SEMARAK ILMU PUBLISHING

Semarak International Journal of Machine Learning

Journal homepage:
https://semarakilmu.my/index.php/sijml/index
ISSN: 3030-5241

Enhancing Cybersecurity Competence through Experiential Lab-Based Learning: A Post-Survey Evaluation of the Cybersecurity Fundamentals Course in Malaysian TVET

Siti Sharmila Osmin[1,*], Tasneem Darwish[2], Mazidah Mukri[3]

[1] Department Information Technology, Pasir Salak Community College, Lebuh Paduka, Changkat Lada, 36800 Kampung Gajah, Perak, Malaysia
[2] Department of Computer Science, St. Francis Xavier University, 4130 University Ave, Antigonish, NS B2G 2W5, Canada
[3] Faculty of Civil Engineering, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 24 December 2025
Received in revised form 19 February 2026
Accepted 10 March 2026
Available online 31 March 2026

Keywords:
Experiential learning; cybersecurity competence; TVET; digital ethics, workforce readiness; lab-based pedagogy

ABSTRACT

The rapid escalation of cyber threats has intensified the global demand for professionals who are not only technically competent but also ethically grounded. Addressing this need, the Cybersecurity Fundamentals course at Kolej Komuniti Pasir Salak, Malaysia, was designed as a fully lab-based experiential learning model emphasizing authentic, hands-on engagement with industry-standard tools. This study evaluates the effectiveness of that model in developing technical proficiency, ethical awareness, and learner engagement among Certificate in Information Technology students. A post-course quantitative survey involving 19 participants from the first cohort was conducted using a validated 4-point Likert-scale instrument covering engagement, tool mastery, and ethical understanding. Results indicated high overall satisfaction (mean = 3.28/4), with students reporting notable gains in applied competence and critical awareness of digital ethics. Qualitative responses further revealed that experiential learning improved confidence, problem-solving ability, and appreciation of real-world cybersecurity challenges. These findings provide empirical evidence that structured, lab-centered pedagogy significantly enhances the learning experience and workforce readiness of TVET students. The study contributes to the growing discourse on experiential cybersecurity education by offering a replicable model for skill-based learning that aligns with Malaysia's Digital Economy Blueprint and global Industry 4.0 transformation goals.

1. Introduction

Cybersecurity has emerged as one of the most critical disciplines in the global digital economy. With the increasing interconnectivity of systems and the widespread adoption of cloud computing, mobile technology, and the Internet of Things (IoT), organizations are facing an unprecedented volume and complexity of cyber threats. The rapid evolution of malware, phishing, data breaches, and ransomware attacks has created an urgent demand for a workforce capable of protecting digital assets while upholding ethical and legal standards.

* *Corresponding author.*
E-mail address: sitisharmila@kkpsa.edu.my

Malaysia, like many other nations, recognizes that cybersecurity readiness is central to sustaining its digital transformation agenda under the Malaysia Digital Economy Blueprint [1] and National Cybersecurity Strategy 2020–2024 [2]. These frameworks emphasize the need for a digitally skilled and ethically responsible workforce, which can only be achieved through education models that go beyond theoretical teaching. Within the national Technical and Vocational Education and Training (TVET) ecosystem, the Department of Polytechnic and Community College Education (JPPKK) has prioritized competency-based and experiential learning approaches to produce job-ready graduates capable of meeting industry expectations.

The Cybersecurity Fundamentals course at Kolej Komuniti Pasir Salak embodies this vision through a fully experiential and lab-based pedagogy. Instead of relying on traditional classroom instruction, the course immerses students in authentic, scenario-driven activities where they actively engage with professional cybersecurity tools and real-world challenges. Each lab session is designed to simulate practical contexts that mirror industry tasks from identifying password vulnerabilities to analyzing digital evidence allowing learners to translate knowledge into demonstrable skill.

The course integrates 21 structured lab activities based on the official syllabus for Cybersecurity Fundamentals (SFC31663), combining technical operations, analytical reasoning, and ethical awareness. Tools such as Wireshark, Nmap, OWASP ZAP, Autopsy, VeraCrypt, and Autopsy are used to replicate authentic cybersecurity workflows. For instance, in Lab 6: Wireshark Packet Capture, students observe network traffic to identify plaintext credentials ethically, while in Lab 21: Autopsy Forensics, they conduct data recovery and evidence analysis. This systematic, tool-oriented design ensures that students not only learn to perform technical tasks but also develop a sense of ethical responsibility in handling sensitive information.

Experiential learning in cybersecurity aligns closely with Kolb's Experiential Learning Theory [3], which emphasizes the transformation of experience into knowledge through reflection and practice. When students perform, observe, and analyze tasks directly, they engage in higher-order cognitive processes that strengthen conceptual understanding and retention. Within this framework, cybersecurity labs act as catalysts for critical thinking, bridging the gap between abstract concepts such as "network defence" and tangible, real-world implementation.

Globally, research consistently demonstrates the benefits of simulation-driven pedagogy across various metrics. While Tsirulnikov *et al*., [4] emphasize that simulations primarily drive student performance and intrinsic motivation, Detyna *et al*., [5] offer a broader meta-analysis confirming these outcomes specifically within higher education laboratory settings. In contrast to these focus areas on academic performance, Hussain et al., [6] provide a longitudinal perspective, arguing that the primary contribution of lab-based learning is the long-term enhancement of student employability. By comparing these studies, it is evident that while Tsirulnikov *et al*., [4] and Detyna *et al*., [5] validate the classroom experience, Hussain *et al*., [6] bridges the gap toward professional readiness, a core goal of the TVET framework.

Despite the global success of experiential models, a significant research gap exists within the Malaysian TVET ecosystem; most existing literature focuses on university-level simulations, leaving a lack of empirical evidence regarding fully lab-based cybersecurity courses at the certificate level in community colleges. To address this, the primary objective of this study is to evaluate the impact of a structured 21-lab experiential framework on student engagement, technical proficiency, and ethical maturity. The significance of this research lies in providing the first documented evidence of such a model in a Malaysian community college, offering a replicable pedagogical blueprint that aligns with the Malaysia Digital Economy Blueprint to produce industry-ready graduates.

2. Literature Review

The importance of experiential learning in cybersecurity education has been widely documented. Traditional lecture-based methods often fail to prepare learners for the complexity and immediacy of cyber threats [7]. To address this gap, researchers have emphasized hands-on, problem-based, and simulation-driven approaches that promote applied understanding and adaptive expertise [8].

2.1 Experimental Learning Theory

Experiential Learning Theory (ELT) posits that knowledge is created through the transformation of experience involving concrete experience, reflective observation, abstract conceptualization, and active experimentation [3]. In cybersecurity education, this cycle enables students to observe, act, and reflect on security challenges, developing both cognitive and behavioural competence. Previous research Melnikovas and Melnikova [9] and Kebande [10] indicates that experiential cybersecurity labs demonstrate significant potential for enhancing learners' retention, engagement, and ethical decision-making compared to traditional educational approaches. They further assert that when students work with authentic tools in simulated environments, they demonstrate higher problem-solving ability and professional accountability.

2.2 Cybersecurity Competency and Ethics

Academic discourse Spurava and Kotilainen [11] emphasizes that ethical literacy is a critical dimension of digital professionalism, with multiple studies providing robust evidence of its importance. Integrating ethical reflection within lab-based environments ensures students understand the real-world consequences of security decisions, from data privacy to system defence. Emerging evidence suggests that ethics-infused cybersecurity curricula are critically important but currently underdeveloped in producing responsible digital practitioners. A global survey Weichert *et al*., [12] revealed that almost half of universities do not offer computing ethics courses, with only 33% requiring an ethics course for graduation. Existing literature Flechais *et al*., [13] further identifies significant ethical challenges across cybersecurity decision-making that requires balancing complex technical and subjective perspectives. Prior interventions Petelka *et al*., [14] demonstrate that integrated ethics training helps students recognize ethical intersections, though students still struggle to confidently navigate ethical dilemmas. Scholars Liao *et al*., [15] suggest that cybersecurity education must become a cross-disciplinary effort involving all stakeholders, not just technical professionals. The evidence indicates a pressing need for more robust, integrated ethical training in cybersecurity education.

2.3 TVET and Workforce Readiness

Within the Malaysian context, the Ministry of Higher Education and the Department of Polytechnic and Community College Education (JPPKK) emphasize experiential learning as a cornerstone of TVET transformation. Programs under this framework prioritize competency-based, hands-on training aligned to Malaysia Board of Technologists (MBOT) standards. As outlined in Malaysia's Digital Economy Blueprint [1] TVET institutions play a critical role in producing industry-ready digital professionals equipped with practical cybersecurity skills.

2.4 Research Gap

Although prior studies have explored experiential learning effectiveness globally, there is limited empirical evidence from Malaysia's community colleges implementing cybersecurity-specific experiential models. This study therefore contributes new insights by evaluating student outcomes from the Cybersecurity Fundamentals course the first fully lab-based cybersecurity module introduced in Kolej Komuniti Pasir Salak.

The primary objective of this study is to evaluate the effectiveness of experiential, lab-based learning in strengthening the cybersecurity competence of students enrolled in the Cybersecurity Fundamentals course at Kolej Komuniti Pasir Salak. Specifically, the research aims to explore how structured, hands-on laboratory activities enhance students' engagement, technical proficiency, and ethical decision-making within authentic cybersecurity contexts. By assessing students' self-reported perceptions and satisfaction levels through a validated post-course survey, the study seeks to determine the extent to which lab-based pedagogy promotes deeper understanding, applied problem-solving, and digital ethics awareness. Furthermore, this investigation intends to generate evidence-based insights that can inform continuous improvement of cybersecurity instruction within Malaysia's TVET framework and serve as a model for similar experiential initiatives in other institutions.

3. Methodology

3.1 Research Design

This study employed a quantitative descriptive research design complemented by reflective elements of action research. The descriptive approach was selected because it allows researchers to gather, analyze, and summarize participants' perceptions in a measurable form, providing a comprehensive understanding of how experiential, lab-based learning influences students' competence and engagement. Meanwhile, the reflective action-research aspect ensured that the findings would not only describe outcomes but also contribute to the continuous improvement of course delivery [15], while Alpert *et al*., [16] describes a doctoral program that uses action research methodology to progressively reinforce and extend research methods. Furthermore, student reflections [17] have been used to understand and enhance course experiences. The evidence suggests that reflective action-research is a robust, multi-step process that enables educators to continuously refine their teaching practices by systematically analyzing and responding to feedback and observed outcomes.

3.2 Participants

The study involved 16 students of Certificate in Information Technology from Kolej Komuniti Pasir Salak who enrolled in the Cybersecurity Fundamentals (SFC31663) course during Semester I of the 2025/2026 academic session. These participants represented the first cohort to undertake the newly developed, fully experiential version of the course. The group was diverse in terms of gender, prior computing experience, and familiarity with cybersecurity concepts, which provided a balanced view of how lab-based learning supports both novice and intermediate learners. Participation was voluntary, and all students provided informed consent before completing the survey. Confidentiality and ethical research principles were upheld throughout the study.

3.3 Instruments

A structured post-course survey instrument was designed and administered during Week 14, immediately after students had completed all 21 lab activities. The survey comprised six sections: demographic information, knowledge gain, engagement, technical skill development, ethical understanding, and overall satisfaction. A four-point Likert scale (1 = Strongly Disagree, 4 = Strongly Agree) was used to ensure participants provided decisive feedback, avoiding neutral responses. The instrument also included open-ended questions to capture students' personal reflections about their most meaningful lab experiences, perceived challenges, and recommendations for course enhancement. To ensure reliability and validity, the survey was reviewed by two cybersecurity educators and one curriculum specialist from another Malaysian community college. Their feedback helped refine question clarity, alignment with course learning outcomes (CLOs), and technical accuracy.

3.4 Learning Procedure and Implementation

The Cybersecurity Fundamentals course was delivered using a 21-lab experiential learning framework. Each lab was conducted in a controlled environment within the college's computer laboratory, where students engaged directly with cybersecurity tools such as Wireshark, Nmap, OWASP ZAP, VeraCrypt, Spyrix, and Autopsy. The lab activities were sequenced to build knowledge progressively:

i. Labs 1–4 (Foundation Level): Introduced students to core cybersecurity principles, password management, malware awareness, and secure online practices.
ii. Labs 5–14 (Application Level): Focused on technical execution, including network scanning, packet sniffing, and vulnerability testing using Wireshark and Nmap. Students performed real-time packet analysis and network mapping, gaining familiarity with legitimate scanning ethics.
iii. Labs 15–21 (Advanced Level): Emphasized digital forensics, encryption, and ethical system monitoring. For instance, in Lab 21: Local File Forensics using Autopsy, students practiced data recovery and evidence tracing, linking theoretical cybersecurity principles to professional forensic investigation scenarios.

Each session followed Kolb's experiential learning cycle beginning with concrete experience (performing tasks), reflective observation (analyzing results), abstract conceptualization (connecting to theory), and active experimentation (applying improvements). Students documented their findings in lab reports, reinforcing reflective thinking and communication skills.

3.5 Data Analysis

Collected data were analyzed using descriptive statistical techniques, including frequency distributions, percentage analysis, and mean score computation. These metrics provided insight into students' perceptions of engagement, technical proficiency, and ethical awareness. Quantitative data were complemented by qualitative findings derived from open-ended survey responses. The qualitative comments were coded thematically to identify recurring ideas and sentiments, such as motivation, self-efficacy, and challenges faced during lab implementation.

To strengthen analytical credibility, results were cross-validated with the course learning outcomes and MBOT competency descriptors. The use of both numerical and narrative data allowed

for a more holistic interpretation of how experiential learning impacted students' knowledge, skills, and values.

3.6 Research Validity and Ethical Considerations

To ensure methodological rigor, triangulation was achieved through multiple data sources quantitative ratings, qualitative feedback, and instructor reflections from the lab sessions. Expert review of the survey instrument and alignment to the course syllabus added construct validity. Ethical approval for data collection was obtained from the institution's research coordinator, ensuring that participation was voluntary and anonymous. No identifying information was recorded, and students were assured that their responses would not influence academic grading. The methodological framework thus ensured that the study not only met academic standards but also reflected authentic classroom practice, offering meaningful insights for future improvement of cybersecurity pedagogy within Malaysia's TVET institutions.

4. Result and Discussion

The post-course survey involving 16 students provided clear evidence of the effectiveness of the experiential, lab-based design of the Cybersecurity Fundamentals course. Analysis of the 26 Likert-scale items revealed consistently positive perceptions across all learning dimensions, with mean scores ranging from 3.12 to 3.50 on a 4-point scale. These results indicate that students not only benefited academically from the hands-on approach but also developed stronger technical confidence and ethical awareness. The descriptive findings across key learning categories and sample survey items are summarized in Table 1.

Table 1
Summary of students' perceptions of the cybersecurity fundamentals course

Category	Example Item	Mean Score
Engagement & Interactivity	"The lab activities made the class engaging."	3.37
Technical Skill Mastery	"I gained confidence using Wireshark and Nmap."	3.40
Ethical Awareness	"I learned to use cybersecurity tools responsibly."	3.19
Overall Satisfaction	"The course improved my understanding of cybersecurity."	3.31
Overall Mean		3.26

Note: n = 40; Scale 1 = Strongly Disagree to 4 = Strongly Agree

Based on the updated analysis of 16 student responses, the findings continue to demonstrate strong support for the experiential, lab-based learning model implemented in the Cybersecurity Fundamentals course. As illustrated in Figure 1, all 26 survey items recorded mean scores above 3, indicating positive perceptions across all learning dimensions. Technical Skill Mastery emerged as the strongest domain, with the highest-rated items including confidence using cybersecurity tools (M = 3.50), enjoyment of hands-on activities (M = 3.50), and increased understanding through practical tools (M = 3.38) reflecting students' enhanced competence in using Wireshark, Nmap, OWASP ZAP, and forensic analysis tools. Engagement and Interactivity also remained high, with mean scores ranging from 3.31 to 3.38, showing that the hands-on, scenario-driven activities substantially improved motivation, attention, and active participation. Ethical Awareness, while slightly lower than the other categories, still demonstrated solid positive perceptions (means between 3.12 and 3.25), suggesting that students gained a clearer understanding of responsible tool usage, legal considerations, and the implications of unethical hacking. Overall Satisfaction averaged 3.31,

confirming that students valued the course structure, sequencing of activities, and authenticity of the lab-based approach. Collectively, these findings reinforce that the experiential model significantly enhanced practical competence, engagement, and ethical understanding among TVET learners, thereby aligning well with industry expectations and Malaysia's broader digital workforce readiness goals.

4.1 Engagement and Interactivity

Items measuring engagement including enjoyment of the labs, perceived interactivity, and motivational aspects recorded mean scores between 3.31 and 3.38, demonstrating that students found the lab-based approach far more stimulating than traditional lecture-driven sessions. The highest rating in this dimension was reflected in the statement "I enjoyed learning cybersecurity concepts through hands-on labs" (M = 3.50), showing that active participation significantly enhanced learner motivation. These findings align with experiential learning principles, which emphasize that meaningful engagement occurs when learners interact directly with real-world tools and scenarios.

4.2 Technical Skill Mastery

Technical competence emerged as the strongest domain in the survey. Items related to the use of Wireshark, Nmap, OWASP ZAP, encryption tools, and forensic analysis tools consistently scored high, with means ranging from 3.38 to 3.50. The item "The tools provided helped me understand better" scored 3.38, while "I can confidently use Wireshark, Nmap, or OWASP ZAP" also recorded 3.38. These results confirm that the structured 21-lab sequence successfully enhanced students' technical confidence and operational proficiency. This is particularly significant for TVET learners, who benefit most from practice-oriented, skills-based learning environments that mirror workplace expectations.

4.3 Ethical Awareness and Responsible Tool Use

The dimension of ethical awareness produced mean scores between 3.12 and 3.25, reflecting solid but slightly lower ratings compared to engagement and technical mastery. Items measuring understanding of ethical hacking consequences, legal awareness, and responsible tool use still demonstrated positive perceptions for example, "I learned about real-world consequences of unethical hacking" (M = 3.19) and "I am more aware of laws and regulations related to cybersecurity" (M = 3.25). Although these scores indicate that ethical learning objectives were met, they also highlight an opportunity for enhancement possibly through more structured ethical case studies, simulated incident response dilemmas, or dedicated ethics discussions integrated into each lab.

4.4 Overall Satisfaction and Perceived Readiness

Overall satisfaction items recorded mean scores ranging from 3.25 to 3.38, indicating that students regarded the course design as effective, relevant, and impactful. They also reported feeling more prepared for cybersecurity-related tasks, with "I feel better prepared for cybersecurity jobs or internships" scoring 3.38. This supports the assertion that experiential, lab-based learning not only builds technical skills but also nurtures confidence and workplace readiness key priorities in Malaysia's TVET transformation agenda.

4.5 Overall Satisfaction and Perceived Readiness

In summary, the updated analysis confirms that the experiential learning model significantly enhanced students' engagement, practical competence, ethical understanding, and overall learning satisfaction. With all items scoring above 3.12, the results reinforce that hands-on cybersecurity labs are an effective pedagogical approach for developing job-ready graduates. The strong performance in technical skill mastery and engagement demonstrates that students gained meaningful real-world experience, while the positive ethical awareness scores highlight the importance of embedding responsible cybersecurity practices within practical learning activities.

4.6 Summary of Findings

The analysis of survey responses from 16 students revealed consistently positive perceptions toward the experiential, lab-based learning model implemented in the Cybersecurity Fundamentals course. All four learning dimensions recorded mean scores above 3.19 on a 4-point scale, indicating that students found the course highly effective in enhancing both their technical competence and learning experience. Engagement and Interactivity achieved the highest category mean (M = 3.38), showing that students strongly valued hands-on learning, interactive activities, and the authentic use of cybersecurity tools. This confirms that the lab-based approach successfully increased motivation, enjoyment, and active participation.

Technical Skill Mastery recorded a mean of 3.24, demonstrating that students gained confidence in using professional cybersecurity tools such as Wireshark, Nmap, and OWASP ZAP. They also reported improved ability to detect threats, apply security measures, and troubleshoot cybersecurity issues evidence that the 21 structured labs effectively strengthened practical, job-relevant skills. Ethical Awareness, with a mean of 3.19, indicates that students developed a solid understanding of responsible tool use, legal implications, and the consequences of unethical hacking. Although slightly lower than other domains, scores remain positive, highlighting the value of integrating ethical reflection within technical lab activities.

Overall Satisfaction achieved a mean score of 3.25, confirming that students were satisfied with the learning experience and felt better prepared for future cybersecurity roles. The majority indicated they would recommend the lab-based design to other learners. Overall, the findings affirm that experiential, tool-centric learning significantly enhances engagement, technical proficiency, ethical understanding, and perceived readiness among TVET learners. These results support the continued use and expansion of lab-based approaches in cybersecurity education to meet Malaysia's growing digital workforce needs.

5. Conclusion

This study evaluated the effectiveness of a fully experiential, lab-based learning model implemented in the Cybersecurity Fundamentals course at Kolej Komuniti Pasir Salak. The analysis of post-course survey data from 16 students demonstrated that the approach successfully enhanced learner engagement, technical proficiency, ethical awareness, and overall satisfaction. All four learning dimensions achieved mean scores above 3.19, indicating consistent positive perceptions across the cohort. The highest ratings were observed in Engagement and Interactivity (M = 3.38), confirming that hands-on labs significantly improved students' motivation and active participation. Technical Skill Mastery (M = 3.24) further highlighted the strong impact of tool-centric activities in developing students' confidence and competence in using cybersecurity tools such as Wireshark,

Nmap, and OWASP ZAP. Ethical Awareness (M = 3.19) showed that students gained a meaningful understanding of responsible cybersecurity practices, legal considerations, and the consequences of unethical behaviour. Overall Satisfaction (M = 3.25) demonstrated that students valued the structure, relevance, and real-world authenticity of the lab-based approach.

Collectively, the findings provide empirical evidence that experiential learning is a highly effective pedagogical model for cybersecurity education within the Malaysian TVET context. The structured sequence of 21 labs not only strengthened technical readiness but also fostered ethical decision-making both essential competencies for today's cybersecurity workforce. The outcomes of this study support the integration of practical, scenario-driven learning environments in future cybersecurity curricula and highlight the need for continued investment in lab-based teaching strategies to meet national digital transformation goals.

Acknowledgement
The authors would like to express their sincere gratitude to the management of Kolej Komuniti Pasir Salak for the continuous support, facilities, and resources provided throughout the development and implementation of the Cybersecurity Fundamentals course. Special appreciation is extended to the Information Technology Department lecturers and technical staff whose assistance in preparing, maintaining, and improving the laboratory environment made the 21 lab-based activities possible. The authors also wish to thank the students of the Certificate in Information Technology programme who participated in this study. Their honest feedback, cooperation, and engagement during the learning sessions contributed significantly to the findings and insights reported in this paper. Deepest appreciation is also conveyed to the curriculum reviewers and cybersecurity educators who provided expert input in validating the survey instrument and ensuring alignment with course learning outcomes and TVET standards. Their guidance greatly strengthened the methodological rigour of the study. Finally, sincere thanks are extended to all individuals who contributed directly or indirectly to this research. Their support, encouragement, and collaboration were invaluable in completing this study successfully.

References

[1] Economic Planning Unit. *Malaysia Digital Economy Blueprint*. Prime Minister's Department, 2021. https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf
[2] National Security Council. *Malaysia Cyber Security Strategy 2020–2024*. Prime Minister's Department, 2020. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf
[3] Kolb, David A. *Experiential Learning: Experience as the Source of Learning and Development*. Prentice-Hall, 1984.
[4] Tsirulnikov, E., A. Sidorova, and Y. Rykov. "The Impact of Simulation-Based Learning on Student Performance and Motivation: A Systematic Review." *Journal of Computer Assisted Learning* 39, no. 4 (2023): 1105–1121. https://doi.org/10.1111/jcal.12792
[5] Detyna, M., E. J. Dommett, and K. J. Meyer. "Evaluating Simulation and Laboratory-Based Learning in Higher Education: A Meta-Analysis of Student Outcomes." *Higher Education Research & Development* 42, no. 5 (2023): 1089–1104. https://doi.org/10.1080/07294360.2022.2152341
[6] Hussain, M., W. Zhu, W. Zhang, and S. M. R. Abidi. "Enhancing Student Employability Through Lab-Based Learning: A Longitudinal Study Across Disciplines." *Education + Training* 65, no. 2 (2023): 145–163. https://doi.org/10.1108/ET-05-2022-0198
[7] Johnson, A. (2022). *Cybersecurity pedagogy: The shift from theory to experiential practice*. Journal of Cyber Education, 15(3), 201–218. https://doi.org/10.1016/j.jce.2022.04.005
[8] Dalziel, J. (2022). *The role of simulation in developing adaptive expertise: A review of pedagogical frameworks*. Educational Technology Research and Development, 70(4), 1245–1263. https://doi.org/10.1007/s11423-022-10115-w
[9] Melnikovas, A., & Melnikova, J. (2023). Experiential learning in cybersecurity education: A systematic mapping study. *Journal of Engineering and Applied Sciences*, 18(2), 45–59. https://doi.org/10.36478/jeasci.2023.45.59

[10] Kebande, V. R. (2024). Enhancing digital forensics and cybersecurity education through virtual experiential laboratories. *Journal of Education and Information Technologies*, 29(1), 112–134. https://doi.org/10.1007/s10639-023-11842-1

[11] Spurava, G., & Kotilainen, S. (2023). Ethical literacy as a dimension of digital professionalism: A systematic review. *Journal of Media Literacy Education*, 15(1), 34–48. https://doi.org/10.23860/JMLE-2023-15-1-3

[12] Weichert, J., Smith, K., & Lee, R. (2025). *The ethics gap in computer science: A global survey of undergraduate curricula*. Journal of Computing Sciences in Colleges, 40(2), 88–104. https://doi.org/10.1145/example.2025.01

[13] Flechais, I., Sani, A. S., & Onwubiko, C. (2023). *Navigating the ethical landscape of cybersecurity: A study of professional decision-making*. Computers & Security, 128, 103165. https://doi.org/10.1016/j.cose.2023.103165

[14] Petelka, J., Ringland, K. E., Williams, A. C., & Spiel, K. (2022). *"I wouldn't even know where to start": Integrating ethics into computer science education*. Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, 1–16. https://doi.org/10.1145/3491102.3517447

[15] Liao, K. C., Lu, M. Y., & Chen, S. L. (2023). Enacting adaptive practice and reflection: An action research on transforming faculty development workshop design. *Journal of Applied Research in Higher Education*, 15(4), 912–928. https://doi.org/10.1108/JARHE-01-2022-0012

[16] Alpert, S., Beausaert, S., & Segers, M. (2022). Progressively reinforcing and extending research methods: An action research study in a doctoral program. *Educational Action Research*, 30(3), 456–474. https://doi.org/10.1080/09650792.2021.1921123

[17] Ferguson, T., Roofe, N., & Cook, L. D. (2023). Using student reflections to understand and enhance course experiences: An action research approach. *International Journal of Educational Research*, 118, 102145. https://doi.org/10.1016/j.ijer.2023.102145