International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

Artificial Intelligence in Ethical Hacking for Cybersecurity Ethics Awareness among Students

Dwiky Dimas Prihartomo[1], Bisyron Wahyudi[2]

[1] Cyber Defense Engineering, Faculty of Defense Engineering and Technology, Indonesian Defense University, Bogor, Indonesia

[2] Lecturer in Cyber Defense Engineering, Faculty of Defense Engineering and Technology, Indonesian Defense University, Bogor, Indonesia

Corresponding Author: dwikydimasp@gmail.com

Abstract

Artificial intelligence (AI) expands opportunities for cybersecurity education while increasing the risk that students may misuse technical capabilities. This study examined AI-assisted ethical hacking as a means of fostering cybersecurity ethics awareness and identified its benefits, risks, research gaps, and implementation principles. A Systematic Literature Review followed PRISMA stages and reviewed 30 journal articles published during 2016–2026 from Scopus, IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and accredited Indonesian journals. Data were analyzed through extraction and thematic synthesis. The findings showed that cyber ranges, capture-the-flag activities, serious games, and ethical hacking laboratories improved engagement and technical understanding, although knowledge did not always produce safe and ethical behavior. AI could serve as an adaptive tutor, scenario generator, feedback provider, and incident-explanation tool. Major risks included dual use, hallucinations, data leakage, bias, dependency, and academic integrity violations. Implementation should use an AI–Ethical Hacking Learning Cycle combining authorization, isolated environments, guardrails, ethical reflection, knowledge–attitude–behavior assessment, transparency, and meaningful human oversight.

Keywords: Artificial intelligence, ethical hacking, cybersecurity ethics, cyber awareness, students.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

INTRODUCTION

Digital transformation has led school and university students to interact intensively with online services, social media, mobile devices, learning platforms, and generative AI. This exposure expands learning opportunities while also increasing the risks of phishing, credential theft, cyberbullying, data leakage, social engineering, malware, and the use of technology without an adequate understanding of its legal and ethical consequences. Research on information security awareness indicates that knowledge, attitudes, and behavior are interrelated but distinct dimensions; individuals may know the correct practices yet continue to engage in risky actions because of habits, impulsivity, social norms, or the perception that threats are irrelevant to them (Hadlington, 2017; McCormac et al., 2017; Parsons et al., 2017; Zwilling et al., 2022).

Ethical hacking refers to the lawful, authorized, and scope-limited use of security testing techniques to identify and remediate vulnerabilities. Its distinction from illegal hacking lies not merely in the techniques used, but also in authorization, purpose, system boundaries, data protection, documentation, and responsible disclosure. Accordingly, ethical hacking education should not be limited to teaching scanning, exploitation, or vulnerability analysis; it must also instill the principles of consent, harm minimization, accountability, privacy, responsible reporting, and respect for system owners' rights.

Practice-oriented approaches such as cyber ranges, capture-the-flag (CTF) exercises, serious games, and simulation laboratories help learners understand attacks and defenses through direct experience. The literature indicates that game- and scenario-based learning can improve engagement, motivation, and skill acquisition; however, many evaluations still focus on perceptions or short-term technical scores rather than changes in secure behavior and ethical reasoning (Katsantonis et al., 2021; Khan et al., 2022; Pahlavanpour & Gao, 2024; Weeratunge et al., 2026). A resulting risk is the development of a "skills-first" orientation: learners may become capable of conducting attacks without being able to determine when an action is permissible, what data must be protected, or when an experiment should be stopped because it may harm others.

AI can strengthen such learning through adaptive tutoring, question and scenario generation, difficulty classification, log interpretation, adversarial simulation, and automated feedback. In education more broadly, AI enables personalization and rapid learning support, but also raises concerns regarding fairness, accountability, transparency, ethics, privacy, dependency, and academic integrity (Zawacki-Richter et al., 2019; Laupichler et al., 2022; Chiu et al., 2023; Memarian & Doleck, 2023). In cybersecurity, the dual-use nature of AI is particularly

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

pronounced because outputs that support defense may also be used to construct attacks, automate social engineering, or generate malicious code. The use of AI in ethical hacking education must therefore be guided by technical and pedagogical guardrails, instructor involvement, and explicit ethical assessment.

Based on these issues, this paper addresses four questions: (RQ1) how is ethical hacking used to foster cybersecurity ethics awareness among school and university students; (RQ2) which roles of AI have the greatest potential in this process; (RQ3) which ethical and security risks must be controlled; and (RQ4) which design principles are required for safe, ethical, and measurable implementation? The purpose of this SLR is to synthesize findings across cybersecurity education, AI in education, AI ethics, and human factors in order to develop an implementation framework relevant to schools and higher education institutions.

METHOD

SLR Design and Literature Sources

This study employed a Systematic Literature Review approach using the PRISMA stages of identification, screening, eligibility, and inclusion. Searches were conducted in Scopus, IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and nationally accredited SINTA journals to strengthen the Indonesian context. The publication period was set from January 2016 to July 2026. Mendeley or Zotero was used to import metadata, remove duplicates, organize the reference library, and generate citations in APA 7th edition style.

Search Strategy

The search combined four groups of concepts: AI, ethical hacking/cybersecurity practice, awareness or ethics, and educational populations. An example of the general search string is:

("artificial intelligence" OR "generative AI" OR "machine learning" OR "large language model" OR "AI tutor") AND ("ethical hacking" OR "penetration testing" OR "capture the flag" OR "cyber range" OR "serious game") AND ("cybersecurity awareness" OR "cyber ethics" OR "digital ethics" OR "responsible use") AND (student* OR learner* OR school OR university OR college)

The string was adapted to the syntax of each database. Additional searches were conducted through backward and forward citation tracking of key articles. The use of SciSpace, Elicit, or Consensus was limited to supporting semantic discovery, question mapping, and preliminary summary checks; all articles still had to be verified on the publisher's website or in a bibliographic index, and inclusion decisions were not delegated to AI.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

Inclusion and Exclusion Criteria

Table 1. Literature Inclusion and Exclusion Criteria

~~Aspect~~	Inclusion	Exclusion
Year and document type	Peer-reviewed journal articles published during 2016–2026	Outside the specified period; editorials, blogs, news items, theses, or conference proceedings when the corpus is restricted to journal articles
Topic	Addresses AI, ethical hacking/cybersecurity practice, security awareness, ethics, or education involving school or university students	Focuses solely on technical detection without a connection to education, awareness, behavior, or ethics
Population/context	School students, university students, educators, or educational program designs applicable to these groups	Organizational contexts with no educational implications and no transferable relevance
Access and quality	The abstract and the methods/findings can be assessed; source is indexed or accredited	Unclear metadata, duplicates, retracted articles, or inadequate methodological quality

Screening, Quality Appraisal, and Data Extraction

Screening was conducted sequentially at the title, abstract, and full-text stages. Each article was assessed for clarity of purpose, appropriateness of design, transparency of the sample and context, instrument validity, adequacy of analysis, relevance to the research questions, and disclosure of ethical considerations. Extracted data included article identity, country and educational level, research design, type of ethical hacking activity, AI function, awareness variables, findings, limitations, and recommendations.

Role of Supporting Tools and Qualitative Analysis

MaxQDA, NVivo, or ATLAS.ti was used after articles had passed full-text screening, specifically during data extraction and thematic synthesis. Article PDFs were imported, relevant

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

excerpts were coded, analytical memos were written, and the codes were subsequently grouped into categories and themes. These applications are not database search engines and do not replace the researcher's scholarly judgment. SciSpace, Elicit, and Consensus are more appropriately positioned in literature discovery and preliminary extraction, whereas Mendeley/Zotero is used for reference management.

Table 2. Position and Function of Supporting Tools in the SLR

Tool	Stage of use	Appropriate function
Scopus/IEEE/Springer/Science Direct/ACM	Literature identification	Structured searching, filtering by year, document type, and field, and exporting metadata.
Mendeley/Zotero	Reference management	Importing RIS/BibTeX/CSV files, deduplication, corpus folders, annotation, and APA citation management.
SciSpace/Elicit/Consensus	AI-assisted discovery and extraction	Identifying related terms, summarizing claims, extracting study elements, and tracing supporting articles; all outputs must be verified.
MaxQDA/NVivo/ATLAS.ti	Data analysis/thematic synthesis	Full-text coding, memo writing, article–code matrices, frequency/co-occurrence analysis, case comparison, and theme development.
VOSviewer/Bibliometrix (optional)	Bibliometric analysis	Mapping co-words, co-authorship, citations, and trends; it does not replace qualitative synthesis.

The initial codebook included authorization_scope, legal_ethics, privacy_data, responsible_disclosure, AI_as_tutor, AI_scenario_generation, adaptive_feedback, CTF_cyber_range, dual_use_misuse, hallucination_accuracy, bias_explainability, academic_integrity, knowledge_attitude_behavior, and assessment_retention. Coding was

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

conducted deductively on the basis of the research questions and was then expanded inductively when new themes emerged. Coding consistency was re-examined by reviewing the relevant excerpts and analytical memos.

PRISMA Flow and Data Transparency

A total of 30 journal articles met the criteria and were included in the final synthesis. Metadata, inclusion and exclusion decisions, and reasons for exclusion at the full-text stage were recorded in a PRISMA worksheet to maintain traceability and enable the review process to be audited.

RESULTS AND DISCUSSION

Profile and Direction of the Literature

The 30 core articles revealed four major research clusters. First, studies on human factors and cybersecurity awareness examined relationships among knowledge, attitudes, individual characteristics, and security behavior. Second, studies on game-based learning, cyber ranges, and serious games evaluated practice-oriented learning. Third, research on AI in education addressed personalization, AI literacy, intelligent tutoring, and academic integrity. Fourth, studies on AI ethics and AI for cybersecurity examined accountability, transparency, explainability, dual use, and implementation risks. Integration across these four clusters remains limited, as most articles investigate only one dimension in isolation.

Awareness Is Not Equivalent to Knowledge

A consistent finding is that cybersecurity awareness is multidimensional. HAIS-Q, knowledge–attitude–behavior studies, and reviews of awareness scales demonstrate the need to distinguish between what individuals know, what they believe, and what they actually do (Parsons et al., 2017; Alzubaidi, 2021; Zwilling et al., 2022; Rohan et al., 2023). Knowledge of passwords or phishing may improve after training, yet behavior may revert to previous patterns when participants face time pressure, convenience, peer influence, or low perceived risk. Therefore, evaluation of AI–ethical hacking programs should not rely solely on knowledge pre-tests and post-tests.

For school and university students, stronger indicators include the ability to request authorization before testing, comply with the defined scope, select non-sensitive test data, stop activities when risks arise, document evidence without exposing data, report vulnerabilities responsibly, and reject AI instructions that violate ethical principles. Assessment should include

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

observation of actions in scenarios, reflection on ethical reasoning, and retention measured several weeks or months after the intervention.

Ethical Hacking as Experiential Learning

Cyber ranges, CTF exercises, serious games, and isolated laboratories provide opportunities to conduct reconnaissance, log analysis, limited exploitation, hardening, and incident response without targeting real systems. This approach supports experiential learning because participants move through a cycle of action, feedback, reflection on mistakes, and experimentation with new strategies. The COFELET framework and game-based platforms highlight the importance of aligning learning objectives, activities, challenges, narratives, artifacts, feedback, and evaluation (Katsantonis et al., 2021; Khan et al., 2022).

However, game designs that reward only the speed of capturing a flag may encourage a win-oriented mindset while neglecting ethics. Technical scores should therefore be balanced with compliance scores that assess authorization validation, selection of minimum-impact methods, evidence protection, documentation, communication, and responsible disclosure. Mandatory debriefing should follow each exercise so that learners explain not only "how the attack succeeded," but also "why the action was justified in the laboratory and must not be transferred to a real system." Recent reviews likewise emphasize the need to standardize learning outcomes and strengthen evaluation in game-based cybersecurity awareness education (Pahlavanpour & Gao, 2024; Weeratunge et al., 2026).

Potential Roles of AI

The literature supports four principal roles for AI. First, AI can function as an adaptive tutor that adjusts the complexity of the material, provides progressive hints, and identifies misconceptions. Second, AI can serve as a scenario generator by producing variations of phishing attempts, vulnerable configurations, incident logs, or ethical dilemmas appropriate to the learner's level. Third, AI can provide feedback by explaining why a command is risky, connecting actions to legal and ethical principles, and asking learners to improve their reasoning. Fourth, AI can support reflection by comparing learners' choices with safer and more responsible alternatives.

These possibilities are consistent with the AI literacy and AI ethics education literature, which emphasizes understanding AI capabilities, limitations, and social impacts, as well as the ability to critically evaluate AI outputs (Laupichler et al., 2022; Kajiwara & Kawabata, 2024; Wiese et al., 2025; Kong & Zhu, 2025). In cybersecurity, explainable AI is important because

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

recommendations that cannot be explained may encourage blind compliance. Learners should be able to examine the evidence base, confidence level, assumptions, and limitations of AI recommendations rather than merely accepting a final answer (Zeadally et al., 2020; Capuano et al., 2022; Naik et al., 2022).

Ethical and Security Risks

The most prominent risk is dual use. AI models can accelerate the development of payloads, phishing content, enumeration, obfuscation, or exploits; therefore, learning environments must restrict prompts, tool access, connectivity, and data. The second risk is hallucination: AI may provide incorrect, dangerous, or version-incompatible instructions. The third risk concerns privacy, particularly when learners submit logs, credentials, configurations, source code, or personal data to external services. Other risks include assessment bias, unclear scoring rationales, dependency, deskilling, plagiarism, and the use of AI to complete assignments without understanding the underlying process.

Global AI ethics guidelines generally converge on transparency, fairness, non-maleficence, responsibility, privacy, and human control, although implementation varies across contexts (Jobin et al., 2019). In higher education, FATE principles and AI-use policies need to be translated into operational rules: which data may be entered, when AI may be used, how its use must be disclosed, how outputs are verified, who is accountable, and how learners can challenge automated assessments (Memarian & Doleck, 2023; Chan, 2023). Adopting AI because of hype without conducting a risk assessment may also weaken security and accountability (Humphreys et al., 2024; Hagendorff, 2024).

AI–Ethical Hacking Learning Cycle Framework

Based on the synthesis, this paper proposes an AI–Ethical Hacking Learning Cycle (AI-EHLC) comprising five layers. The first layer is an authorization and ethics contract, in which objectives, scope, prohibitions, data, duration, and disclosure rules are agreed upon before practice begins. The second layer is an isolated cyber range with synthetic targets, temporary accounts, snapshots, logging, network restrictions, and a kill switch. The third layer is a guardrailed AI tutor with role-based access, prompt and output filtering, retrieval from verified learning materials, audit logs, and escalation to an instructor. The fourth layer is execute–explain–reflect: learners perform tasks, explain their technical and ethical reasoning, receive feedback, and revise their actions. The fifth layer is multidimensional assessment covering knowledge, attitudes, behavior, technical skills, scope compliance, documentation quality, and

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

retention.

This framework positions AI as scaffolding rather than as a substitute for instructors or accountable decision-makers. For beginners, AI provides conceptual guidance and warns about ethical boundaries. For advanced learners, AI can present ambiguous scenarios that test decision-making, such as discovering a vulnerability outside the authorized scope or encountering logs that contain personal data. The highest score should not be awarded to the fastest exploitation, but to a solution that is safe, explainable, well documented, and consistent with authorization.

Research Trends and Gaps

Table 3. Trends, Research Gaps, and Future Directions

Finding/trend	Research gap	Future research direction
Games, CTFs, and cyber ranges increase engagement	Evaluations are often based on perceptions and short-term scores	Controlled experiments, behavioral tasks, and retention measurement.
AI provides personalization and rapid feedback	Few studies compare AI-assisted learning with conventional instruction	Quasi-experimental or randomized controlled trials with comparison groups.
AI ethics is widely discussed at the level of principles	These principles have rarely been translated into operational rules for ethical hacking practice	Testing of guardrails, audit logs, escalation policies, and responsible disclosure procedures.
Awareness instruments are available	They do not specifically measure ethical decision-making during hacking activities	Development of AI–ethical hacking scales and rubrics covering knowledge, attitudes, and behavior.
The literature is dominated by higher education and developed-country contexts	Evidence concerning school students and the Indonesian context remains limited	Cross-level studies addressing Indonesian language, culture, gender, access, and the digital divide.

CONCLUSION

This SLR concludes that ethical hacking can serve as an effective means of developing

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

cybersecurity ethics awareness when it is conducted in an authorized, isolated, reflective, and measurable manner. Practical activities increase engagement and technical understanding, but they do not automatically produce secure behavior. AI strengthens the process through personalization, scenario generation, explanation, and feedback, while simultaneously increasing the risks of dual use, hallucination, privacy breaches, bias, dependency, and academic integrity violations.

Schools and higher education institutions are advised to: (1) integrate the principles of authorization, scope, harm minimization, privacy, documentation, and responsible disclosure into every exercise; (2) use cyber ranges with segmentation, snapshots, logging, and connectivity restrictions; (3) implement AI through a human-in-the-loop approach using verified knowledge sources, guardrails, audits, and escalation mechanisms; (4) assess knowledge, attitudes, behavior, skills, and retention rather than merely exploitation success; (5) establish transparent policies on AI use and academic integrity; and (6) train educators to evaluate AI outputs and facilitate ethical debriefing.

Future research should test the AI-EHLC through longitudinal experiments involving school and university students, compare AI-assisted learning with conventional methods, develop validated ethical hacking ethics instruments, and assess the effectiveness of guardrails in preventing the transfer of skills to real systems. In the Indonesian context, studies should consider digital literacy, variation in institutional facilities, learning culture, data protection regulations, and disparities in access across institutions.

REFERENCE

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437–443.

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. IEEE Access, 10, 93575–93600. https://doi.org/10.1109/ACCESS.2022.3204171

Chan, C. K. Y. (2023). A comprehensive AI policy education framework for university teaching and learning. International Journal of Educational Technology in Higher Education, 20, 38.

Chiu, T. K. F., Xia, Q., Zhou, X., Chai, C. S., & Cheng, M. (2023). Systematic literature review on opportunities, challenges, and future research recommendations of artificial intelligence

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

in education. Computers and Education: Artificial Intelligence, 4, 100118.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hagendorff, T. (2024). Mapping the ethics of generative AI: A comprehensive scoping review. Minds and Machines, 34, 39. https://doi.org/10.1007/s11023-024-09694-w

Humphreys, D., Koay, A., Desmond, D., & Mealy, E. (2024). AI hype as a cyber security risk: The moral responsibility of implementing generative AI in business. AI and Ethics, 4, 791–804. https://doi.org/10.1007/s43681-024-00443-4

Ismail, M., Kuppusamy, K. S., & Paiva, S. (2024). Cybersecurity activities for education and curriculum design: A survey. Computers in Human Behavior Reports, 16, 100501. https://doi.org/10.1016/j.chbr.2024.100501

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1, 389–399.

Kajiwara, T., & Kawabata, T. (2024). AI literacy education using an ethical chatbot. Computers and Education: Artificial Intelligence, 6, 100251. https://doi.org/10.1016/j.caeai.2024.100251

Kasneci, E., Sessler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., Gasser, U., Groh, G., Günnemann, S., Hüllermeier, E., Krusche, S., Kutyniok, G., Michaeli, T., Nerdel, C., Pfeffer, J., Poquet, O., Sailer, M., Schmidt, A., Seidel, T., Stadler, M., Weller, J., Kuhn, J., & Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. Learning and Individual Differences, 103, 102274.

Katsantonis, M. N., Mavridis, I., & Gritzalis, D. A. (2021). Design and evaluation of COFELET-based approaches for cyber security learning and training. Computers & Security, 105, 102263. https://doi.org/10.1016/j.cose.2021.102263

Khan, M. A., Merabet, A., Alkaabi, S., & El Sayed, H. (2022). Game-based learning platform to enhance cybersecurity education. Education and Information Technologies, 27(4), 5153–5177. https://doi.org/10.1007/s10639-021-10807-6

Kong, S. C., & Zhu, H. (2025). Developing and validating an artificial intelligence ethical awareness scale for secondary and university students. Computers and Education: Artificial Intelligence, 9, 100447.

Laupichler, M. C., Aster, A., Schirch, J., & Raupach, T. (2022). Artificial intelligence literacy in higher and adult education: A scoping literature review. Computers and Education: Artificial Intelligence, 3, 100101.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behavior, 69, 151–156.

Memarian, B., & Doleck, T. (2023). Fairness, accountability, transparency, and ethics (FATE) in artificial intelligence and higher education: A systematic review. Computers and Education: Artificial Intelligence, 5, 100152. https://doi.org/10.1016/j.caeai.2023.100152

Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. Complex & Intelligent Systems, 8, 1763–1780. https://doi.org/10.1007/s40747-021-00494-8

Pahlavanpour, M. M., & Gao, S. (2024). A systematic mapping study on gamification in information security awareness programs. Heliyon, 10(19), e38474. https://doi.org/10.1016/j.heliyon.2024.e38474

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Quayyum, A., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, 100343.

Rohan, R., Pal, D., & Funilkul, S. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9(3), e14234. https://doi.org/10.1016/j.heliyon.2023.e14234

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

Tlili, A., Shehata, B., Adarkwah, M. A., Bozkurt, A., Hickey, D. T., Huang, R., & Agyemang, B. (2023). What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education. Smart Learning Environments, 10, 15.

Weeratunge, N. H., Hjelsvold, R., & Katt, B. (2026). A systematic scoping review on game-based cybersecurity awareness education. International Journal of Information Security, 25, Article 71. https://doi.org/10.1007/s10207-026-01239-9

Wiese, L. J., Patil, I., Schiff, D. S., & Magana, A. J. (2025). AI ethics education: A systematic literature review. Computers and Education: Artificial Intelligence, 8, 100405.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

https://doi.org/10.1016/j.caeai.2025.100405

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education—Where are the educators? International Journal of Educational Technology in Higher Education, 16, 39.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access, 8, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.