begins with digital devices such as digital watches or smartphones. Cybersecurity is one of the major concerns in this era. Every device is connected, and hence, it is one of the reasons for most of the data security issues. The aim of this paper is to find out if it is necessary to conduct cybersecurity awareness sessions among students of different fields of study [2].

The poster will present the three-year project that aims to develop and assess three educational games with in-game assessments to effectively teach cyber security concepts (access control, LAN vulnerabilities, and buffer overflow). These games will be designed with different levels of difficulty to target students from freshmen to seniors and integrated into the existing computer science curriculum at Winston-Salem State University and North Carolina A&T State University to benefit a wide range of students. In addition, all these games will be portable, self-contained, and available for download from the project website [3].

This research paper aims to analyse the strengths and weaknesses associated with the utilisation of ChatGPT as an educational tool in the context of undergraduate computer science education. ChatGPT's usage in tasks such as solving assignments and exams has the potential to undermine students' learning outcomes and compromise academic integrity. This study adopts a quantitative approach to demonstrate the notable unreliability of ChatGPT in providing accurate answers to a wide range of questions within the field of undergraduate computer science. While the majority of existing research has concentrated on assessing the performance of large language models in handling programming assignments, our study adopts a more comprehensive approach. Specifically, we evaluate various types of questions, such as true/false, multi-choice, multi-select, short answer, long answer, design-based, and coding-related questions.

Our evaluation highlights the potential consequences of students excessively relying on ChatGPT for the completion of assignments and exams, including self-sabotage. We conclude with a discussion on how students and instructors can constructively use ChatGPT and related tools to enhance the quality of instruction and the overall student experience [4]. The purpose of this paper is to describe the role of cybermedia in educating the public about science. This is very elementary because practical science knowledge will provide construction of knowledge and experience to students and society in general. This research method is descriptive-qualitative with a literature study approach. The data sources in this study are journal articles that are compatible with the research theme; other sources are manuscripts, thoughts, videos, and others that can be substantially elaborated so as to produce a complete picture of the theme of the study being discussed. The results of the study found how cybermedia made a significant contribution to the science education of the community and students. The role can be detailed, namely it plays a role in cognitive effects, so that practical science can be absorbed by the wider community. In affective effects, cybermedia is able to influence mental attitudes when people meet with various empirical realities day by day.

Cybermedia provides a wealth of information about science and technology to the general public. It is a form of technological devotion to humans to create convenience in celebrating life, which is increasingly complicated in an overflow of unexplainable needs. In the end, this technological dedication provides a real mirror of how the civilisation built by humans with the permission of the almighty is the glory of humans equipped with qualified reason. In the context of this study, the content of cybermedia provides three strata of effects, namely cognitive, affective, and psychomotor, whose final result is an increasingly complex change in civilisation [5].

The current study's objective is to ascertain students' awareness of cybercrime in the Chhattisgarh region. In the world we live in, technology is now required in every aspect of life, from housekeeping work to running a multinational company and national security. Although technology makes life easier, there are risks associated with it, such as cybercrime (fraud, assault, bullying, sexual harassment, phishing). Students must understand that cybersecurity awareness is necessary to prevent any kind of cybercrime. For understanding the cyber-awareness among students of Chhattisgarh, we collected data from Pt. Ravishankar Shukla University in Raipur. The cybercrime awareness scale created by Dr. S. Rajasekar (2011) was used to test students' awareness of cybercrime using a questionnaire-based survey method. In this study, student demographic information (gender, location) is taken into account when measuring understanding of cyberthreats. The hypothesis is tested using the t-test. The results show that although male and female students' knowledge of cybercrime is not statistically different, there is a significant difference between students in rural and urban locations [6].

This survey aims to provide an overview of the current state of computer cybersecurity by examining key areas of concern, emerging threats, and the measures taken to mitigate risks. This survey begins by exploring the fundamental concepts of computer cybersecurity, including the importance of confidentiality, integrity, and availability of data. It delves into the various types of cyber threats faced by computer systems, such as malware, phishing attacks, data breaches, and social engineering techniques. Next, the survey investigates the common vulnerabilities and weaknesses that cyber attackers exploit to compromise computer security. This includes software vulnerabilities, weak authentication mechanisms, inadequate network security, and the challenges posed by emerging technologies like the Internet of Things (IoT) and cloud computing. The survey then discusses the countermeasures and best practices employed to safeguard computer systems against cyber threats. It covers the implementation of firewalls, antivirus software, intrusion detection systems, encryption protocols, and regular security updates. Additionally, it highlights the significance of user awareness training and policies to promote a culture of security within organizations [7].

This study recommends that in order to lessen the context of cyberbullying, particularly among our youth, people must strike a balance between cybersecurity awareness and cyberhuman values. To increase awareness of cybersecurity and develop cybersecurity competence at all levels, ongoing education and advocacy efforts are crucial [11]. The research paper extensively examines the critical exigency for cybersecurity measures and advocates for increased public awareness regarding the nature of cybercrimes, along with the proactive measures to shield against these pervasive threats. Cybersecurity entails a strategic practice designed to fortify systems, networks, and program files from potential infiltrations within digital networks. Cybercrimes predominantly focus on illicitly accessing or obliterating sensitive information, posing substantial risk to individuals and organizations alike. This comprehensive study is based on a combination of primary and secondary data sources. The primary data set encompasses responses to a meticulously crafted questionnaire provided by 298 individuals across diverse age groups, while the secondary data comprises information collated from a multitude of esteemed researchers.

The findings gleaned from the data analysis reveal alarming instances of individuals being subjected to abuse resulting from the compromise of their social media accounts, falling victim to various forms of financial fraud, and incurring substantial monetary losses through investment in spurious accounts. The study highlights the paramount need to assess the populace’s level of awareness regarding cybersecurity guidelines, with a considerable proportion of respondents demonstrating a commendable understanding of prescribed courses of action to undertake in the event of succumbing to cybercrimes. The overarching objective of this study is to obtain a comprehensive understanding of cybersecurity [12].

This study aimed to investigate the level of students' awareness of cybersecurity and cybersecurity education in Nigerian polytechnics. The survey objective was to assess the extent to which students in this developing country are adequately educated about cybersecurity, aware of cyberattacks, and knowledgeable in mitigating these attacks. Additionally, the study sought to determine if there is an inclusion of cybersecurity awareness and education programs within the Polytechnic curriculum. Initial findings revealed that while students claimed to possess basic knowledge of cybersecurity, they lacked sufficient understanding of data protection methods. Moreover, it was observed that most Polytechnics lacked an active cybersecurity awareness program to enhance students' knowledge of safeguarding themselves against cyber threats. The surveyed students expressed a desire for increased awareness and further education in the field of cybersecurity [13].

In this research paper, the authors designed a questionnaire instrument to measure the current level of cyber security awareness (CSA) among Fahad Bin Sultan University (FBSU) students. The questionnaire is designed to fulfill the goals of this research project aims and objectives. The main goal of this paper is to evaluate the level of cyber security awareness among FBSU students. Furthermore, cybersecurity students' awareness level questionnaire is adapted from a few other cybersecurity awareness-related questionnaires. A total of 212 students have participated in the survey. The study findings show that the students’ awareness is at an average level, and there is no difference in cybersecurity awareness level between male and female students. Furthermore, the survey instrument's results indicate that the module has been effective in measuring students' awareness [14].

This present research aims to determine the growing needs and challenges faced by Data Science and Cybersecurity students at Al Istiqlal University's Faculty of Information Technology when learning the English language. It also tries to ascertain whether gender and level of competence affected their requirements and difficulties in mastering the English language. 35 cadets who are specializing in data science and cybersecurity make up the sample. The researcher gave out 39 questionnaire items divided into eight domains. The results show that cadets in Data Science and Cybersecurity did not undergo any guidance regarding how to utilise English in the discipline while engaging in the analysis of data or cybersecurity keywords. Additionally, the study demonstrates that cadets majoring in data science and cybersecurity did not receive any guidance on how to learn to communicate in English, and the teaching activities in the English programs they had taken did not match their notions of the standards for expert English. Moreover, English proficiency requirements for cadets enrolling in Data Science and Cybersecurity courses should be taken into consideration. Additionally, no statistically meaningful differences in the demands for key competencies and barriers faced by Data Science and Cybersecurity cadets are found when gender and competency traits are taken into consideration [15].

This study examines the level of attitudes and awareness of university students towards cybersecurity. Based on quantitative research, the survey contrasts the attitudes of students in two disciplines computer science and media studies on a sample of 570 students. The results collected from the statistical analysis show similarities and differences in the responses of students in the two disciplines [16].

III. THE BENEFITS OF EDUCATIONAL CYBERSECURITY AWARENESS

1) Enhanced Security Posture: Reduced risk of cyber threats to students and staff.
2) Improved Compliance: Adherence to regulations and policies set by government and other relevant institutions.
3) Increased Awareness: Educated community on cybersecurity best practices makes the community more secure.
4) Better Incident Response: Swift and effective response to security incidents is critical during cybersecurity breach.
5) Protection of Sensitive Data: Safeguarding student and institutional data is important. Particularly, countries are enacting laws on Data Protection Regulations.
6) Cost Savings: Avoidance of financial losses due to cyber-attacks as more than 7 trillion USD is being lost annually due to cybercrime.
7) Reputation Protection: Maintenance of institutional reputation, as cybercrime and date breach tarnish the reputation of institutions [19].

IV. THE FOLLOWINGS ARE EFFECTIVE STRATEGIES TO BE DEPLOYED IN ORDER TO ENSURE THE SUCCESS OF EDUCATIONAL CYBERSECURITY AWARENESS CAMPAIGNS

1) Incentives and Awards: Recognition to individuals and institutions on cybersecurity success is key to the sustainability of educational cybersecurity awareness.
2) Real-world scenarios and case studies are also relevant and effective.
3) Collaborative Learning and Group Discussions
4) Phishing Simulations and Awareness Campaigns
5) Guest Lectures from Cybersecurity Experts from government institutions, academia, and industry are essential.
6) Integration with effective curriculum and academic programs.
7) Regular Security Audits and Vulnerability Assessments of ICT systems.

V. THE FOLLOWINGS ARE CYBERSECURITY AWARENESS FRAMEWORKS DEVELOPED FOR CYBERSECURITY

1) NIST Cybersecurity Framework
2) ISO 27001
3) SANS Cyber AWARE
4) Cybersecurity and Infrastructure Security Agency (CISA) Guidelines.

VI. The followings are also Key Performance Indicators (KPIs) in order to achieve educational cybersecurity awareness

1) Participation rates in training programs
2). Quiz and assessment scores
3) Incident response time and effectiveness
4) Number of reported security incidents
5) User behaviour and policy compliance.

VII. The followings are tools and resources for Educational Cybersecurity Awareness

1. Cybersecurity awareness platforms (e.g., KnowBe4)
2. Online training modules (e.g., SANS Securing the Human)
3. Phishing simulation tools (e.g., PhishMe)
4. Incident response software (e.g., Splunk)
5. Cybersecurity frameworks and guidelines (e.g., NIST, ISO).

VII. CONCLUSION/RECOMMENDATIONS

This comprehensive literature review has extensively examined the critical role of cybersecurity awareness in the educational sector, highlighting the alarming rise of cyber threats and the need for proactive defence strategies. The study has synthesised existing research, industry reports, and expert experiences to inform evidence-based cybersecurity awareness programs.

Key findings underscore the importance of educational interventions in mitigating user-related vulnerabilities, enhancing information system security, protecting sensitive data, reducing cyber-attack risks, and improving compliance with security protocols.

Based on these findings, the following recommendations and strategies are proposed:

Recommendations:
1) Integrate cybersecurity awareness into educational curricula.
2) Conduct regular phishing simulations and training exercises.
3) Develop incident response plans and protocols.
4) Foster a culture of cybersecurity awareness through workshops and campaigns.
5) Collaborate with cybersecurity experts and industry partners.

Strategies:
1) Incentives for cybersecurity awareness.
2) Real-world scenario-based training.
3) Collaborative learning and group discussions.
4) Integration with existing educational technologies.
5) Continuous monitoring and evaluation of cybersecurity awareness programs.

Implementing these recommendations and strategies will empower educational institutions to safeguard sensitive data, protect against cyber threats, and foster a culture of cybersecurity awareness among students, faculty, and staff.

Future research directions include exploring the effectiveness of these strategies and investigating emerging trends in cybersecurity threats and defence mechanisms [20-25].

REFERENCES

1. Per G., Beata G., ”Computer Games as a Pedagogical Tool for Creating Cyber Security Awareness”, Proceedings of the 17th European Conference on Games Based Learning, Vol. 17 No. 1, https://papers.academic conferences.org/index.php/ecgbl/article/view/1407, 2023.
2. Arshiya S., Iftikhar A. K., Usman A., ”Importance of Conducting Cyber Security Awareness Sessions among Undergraduate Students”, Journal of Advanced Research in Social Sciences and Humanities Volume 8, Issue 2, pp.59-68, 2023, DOI: https://dx.doi.org/10.26500/JARSSH-08-2023-0202.
3. Jinghua Z., Xiaohong Y., Jinsheng X., Elva J. J., “Developing and Assessing Educational Games to Enhance Cyber Security Learning in Computer Science”, In Proceedings of the ACM Conference on Global Computing Education (CompEd '19). Association for Computing Machinery, New York, NY, USA, 241, 2019, https://doi.org/10.1145/3300115.3312511.
4. Ishika J., Ritvik B., Harshal D., Jahnvi K., Mohammad O. A., Sayan M., Harshal D. A., Dhruv K., “ChatGPT in the Classroom: An Analysis of Its Strengths and Weaknesses for Solving Undergraduate Computer Science Questions” In Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2024). Association for Computing Machinery, New York, NY, USA, 625–631, 2024, https://doi.org/10.1145/3626252.3630803.
5. Yunita S., Siti N. S., “The Role of Cyber Media and Public Science Education”, Jurnal Penelitian Pendidikan IPA Journal of Research in Science Education, Vol. 9, No. 11, 2023, http://jppipa.unram.ac.id/index.php/jppipa/index.
6. Sahu et, al., “A Study on Cyber-Crime Awareness Among Students in Chhattisgarh. Journal of Ravishankar University”, SOCIAL-SCIENCE, Vol. 30, No. 1, Pp.54-60, 2024, https://doi.org/10.52228/JRUA.2024-30-1-6.
7. Chya O. Q., Ann Z. A., “Survey on Computer Cyber Security”, Journal on Modern Research Methodologies, Volume 2, Issue 9, https://univerpubl.com/index.php/woscience.
8. Ponemon Institute, The State of Cybersecurity in Organizations: A Global Survey, (2019).
9. Zawoad et al., “Cybersecurity Threats, Vulnerabilities, and Countermeasures A Survey", (2018).
10. Alaba et al., “A Systematic Review of Internet of Things (IoT) Security: Current State, Challenges, and Countermeasures,”, 2020.

11. Cheong S, X,, Muslihah H., "Cybersecurity Awareness, Cyber Human Values and Cyberbullying Among University Students in Selangor, Malaysia", International Journal of Advanced Research in Technology and Innovation, Vol. 5, No. 2, Pp. 1-11, 2023, http://myjms.mohe.gov.my/index.php/ijarti.
12. Padmavati S. U., Vedant S., "Digital Transformation and Cyber Security: Unveiling Awareness", International Journal of Linguistics, Humanities, and Education, Volume 1 Issue 3, June 2024.
13. Aliyu A., et al., "Cyber Security Education and Awareness", Ilaro Journal of Science and Technology (IJST), Volume 3, https://sciencetechjournal.federalpolyilaro.edu.ng, 2023.
14. Wejdan A., Nazar E., "Measuring Cyber Security Awareness of Students: A Case Study at Fahad Bin Sultan University", International Journal of Computer Science and Mobile Computing, Vol.9, Issue.6, Pp. 141-155, June-2020.
15. Khaled M. M., "English Competencies and Challenges for Data Science and Cyber Security Students at Al Istiqlal University", The Creative Launcher, Vol. 7, Issue 5, https://www.thecreativelauncher.com/index.php/tcl. October, 2022.
16. Ladislav H., at al., "Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students", TEM Journal. Volume 12, Issue 2, pages 623-633, DOI: 10.18421/TEM122-05, May 2023.
17. Muhammad A. B, Aminu Ya'u, Sirina F. Ibrahim, Bello A.Imam, M. Aliyu Yusif, Abubakar S. M, Aliyu M. Lawan, & Abdulmuhamin M. "Management of Vulnerabilities in Cyber Security", Global Journal of Research in Engineering & Computer Sciences, Vol. 3, No. 2, Pp. 14–18, 2023, https://doi.org/10.5281/zenodo.7779507.
18. Muhammad Ahmad. Baballe, A. Hussaini, M. Ibrahim Bello, & U. S. Musa. "Online Attacks Types of Data Breach and Cyber attack Prevention Methods", Global Journal of Research in Engineering & Computer Sciences, Vol 2, No. 5, Pp. 1–5, 2022, https://doi.org/10.5281/zenodo.7144657.
19. https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/.
20. Isa A. I., Muhammad A. B. "An overview of the Internet of Things (IoT) Architecture", In Global Journal of Research in Engineering & Computer Sciences, Vol. 4, Number 5, pp. 34–39, 2024, https://doi.org/10.5281/zenodo.13750012.
21. Isa A. I., "National Security in Nigeria: Emerging Technology and Prospects for Enhanced Military Operations", https://www.researchgate.net/publication/360778779_National_Security_in_Nigeria_Emerging_Technology_and_Prospects_for_Enhanced_Military_Operations, 2021.
22. Isa A. I. P., Femi D., "Cyber-Terrorism: Legal and Policy Options forCoordinated National Preparedness", National Journal of Cyber Security Law, Volume 1, Issue 1, www.stmjournals.com, 2018.
23. Isa, A. I., "Nigeria's Ethical Issues in the Use of ICT", 2018, https://www.researchgate.net/publication/325253081.
24. Lukman L. I., Isa, A. I., Usman G. A., "A Model and Architecture for Building a Sustainable National OpenGovernment Data (OGD) Portal", ICEGOV'18, April 2018, Galway, Ireland.
25. Isa, A., I., "Cybersecurity Initiatives For Securing a Country", University Press PLC, (March 9, 2023).

CITATION

Abubakar S. I., Nurudeen D. G., Muhammad M. H., & Muhammad A. B. (2024). Educational Cybersecurity Awareness in the Digital Era: A Comprehensive Review. In Global Journal of Research in Engineering & Computer Sciences (Vol. 4, Number 6, pp. 89–94). https://doi.org/10.5281/zenodo.14488381