Scholarly Research Journal for Interdisciplinary Studies
Online ISSN 2278-8808, SJIF 2024 = 8.153
https://www.srjis.com/issues_data/246
Peer Reviewed & Refereed Journal, JAN-FEB 2025, Vol- 13/87

CYBERSECURITY AWARENESS AMONG STUDENTS: A RESEARCH REVIEW

Prof. Shaheen Shaikh

Department of Education and Training, MANUU, Hyderabad

Email-shaikh.shaheen9@gmail.com

Paper Received On: 20 JAN 2025

Peer Reviewed On: 24 FEB 2025

Published On: 01 MAR 2025

Abstract

The incorporation of digital technology in education has increased students' exposure to cyber threats, making cybersecurity awareness a critical concern. This literature review examines students' awareness of cyber threats, prevalent vulnerabilities, and the efficacy of educational interventions. The findings indicate that while students grasp basic risks, their cybersecurity practices are inconsistent and often render them susceptible to phishing, social engineering, and ransomware attacks. Common perilous practices encompass password reuse, neglecting software updates, and carelessly accessing unsecured public Wi-Fi networks. Through efforts such as seminars, gamification, and peer-driven campaigns, which have proven effective in enhancing students' ability to recognize and combat cyber dangers, educational institutions play a crucial role in raising awareness. The research demonstrates the influence of parental involvement, peer networks, and social media on students' digital conduct. Two-factor authentication and the incorporation of cybersecurity modules into the curriculum significantly reduce hazardous behaviors through institutional rules. Awareness programs must adapt to evolving cyberthreats to cultivate improved digital practices among students. The paper underscores the necessity of a dynamic and multifaceted approach to cybersecurity education, integrating frequent training, practical experience, and community involvement to foster a safer digital environment for students.

Keywords:- *Cybersecurity Awareness, Student Digital Safety, Cybersecurity Threats, Cybersecurity Education.*

Introduction

Students are more interconnected than ever in the digital era, relying on technology for entertainment, communication, and education. The significance of cybersecurity knowledge among students has increased as online learning and the incorporation of digital resources into educational environments become more prevalent (Kim et al., 2022). Students frequently engage with academic resources, manage personal data, and interact on social media, often

without fully understanding the associated hazards (Alqahtani et al., 2021). Consequently, they have become primary targets for cyberattacks, encompassing phishing, malware, identity theft, and social engineering (Vishwanath et al., 2020). The growing dependence of students on digital media has subjected them to several online dangers. Despite a comprehension of basic security concepts among several students, research indicates that their actual conduct often fails to safeguard their digital presence (Alotaibi et al., 2021; Abdulhamid et al., 2022). For instance, numerous students either fail to recognize phishing attempts or reuse passwords across multiple accounts, so becoming themselves vulnerable to fraudsters (Singh & Sharma, 2023). Moreover, the increasing utilization of public Wi-Fi networks and personal devices for academic activities exacerbates risk; hence, students must cultivate robust cybersecurity practices (Patel & Jones, 2023).

The cybersecurity expertise of students is significantly influenced by universities and other educational institutions. Through comprehensive awareness campaigns, implementation of security policies, and practical training, students' vulnerability to cyberattacks can be significantly reduced (Kapoor & Singh, 2022). Despite several awareness programs, many students remain uninformed about the actionable measures necessary for their online protection (Tade & Aliyu, 2020). Formulating effective instructional tactics necessitates an understanding of the factors influencing cybersecurity behavior and knowledge. This paper seeks to encapsulate contemporary research on cybersecurity awareness among students, highlighting principal concerns, prevalent dangers, and the efficacy of institutional interventions. The study seeks to elucidate the gap between knowledge and behavior to enhance cybersecurity education and promote improved digital conduct among students.

Methodology - Literature Review

This review synthesizes results from surveys, academic papers, and instructional reports published between 2015 and 2023. The literary search yielded phrases such as "cybersecurity awareness," "student digital safety," and "cyber threat education." To ensure comprehensive coverage of the topic, data was collected from reputable sources like IEEE Xplore, Springer, and Google Scholar.

Findings

Identifying Cybersecurity Threats - Research indicates that students typically underestimate the gravity of cyberattacks. According to a 2019 Johnson survey, only 45% of students were able to accurately identify phishing attempts. Alotaibi (2020) underscores that ignorance on the operations of cybercriminals frequently renders students susceptible to social engineering

tactics.

Common Vulnerabilities - Students frequently engage in perilous actions such as password sharing and unsafe utilization of public Wi-Fi. Williams (2021) asserts that 60% of students acknowledged utilizing passwords across several platforms. Additionally, research by Sharma and Gupta (2022) illustrates the frequency with which students neglect software updates and lack comprehension of the importance of antivirus protection.

In 2018, a prominent university experienced a targeted phishing attack that compromised the personal information of over 1,000 students. The attackers solicited students' login credentials by dispatching fraudulent emails impersonating university IT support. A post-incident survey revealed that 65% of the affected pupils had not received formal training on recognizing phishing efforts. Subsequent to mandatory cybersecurity training, additional phishing simulations indicated a 40% reduction in students employing associated tactics (Kumar et al., 2021).

Gamification in Cybersecurity Education - Ntim (2021) documented a project that integrated gamified learning into a high school cybersecurity curriculum. Students participated in capture-the-flag competitions and other interactive activities designed to enhance their ability to identify and mitigate cyber risks. The study revealed increased engagement and a 35% improvement in students' proficiency in recognizing potential intrusions. Interventions such as gamification, simulations, and seminars have demonstrated efficacy in enhancing awareness and fostering proactive behavior. Incorporating game-based learning into cybersecurity education enabled Ntim (2021) to enhance both engagement and information retention. Tariq et al. (2019) assert that the sustainability of awareness relies on consistent reinforcement through practical simulations and training.

Role of Peer Influence and Social Media - The role of peer influence and social media in shaping students' cybersecurity behaviors is significantly crucial. Research conducted by Kritzinger and von Solms (2018) emphasizes that peer-driven efforts may create a domino effect, hence enhancing knowledge within student communities. A 2020 study conducted at a European institution examined the implications of students over disclosing personal information on social media. A child inadvertently disclosed sufficient personal information on Instagram to facilitate a fabricated identity theft. After participating in a cybersecurity awareness program featuring real-world instances of identity theft, students exhibited increased caution regarding their online activities, resulting in a 50% reduction in risky behavior within six months (Kay et al., 2018). Utilizing social media platforms to provide cybersecurity

guidance and real-life hacking incidents has demonstrated effectiveness in reaching broader audiences (Kay et al., 2018).

Parental and Teacher Involvement - Parental and teacher involvement significantly affects students' cybersecurity behaviors. Kumar et al. (2021) assert that institutions incorporating cybersecurity components into their standard curricula have heightened levels of student awareness. Involvement of family—particularly with younger learners—fosters positive digital practices at home. The ever-evolving nature of cyber threats necessitates a flexible approach to cybersecurity education. Emerging threats necessitate the adaptation of curricula and awareness activities. Brown (2018) underscores the necessity of keeping teaching materials updated and aligned with the latest risk contexts to prepare students for current and future threats.

Cybersecurity Proficiency - Research indicates that students' understanding of cybersecurity differs. According to Alotaibi et al. (2021), 65% of students could identify common cyber threats, although only 30% practiced effective password hygiene. Forty percent of university students indicated that Abdulhamid et al. (2022) employed passwords across several platforms, hence increasing their susceptibility to credential stuffing assaults. Only 25% of students employ distinct passwords for many accounts, while Tade and Aliyu (2020) discovered that students often underestimate the risks associated with weak passwords. Research by Aslam et al. (2021) and Kapoor and Singh (2022) indicates that students often exaggerate their cybersecurity awareness, leading to perilous online behaviors. Alqahtani et al. (2021) emphasized that while students were aware of basic threats, hardly 15% could identify more advanced assaults such as pharming or spear phishing.

Common Cyber Attacks Encountered by Students - Students frequently confront phishing as a significant concern. Vishwanath et al. (2020) report that at least 47% of students had succumbed to phishing scams at least once. According to Jayanthi et al. (2021), approximately 35% of students inadvertently downloaded malware, frequently from questionable email attachments. Alqahtani et al. (2021) observed that students frequently encountered social engineering attempts, with 60% admitting to having disclosed confidential information online without verifying the source. Singh and Sharma (2023) demonstrated that a 15% rise in remote learning corresponded with a 15% increase in ransomware incidents among students during the prior two years. According to estimates by the National Cybersecurity Alliance (2023) and Patel and Jones (2023), 55% of students connect without utilizing VPNs, highlighting significant concerns regarding unsafe public Wi-Fi networks.

Impact of Cybersecurity Training - Training in cybersecurity significantly enhances awareness and behavior. Students that participated in cybersecurity seminars increased their phishing detection rates by 60%, as reported by Kim et al. (2022). Training, as noted by Abdulhamid et al. (2022), resulted in a 45% reduction in hazardous behaviors, such as password sharing. Students who received training were 70% more inclined to utilize two-factor authentication, according to research by Singh and Sharma (2023) and Tade and Aliyu (2020). Patel and Jones's (2023) investigation indicated that taught students were 50% less likely to connect to unprotected Wi-Fi networks. Renaud et al. (2022) found that training increased the adoption of antiviral software by 40%, but Kapoor and Singh (2022) noted that awareness campaigns enabled students to recognize social engineering approaches.

Employing Security Instruments and Strategies - The adoption of security tools among students is highly variable. According to Renaud et al. (2022), eighty percent of students utilized antiviral software, although only thirty-five percent maintained its currency. Despite its availability, only 50% of students activated two-factor authentication, as reported by Kim et al. (2022). Research by Vishwanath et al. in 2020 indicated that just 20% of students reported using password managers. Research conducted by Alqahtani et al. (2021) and Jayanthi et al. (2021) indicated that the majority of students connected to public Wi-Fi without employing VPNs, so becoming themselves vulnerable to man-in-the-middle attacks. Singh and Sharma (2023) noted that 40% of students disregarded software upgrades, mostly due to inadequate understanding of vulnerability remediation.

The Efficacy of Institutional Policies - The nature of cybersecurity activity is profoundly affected by institutional policies. Universities mandating cybersecurity training had a 50% reduction in reported cyber incidents, as stated by Patel and Jones (2023). In 2023, Singh and Sharma emphasized that student compliance rose to 85% with the implementation of two-factor authentication by institutions. Abdulhamid et al. (2022) observed that consistent awareness campaigns led to a 40% increase in students updating their devices. Alqahtani et al. (2021) observed that universities with extensive regulations exhibited higher acceptance of VPNs and password managers. Kim et al. (2022) and Kapoor and Singh (2022) indicated that institutions providing practical training significantly reduced detrimental online behaviors, such as accessing unfamiliar URLs and downloading unauthorized applications.

Conclusion

The findings of this study reveal significant new insights into students' awareness of cybersecurity. The diverse levels of students' awareness indicate a gap in formal instruction and training about digital safety. Abawajy et al. (2016) assert that numerous students lack awareness of essential cybersecurity concepts, rendering them vulnerable to phishing and identity theft. The illusory sense of safety provided by digital devices significantly contributes to adolescents' perilous online behavior. Hadlington (2017) asserts that complacency arises when students perceive cybersecurity as the responsibility of service providers or institutions. This perspective underscores the necessity of tailored teaching that fosters accountability for individual digital safety. Interventions such as gamification, simulations, and seminars have demonstrated efficacy in enhancing awareness and fostering proactive behavior. Integrating game-based learning into cybersecurity education enabled Ntim (2021) to enhance both engagement and information retention. Tariq et al. (2019) assert that the sustainability of awareness relies on consistent reinforcement through practical simulations and training. The role of peer influence and social media in shaping students' cybersecurity behaviors is significantly crucial. Research conducted by Kritzinger and von Solms (2018) emphasizes that peer-driven efforts may have a cascading effect, inherently enhancing knowledge within student groups. Utilizing social media platforms to provide cybersecurity guidance and real-life hacking incidents has effectively expanded audience reach (Kay et al., 2018). Moreover, parental and institutional involvement significantly impacts students' cybersecurity behaviors. Kumar et al. (2021) assert that institutions incorporating cybersecurity components into their standard curricula have heightened levels of student awareness. Family involvement—particularly with younger students—fosters positive digital practices at home. The ever-evolving nature of cyberthreats necessitates a flexible approach to cybersecurity education. Emerging threats necessitate the adaptation of curricula and awareness activities. Brown (2018) underscores the necessity of keeping educational materials up-to-date and aligned with contemporary risk contexts to ensure students are equipped to handle current and future threats. Essentially protecting pupils' digital existence relies on enhancing their cybersecurity awareness. The primary emphasis of future studies should be on long-term intervention outcomes and the exploration of innovative teaching methodologies. A secure digital environment for pupils relies on collaborative initiatives among legislators, cybersecurity experts, and educational institutions.

References

Abawajy, J. (2016). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 35(3), 1–10. https://doi.org/10.1080/0144929X.2015.1015166

Abdulhamid, S. M., et al. (2022). Analyzing students' cybersecurity behavior and awareness. Journal of Information Security and Applications, 62, 102933. https://doi.org/10.1016/j.jisa.2022.102933

Alotaibi, S. (2020). Investigating students' awareness of social engineering attacks. Computers & Security, 90, 101707. https://doi.org/10.1016/j.cose.2020.101707

Alotaibi, S., et al. (2021). Evaluating cybersecurity awareness among university students. International Journal of Computer Science and Information Security, 19(4), 35–45.

Alqahtani, F., et al. (2021). Understanding students' cybersecurity awareness and behaviors. Education and Information Technologies, 26(3), 2535–2552. https://doi.org/10.1007/s10639-020-10432-1

Aslam, M., et al. (2021). The gap between knowledge and practice in cybersecurity: An assessment of university students. Journal of Cybersecurity Education, 5(1), 45–60.

Brown, C. (2018). Updating cybersecurity education to address emerging threats. Journal of Cyber Policy, 3(2), 215–230. https://doi.org/10.1080/23738871.2018.1509045

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction and risky online behavior. Cyberpsychology, Behavior, and Social Networking, 20(9), 567–572. https://doi.org/10.1089/cyber.2017.0175

Jayanthi, N., et al. (2021). Identifying risky behaviors leading to malware attacks among students. Journal of Information Security, 12(2), 105–119.

Kapoor, A., & Singh, R. (2022). Enhancing cybersecurity awareness through educational interventions. International Journal of Technology in Education and Science, 6(1), 54–67.

Kay, R., et al. (2018). Reducing social media oversharing among students: A cybersecurity awareness initiative. Journal of Educational Technology Systems, 47(2), 143–160. https://doi.org/10.1177/0047239518777607

Kim, H., et al. (2022). The impact of cybersecurity training on students' online behavior. Journal of Information Security and Applications, 65, 103077. https://doi.org/10.1016/j.jisa.2022.103077

Kritzinger, E., & von Solms, S. H. (2018). Cybersecurity education and awareness: A pedagogical perspective. SA Journal of Information Management, 20(1), 1–8. https://doi.org/10.4102/sajim.v20i1.937

Kumar, V., et al. (2021). Institutional strategies to enhance cybersecurity awareness among students. Education and Information Technologies, 26(2), 987–1004. https://doi.org/10.1007/s10639-020-10344-2

Ntim, S. (2021). Gamification in cybersecurity education: Improving engagement and awareness. Journal of Information Systems Education, 32(1), 45–56.

Patel, R., & Jones, T. (2023). Assessing public Wi-Fi risks and students' security practices. Cybersecurity Journal, 12(1), 67–82.

Renaud, K., et al. (2022). Promoting the use of security tools among students: A behavioral approach. Computers & Security, 118, 102752. https://doi.org/10.1016/j.cose.2022.102752

Sharma, P., & Gupta, S. (2022). Examining students' password management practices. International Journal of Cybersecurity Intelligence & Cybercrime, 5(2), 23–38.

Singh, A., & Sharma, R. (2023). Understanding students' cybersecurity behaviors in remote learning environments. Journal of Information Security, 13(1), 31–45.

Tade, O., & Aliyu, A. (2020). Exploring university students' cybersecurity practices. African Journal of Information Systems, 12(1), 45–60.

Tariq, R., et al. (2019). Enhancing cybersecurity awareness through continuous education. Information & Computer Security, 27(4), 498–512. https://doi.org/10.1108/ICS-09-2018-0115

Vishwanath, A., et al. (2020). Phishing susceptibility among students: An experimental study. Social Science Computer Review, 38(2), 223–239. https://doi.org/10.1177/0894439318771015

Williams, C. (2021). Investigating password practices among students. Journal of Digital Security, 14(3), 78–92.

National Cybersecurity Alliance. (2023). State of cybersecurity awareness in education: Annual report. https://staysafeonline.org/reports