Cybersecurity in Higher Education: A Systematic Review of Threats, Challenges, and Mitigation Strategies

Hanan Mahmood Baleid[1]
Mohammed Fadhl Abdullah[1*]

Received: 01/01/2026
Revised: 04/01/2026
Accepted: 12/01/2026

[1] College of Engineering and Computing, University of Science and Technology, Aden, Yemen.
*Corresponding Author's Email: h.baleid @student.ust.edu

Cybersecurity in Higher Education: A Systematic Review of Threats, Challenges, and Mitigation Strategies

Hanan Mahmood Baleid[1,2], Mohammed Fadhl Abdullah[1,3]
[1]*College of Engineering and Computing, University of Science and Technology, Aden, Yemen*
[2] h.baleid @student.ust.edu,[3]m.albadwi@ust.edu

Abstract— The digital transformation in institutions of higher learning has been very rapid, hence becoming a good target for the changing cyber threats. This study presents a systematic review of cybersecurity research in higher education published between 2020 and 2025. It aims to identify dominant threat types, key challenges, and prevailing mitigation strategies. A total of 45 peer-reviewed studies were analyzed, and the findings indicate that phishing attacks remain the most prevalent threat, reported in 75% of the reviewed studies, followed by denial-of-service attacks (62.5%) and ransomware (60%). This review exposes an interesting paradox, namely, although artificial intelligence and machine learning models are more effective in detecting the threat, the application of the traditional method is still prevalent (62.5%), as opposed to 15 percent of the studies devoted to the use of AI-based solutions, because of financial limitations, knowledge gaps, and the problem of privacy. The findings also indicate that the main causes of weakness in the open academic institutions are the human factor and the poor internal governance. Therefore, to keep the academic environment safe and to deal with the evolving cyber threats, it is essential to activate a multi-faceted security approach that involves the use of operative technologies, active educational programs (that are anchored on simulation and evaluation), and strengthened institutional cooperation.

Keywords— *Cybersecurity in higher education, phishing, human factor in cybersecurity, cybersecurity awareness, mitigation strategies*

I. Introduction

A. Digital Transformation and Cybersecurity in Higher Education

The broad use of technology in the modern-day digital age has essentially changed the face of higher education and redefined the nature of teaching, management, and the interaction among students. Higher education is characterized by openness, diversity of users, and reliance on external services. Online platforms, research databases, and communication tools have been used every day by students, faculty, and staff with massive amounts of personal, sensitive data, including institutional data. Although this digital transformation has provided the sector with unprecedented flexibility, it has also left the sector vulnerable to major and increasing cybersecurity [1]. As a result, the sphere of higher education has been a major target of ill-intentioned players, and cyberattacks have been a common occurrence with profound data leaks and operational destabilization across the world.

B. Predominant Cybersecurity Threats and the Human Factor

The issue of cybersecurity is characterized by the alarming rate of the high occurrence of attacks and a high level of sophistication. Cybersecurity trends in the world affirm that the trend of cybercrime has increased dramatically, and the FBI registers over 880,418 complaints with losses of over 12.5 billion in 2023 alone [2]. Interestingly, data breaches in 2020-2021 were largely conducted by phishing and other social engineering methods, business email compromise, and malware. As of 2022, ransomware attacks became more common than phishing, and the reason is that they tend to be more effective at causing massive data breaches and extortion [3]. This shifting threat landscape highlights a very important weakness: the human factor. The first line of defense depends on the capabilities of end users who are members of the educational institution; nevertheless, the ongoing problem is that many of them do not know how to detect deceptive material and understand that it is an attack [4].

C. Impacts and Challenges for Higher Education Institutions

Cyberattacks on the academic institutions can result in, besides the high financial losses, a continued disruption of the services and compromise of sensitive institutional data. Academic institutions are also complicated by the uptake of cloud services in terms of their security posture. It has been shown that 48 percent of institutions have employee data stored in the cloud, and 30 percent have student data stored in the cloud. Nevertheless, this change brings about shared responsibility models in which, as Gartner states, more than 95 percent of security faults in the cloud setting can be placed on customer misconfiguration or error. In 2020, 60 percent of learning institutions reported having become victims of phishing, and 33 percent of them had their accounts compromised. The specified example illustrates the extent to which these threats are targeted: in June-September 2020, spear-phishing scams were launched targeting the organizations representing about 1,000 schools, colleges,

and universities [5]. Phishing is among the most widespread and is constantly growing in nature, and one of the fundamental challenges is to ensure the confidentiality, integrity, and availability of the data in the distributed environments [6].

Therefore, it is necessary to promote effective cybersecurity awareness to enable the members of the academic circles to identify these tricks, make wise choices, and embrace more active security practices, thus eliminating the attack surface directly [7]. The provision of specific cybersecurity education and training to all stakeholders, students, faculty, and staff, is a pressing issue that the higher learning institutions should address. This is exacerbated by the fact that the sector has an open culture, can attract a wide range of users, and that breaches can have devastating financial and reputational effects when they are successful [8]. It is in this light that in an environment framed by widespread instances of data breaches and high-profile attacks, the necessity to establish resilient cybersecurity measures is an urgent mandate among educational institutions [9]. The volume of digital interaction intensifies this requirement, with a global count of over 7 billion mobile users and over 2 billion internet users sending out nearly 294 billion emails and 5 billion mobile messages each day [10], [11], [12]. Such a large attack surface requires a multifaceted and holistic approach to defense.

D. Research Gap, Objectives, and Contributions

The rapid pace of digital transformation and the emergence of new attack vectors necessitate an aware synthesis of new research findings and the development of an integrated view of the evolving threat landscape. To address this gap, this review study set a goal to generalize the existing studies on cybersecurity in the field of education. It discusses the specific issues of higher education establishments, identifies the common threat vectors, especially social engineering and cloud vulnerability, and reviews existing models and practices of cybersecurity awareness, education, and training. The study also offers a consistent perspective of the prevailing situation and offers significant research gaps to be addressed in the future that will enhance the educational sector against the constantly changing line of various cyber threats.

Accordingly, the main research question guiding this study is, "What are the prevailing research trends and findings in cybersecurity within the higher education sector based on studies published between 2020 and 2025?"

Although several studies have examined cybersecurity in education, few provide a comprehensive and up-to-date synthesis focusing specifically on higher education institutions in the post-COVID digital transformation era. This study addresses this gap by systematically reviewing recent research (2020–2025) and identifying dominant threats, challenges, and mitigation strategies.

II. Research Methodology and Review Design

The research methodology used in this study is a comprehensive systematic literature review, which helps to summarize and evaluate the studies published in the sphere of educational cybersecurity during the period of 2020-2025. In the main academic databases (IEEE Xplore, Scopus, Web of Science, ScienceDirect, and ACM Digital Library), a systematic search was implemented with the set of search words "cybersecurity in education" OR "educational cybersecurity" and "higher education" or "online learning" and "threats" or "attacks" or "vulnerabilities" or "solutions." The search was narrowed down to the educational context and needed empirical or theoretical analysis. Articles that were not peer-reviewed, those studies that were published earlier than 2020, and non-academic reports were eliminated. A total of 150 articles were initially identified. After removing duplicates and applying inclusion and exclusion criteria, 45 studies were selected for final analysis.

III. Cybersecurity in Higher Education: Review of Existing Studies

Past research has been a pillar in the context of the interpretation of present trends and future prospects in cybersecurity within the educational system. As modern technologies gain more and more popularity in the educational and administrative activities, and the pace of the process of digital transformation increases, educational institutions become the target of different cyberattacks. The goal of this section is to review and analyze the most notable publications and studies published since 2020, which is a review of the most significant research trends and challenges, as well as solutions to the cybersecurity issue in a classroom, which would help improve the state of affairs in educational settings, as demonstrated in Table 1.

The paper offers that the education sector is yet another sector that has been a victim of the cyberattacks, citing intricate technical, human, and structural aspects. As it has been shown, the most prevalent types are phishing, malware, and ransomware [13], [14], [15], and attacks are becoming more advanced and use the open nature of universities, which is challenging to manage on a technical level [16].

Other works also indicate that the human factor is the most vulnerable aspect of the educational institutions because of a low level of security consciousness among the students and employees, ineffective password usage, and inadequate training [17], [18], [19], [20]. The absence of definite governance and control policies, it

has been confirmed by other studies, is one of the most significant vulnerabilities, particularly in institutions of higher learning that have disjointed technology infrastructure and depend heavily on external service providers [21], [22], [23].

Moreover, a literature review suggests that the accelerated digital transformation, in particular after the COVID-19 pandemic, has increased the attack surface and the number of denial-of-service attacks, videoconferencing attacks, and cloud and LMS attacks [13], [24], [25].

Other researchers have found that there is a large gap between the security policies and their real application in educational institutions that contributes to the existing threat despite the possibilities of the use of technological means [26], [27], [28]. Other reports point out that the shortage of professional staff and the inability to afford complex security systems like artificial intelligence or multi-layered systems are one of the greatest barriers to implementing advanced security measures [29], [30], [31], which are not yet on the list.

IV. Results of the Systematic Literature Review

The temporal distribution in Table 2 indicates the growing attention to the topic of cybersecurity in education. The latest figures (including the phishing paper of 2023), obtained after adding it, show that 92.5% of papers (37 of 45) were written within the past four years, which can be taken as the testimony of the exceptional urgency of the topic. There are 24.5% of publications in 2024, and 22.2% of publications in 2025, meaning that the topic is still actively researched. The number of 2023 publications increased to 12 articles (26.7%), which have been added, and the research has reacted quite fast to the current challenges. The comparatively low publication level in 2020 (4.4%) indicates how the discipline shifted its status from an emerging issue into a pressing problem in a short period of time.

Table 1. Temporal Distribution of Reviewed Studies (2020–2025).

Published Year	Frequency	Percentage
2025	10	22.2%
2024	11	24.5%
2023	12	26.7%
2022	5	11.1%
2021	5	11.1%
2020	2	4.4%
Total	45	100.0%

A. Predominant Cybersecurity Threats in Higher Education

The aforementioned 45 works cited in the previous studies in the area of cybersecurity in education. Table 2 shows that there is a complex threat environment that is aimed at the education sector. The most mentioned threat is phishing attacks (72.5%), which proves that the human factor is still the weakest point in the security chain. It is highly related to social engineering (57.5%), which means that most successful attacks are initiated by taking advantage of the gaps in user psychology and security awareness, but not only by the intricate technical vulnerabilities. In its turn, the data has demonstrated the prevalence of two critical technical threats, namely DDoS attacks (62.5%) and ransomware (60.0%). The latter represents the immediate danger to the survival of the digital learning processes as remote learning becomes prominent. The latter is the most damaging threat in terms of payment and interference with the work. The high rate of insider threats (47.5) reflects the complicated security situation in the educational institution, where the risk can be created either purposefully or negligently inside the campuses. Also, the rise of threats such as supply chain attacks (5.0%) and IoT attacks (5.0%), which are currently not very common, is an indication of a growing attack surface as institutions increase their digitalization and dependence on third-party vendors and smart devices [32], [33], [34].

Table 2. Cybersecurity Attacks Types as Identified in Higher Education Institutions

No	Attack / Threat	Freq	%	No	Attack / Threat	Freq	%
1	Phishing Attacks	**30**	**75.0 %**	9	SQL Injection	7	17.5%
2	Malware (General)	26	65.0 %	10	Spoofing/Impersonation	7	17.5%
3	DDoS/DoS Attacks	**25**	**62.5 %**	11	Cross-Site Scripting (XSS)	5	12.5%
4	Ransomware	**24**	**60.0 %**	12	Cyberbullying / Harassment	5	12.5%
5	Social Engineering	**23**	**57.5 %**	13	Vulnerability Exploitation	5	12.5%
6	Insider Threats	**19**	**47.5 %**	14	Zoombombing Attacks	3	7.5%
7	Data Breaches/Theft	18	45.0 %	15	IoT Attacks	2	5.0%
8	Unauthorized Access	12	30.0 %	16	Supply Chain Attacks	2	5.0%

The dominance of phishing attacks (75%) highlights the persistent vulnerability of human users in academic environments. This finding is consistent with ref [38], who emphasize that students remain highly susceptible to social engineering techniques, particularly in remote learning contexts.

A. Key Challenges and Impacts of Cybersecurity Attacks

The major impacts of cybersecurity attacks on higher education institutions are illustrated in Table 3. The data makes Financial Losses & Costs (77.5%) and Disruption of Educational Operations/Services (72.5%) the most crucial outcomes, and cyber incidents should be viewed as a direct trigger of devastating budget crises and the fundamental sabotage of the academic mission of an institution. This operational and financial shock triggers a series of devastating effects: a resultant Sensitive Data Breach/Leakage (67.5%) inevitably gives rise to a devastating Reputational Damage (65.0%), which, further, causes devastating Legal and Regulatory Consequences (37.5%). These three interrelated parts of the triad deplete the most precious capital of stakeholder trust (20.0%). The consequences directly and progressively spread to the human aspect, where Privacy Violation (35.0%) and Psychological and Social Impact (30.0%) emerge as the essential aspects to be considered, and the actual cost is paid by personal welfare and constitutional rights [34], [35]. Moreover, the Intellectual Property & Research Theft (22.5%) poses a serious strategic risk to research-intensive institutions, as they risk losing the source of their competitive advantage and even the nature of scholarly innovations [36], [37].

Table 3. Major Impacts of Cybersecurity Attacks Affecting Higher Education Institutions.

NO	Challenge	Frequency	%
1	Financial Losses & Costs	31	77.5%
2	Disruption of Educational Operations/Services	29	72.5%
3	Sensitive Data Breach/Leakage	27	67.5%
4	Reputational Damage	26	65.0%
5	Privacy Violation	14	35.0%
6	Legal & Regulatory Consequences	15	37.5%
7	Psychological & Social Impact	12	30.0%
8	Intellectual Property & Research Theft	9	22.5%
9	Loss of Stakeholder Trust	8	20.0%
10	Resource/Infrastructure Misuse	4	10.0%
11	**Academic Record Fraud**	3	7.5%

V. Discussion of Findings and Emerging Trends

This systematic review reveals an interesting paradox in the existing situation in cybersecurity in higher education. On the one hand, there is strong evidence that threat detection methods are far better when applied using artificial intelligence. Conversely, the traditional defensive approach is still primarily used at 62.5%, in total opposition to an insignificant 15% of research concentrating on AI-based solutions. The reasons behind this imbalance lie in the substantive material and practical factors, such as the prohibitive nature of the contemporary technologies, a high lack of specialized staff, and valid fears related to the confidentiality of the academic information.

The outlook of certain threats is also persistently dominant despite a substantial amount of research on the topic of security awareness, where phishing attacks come first with 75% and ransomware second with 60%. It means that there is a significant disconnect between theory and practice on the ground, and that it is therefore a pressing requirement to go beyond the conventional training paradigm to an integrated form that integrates practical simulation with continuous assessment [37], [38], [39].

The basic conflict arises between strict security demands and the main principles of the university ethos of openness and sharing of knowledge. These peculiarities of educational space, such as open networks, Bring Your Own Device (BYOD) culture, and high reliance on third-party services, complicate the implementation of the traditional security models and precondition the growth of the scale of attacks significantly. It is within such a complicated context that the findings reveal that effective challenge has to be multi-faceted. Technical solutions are not independent but must be closely linked with sustainable, measurable awareness programs; well-defined governance frameworks with set roles and responsibilities; and institutional liaisons to share intelligence on the unfolding threats [40], [41].

The structural problems also present a complex dimension because most of the institutions are grappling with the challenge of fragmented technical infrastructure, dependence on third parties to deliver certain services, and the long-term unavailability of financial resources that are directed towards dealing with the crisis instead of being proactive in its prevention [42]. Combining these factors, it is possible to state that the development of the educational environment is not the technical task but the whole strategic change. It entails a narrow line balance between the protection of the digital assets and the maintenance of the important academic values and the creation of agile frameworks that have in place the ability to respond to the needs of the specifics of higher education and resource constraints [43], [44], [45].

VI. Conclusions and Future Research Directions

This review contributes to the literature by providing an updated synthesis of cybersecurity threats in higher education and highlighting the persistent gap between advanced detection technologies and their real-world adoption. It demonstrated that in universities, cybersecurity is now more complicated than solely a technical issue; it is strongly influenced by factors such as human behavior and the inherently open and distributed structure of higher education systems.

The impacts of the cybersecurity threats in higher education are shown to be substantial and multidimensional, with financial losses, disruption of educational operations, data breaches, and reputational damage posing serious risks to institutional stability and trust.

The findings offer practical guidance for university administrators and policymakers seeking to design resilient cybersecurity frameworks. Where a three-dimensional security approach is required: first, to implement intelligent systems that enable academic freedom and at the same time to ensure safety; second, to create awareness programs that follow realistic scenarios and assessments to establish safe behavior habits; third, to enhance institutional leadership and cooperation to establish sustainable and progressive defenses. The future of cybersecurity in higher education relies on the capacity of the institutions to bring a cultural shift towards security being a social good and resilience being the necessary element of their digital identity.

Authors' Contributions

Conceptualization, H.M.B.; Methodology, M.F.A. and H.M.B.; Validation, H.M.B; Writing Original Draft Preparation, H.M.B.; Writing Review & Editing, M.F.A; Supervision, M.F.A.

Conflict of Interest

The authors declare that there is no conflict of interest.

REFERENCES

[1] Najiyah, N. L. N. N., & Putriani, R. (2024). Transformation of Hadith Study in the Digital Era: an Effectiveness of Hadith Applications and Websites. Mashdar: Jurnal Studi Al-Qur'an Dan Hadis, 6(1), 27–42. https://doi.org/10.15548/mashdar.v6i1.7882

[2] FED. (2023). FEDERAL BUREAU OF INVESTIGATION. www.ic3.gov

[3] Data-Breach. (2021). ITRC-2021-Data-Breach-Report.

[4] Alnajim, A. M., Habib, S., Islam, M., Albelaihi, R., & Alabdulatif, A. (2023). Mitigating the Risks of

Malware Attacks with Deep Learning Techniques. Electronics (Switzerland), 12(14). https://doi.org/10.3390/electronics12143166

[5] Sharma, S. ,Upreti. (2021). A Comparative analysis of security issues & vulnerabilities of leading Cloud Service Providers and in-house University Cloud platform for hosting E-Educational applications. IEEE.

[6] Mr. Vishal Borate, Dr. Alpana Adsul, Mr. Rohit Dhakane, Mr. Shahuraj Gawade, Ms. Shubhangi Ghodake, & Mr. Pranit Jadhav. (2024). A Comprehensive Review of Phishing Attack Detection Using Machine Learning Techniques. International Journal of Advanced Research in Science, Communication and Technology, 435–441. https://doi.org/10.48175/ijarsct-19963

[7] Alotibi, G. (2024). A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks. Engineering, Technology and Applied Science Research, 14(2), 13787–13795. https://doi.org/10.48084/etasr.7123

[8] Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. In Symmetry (Vol. 15, Issue 12). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/sym15122175

[9] Ponnusamy, S. ,Rafique. (2020). Cybersecurity-Governance-on-Social-Engineering-Awareness.

[10] Sandjojo, N., Zuhriyanto, M., & Pradnyana, I. W. W. (2020). The Effects of Fear of Cybercrime and Information Systems Security Policy on National Vigilance. Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020, 195–200. https://doi.org/10.1109/ICIMCIS51567.2020.9354283

[11] Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information (Switzerland), 13(4). https://doi.org/10.3390/info13040192

[12] Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

[13] Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. In Future Internet (Vol. 13, Issue 2, pp. 1–40). MDPI AG. https://doi.org/10.3390/fi13020039

[14] Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., & Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey. Computers in Human Behavior Reports, 16. https://doi.org/10.1016/j.chbr.2024.100501

[15] Priya Karthikeyan, S. (2024). CYBERSECURITY IN EDUCATION: SAFEGUARDING DIGITAL LEARNING ENVIRONMENTS. International Journal of Engineering and Technology Research (IJETR), 9(2), 43–53. https://doi.org/10.5281/zenodo.13645990

[16] Arina, A., & Anatolie, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. www.ijstr.org

[17] Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences (Switzerland), 12(5). https://doi.org/10.3390/app12052589

[18] Hamdaoui Hamza, E. (2023). CYBERSECURITY IN HIGHER EDUCATION: CHALLENGES AND PREVENTION STRATEGIES CYBERSECURITY IN HIGHER EDUCATION: CHALLENGES AND PREVENTION STRATEGIES. International Journal of Marketing and Strategic Management, 5. https://doi.org/10.34874/PRSM.rimms-vol5iss2.46283

[19] Nadry, Z., Hakimi, M., Sirat, A. W., & Popal, Z. (2025a). Strengthening Cybersecurity Awareness Through Education: The Expanding Role of Cyber Law in Academic Institutions. Jurnal Analisis Hukum, 8(2), 193–209. https://doi.org/10.38043/jah.v8i2.7086

[20] Sepillo, H. D., Arcibal, G. M. P., Batan, B. J. B., Castronuevo, G. B., Estillore, J. V., & Mag-isa, J. C. (2025). Phishing Attack Detection and Prevention in Educational Institutions Using Machine Learning: A Quantitative Experimental Design with Embedded Impact Analysis on Cybersecurity. Cognizance Journal of Multidisciplinary Studies, 5(10), 403–410. https://doi.org/10.47760/cognizance.2025.v05i10.037

[21] Angelova, E. (2024). Cybersecurity in Higher Education: Challenges and Measures for Information Storage. Bulgarian Journal of International Economics and Politics, 4(2), 110–126. https://doi.org/10.37075/bjiep.2024.2.07

[22] Ogochukwu et al. (2024). Awareness of Phishing Attacks in Institutions of Higher Learning A Review of Types and Technical Approaches.

[23] Jawaid, S. A. (2022). Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity. https://doi.org/10.20944/preprints202211.0128.v1

[24] Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). NIPES - Journal of Science and Technology Research, 6(2), 293–311. https://doi.org/10.5281/zenodo.12617068

[25] Yousif Yaseen, K. A. (2022b). Importance of Cybersecurity in The Higher Education Sector 2022. Asian Journal of Computer Science and Technology, 11(2), 20–24. https://doi.org/10.51983/ajcst-2022.11.2.3448

[26] Igbokwe, I. C. (2024). Cyber Security in the Era of Digitalization: Implications for Educational Management. In Unizik Journal of Educational Management and Policy (UJOEMP) (Vol. 6, Issue 2).
[27] Yousif Yaseen, K. A. (2022a). Digital Education: The Cybersecurity Challenges in the Online Classroom (2019-2020). Asian Journal of Computer Science and Technology, 11(2), 33–38. https://doi.org/10.51983/ajcst-2022.11.2.3450
[28] Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. Journal of Big Data, 11(1). https://doi.org/10.1186/s40537-024-0098z
[29] Triplett, W. J. (2023). Addressing Cybersecurity Challenges in Education. International Journal of STEM Education for Sustainability, 3(1), 47–67. https://doi.org/10.52889/ijses.v3i1.132
[30] Vanhoy, J. (2023). A Qualitative Study in Efficacy of Cybersecurity Educational Avenues. https://ssrn.com/abstract=4673616
[31] Wada et al. (2025). AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. World Journal of Advanced Research and Reviews, 25(3). https://doi.org/10.30574/wjarr.2025.25.3.0989
[32] Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. In Symmetry (Vol. 15, Issue 12). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/sym15122175
[33] Singh Lallie, H., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. https://doi.org/10.3390/computers
[34] Sadiqzade, Z., & Alisoy, H. (2025). Cybersecurity and Online Education – Risks and Solutions. Luminis Applied Science and Engineering, 2(1), 4–12. https://doi.org/10.69760/lumin.20250001001
[35] Sreekandan Nair, S. (2023). Ransomware Attacks On Educational Institutions: Recent Trends And Mitigation Strategies. Article in International Research Journal of Modernization in Engineering Technology and Science, 3492. https://doi.org/10.56726/IRJMETS43540
[36] Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). Understanding Cyber Threats Against the Universities, Colleges, and Schools. https://doi.org/10.3390/computers14020049
[37] Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. Computers in Human Behavior, 158. https://doi.org/10.1016/j.chb.2024.108274
[38] Nyasvisvo, B., & Chigada, J. M. (2023). Phishing Attacks: A Security Challenge for University Students Studying Remotely. In The African Journal of Information Systems (Vol. 15, Issue 2).
[39] Armas, R., & Taherdoost, H. (2025). Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm. Information (Switzerland), 16(5). https://doi.org/10.3390/info16050336
[40] Alia, A. (2023). Effect of Cybersecurity Awareness among Students in the Education Framework Using the Internet, E-Learning Platforms and Social Networks. In International Journal of Computer and Information Technology (Vol. 12). www.ijcit.com
[41] Hong, W. C. H., Chi, C. Y., Liu, J., Zhang, Y. F., Lei, V. N. L., & Xu, X. S. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Education and Information Technologies, 28(1), 439–470. https://doi.org/10.1007/s10639-022-11121-5
[42] Shamala, P., Chinniah, M., Binti Ahmad, S. N., Kerk, L. C., & Mohd Rick, A. M. (2025). Cyber Security Awareness on Social Media: Knowledge Sharing Among Orang Asli Students. Journal of Computing Research and Innovation, 10(1), 52–63. https://doi.org/10.24191/jcrinn.v10i1.495
[43] Alsaadat, K. (2025). Cyber Security In Education. In American Journal of Science and Advanced Technology (AJSAAT) (Vol. 7, Issue 1).
[44] Nadry, Z., Hakimi, M., Sirat, A. W., & Popal, Z. (2025b). Strengthening Cybersecurity Awareness Through Education: The Expanding Role of Cyber Law in Academic Institutions. Jurnal Analisis Hukum, 8(2), 193–209. https://doi.org/10.38043/jah.v8i2.7086
[45] Oktavianto, R., Blasius, ·, & Sibarani, E. (2025). Building Cyber-savvy Generation: 15 Years of Research on Cybersecurity Education and Future Research Agendas.