Borneo International Journal eISSN 2636-9826; Vol. 9 (2); 2026; 16-22
Published by *Majmuah Enterprise*
www.majmuah.com

Comparison of the Efficacy of Capture The Flag (CTF) in Gamified Cybersecurity Training in Corporate Workforce

ABDIKANI OSMAN ABDALLA and MOHAMAD FADLI BIN ZOLKIPLI

School of Computing, College of Art and Science, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: abdiqanicusman9@gmail.com, m.fadli.zolkipli@uum.edu.my |Tell: +601137822074| +60 17-724 7779

Received: May 08, 2026
Accepted: May 14, 2026
Online Published: June 04, 2026

Abstract

Gamified cybersecurity education techniques, especially Capture The Flag (CTF) games, have become a growing example of alternative to conventional compliance-based awareness initiatives in business settings. Although they have been increasingly popular, little has been studied on their long-term return on investment (ROI) in actual organizational contexts. In this paper, the impact of CTF-based training relative to traditional cybersecurity training is assessed based on such key performance indicators as knowledge retention, behavioural change, and financial outcomes. To synthesize the existing evidence on training effectiveness and ROI-related measures, a systematic review of 22 peer-reviewed sources published within the period of 2021-2026 was developed. The results show that CTF based consistently outperforms, such as better knowledge retention, better engagement and reduced vulnerability to phishing attacks. Moreover, gamified training strategies show possible economic advantages in the form of a decrease in security attacks and a higher level of employee readiness. Longitudinal research in corporate sittings, however, is not abundant, especially where full-time employees are studied and the duration of evaluation is more than twelve months. To fill this gap, this paper suggests the use of a multidimensional ROI evaluation system that incorporates pre and post training evaluations, behavioural monitoring, incident monitoring and post training follow ups at 3, 6 and 12 months. The framework proposed provides a viable methodology that would assist the organizations to determine the success of the training conducted in CTF and enable them to make informed decisions concerning cybersecurity investment.
Keywords: behavioural change, capture the flag, cybersecurity training, gamification, return on investment, security awareness

1 Introduction

Digital transformation has made the threat landscape more impactful and human error is still the driving force behind 74% of cybersecurity incidents (Kaplan et al., 2022; Karagiannis & Magkos, 2021) Traditional cybersecurity training models focus on compliance, with video training sessions, annual attitudinal check-in, and periodic quizzes which have been found to yield only minimal practical skills and retention of 20-30% of information after six months (Ambrosio et al., 2021; Jean Tirstan T et al., 2022) These passive learning approaches lack interaction and exposure of real threats, leading to low motivation in employees and continuing security loopholes (Qolomany et al., 2024) Gamification offers a promising alternative by incorporating game-like mechanics such as challenges, leaderboards, points, and real-time feedback into training to enhance motivation and learning outcomes (Tan et al., 2025). Among gamified cybersecurity methods, Capture the Flag (CTF) competitions have emerged as particularly effective, providing hands-on competency development in areas such as web exploitation, cryptography, forensics, and network security at two to three times the speed of traditional lecturing (Cole, 2022; Kaplan et al., 2022) Jeopardy-style CTFs can be deployed in virtual environments and integrated with learning management systems (LMS) to enable scalable, enterprise-wide tracking and evaluation(Schafeitel-Tähtinen & Lazarov, 2025; Uluç & Eyüpoğlu, 2025)

Despite the numerous studies conducted on the use of CTF approach in Malaysia, majority of research have been carried out on the students of universities, which is a gap concerning the effectiveness of the CTF approach in corporate(Khoo et al., 2025; Razack & Saad, 2024) There is a lack of evidence regarding long term outcomes of full-time employees and return on investment (ROI) of CTF training in the context of the organisation. This led this paper to review systematically the literature and compare the results of 22 peer-reviewed publications (2021–2026) against the traditional compliance training approach in knowledge retention, skills acquired, employee engagement, employee behaviour, and organisational ROI. The study also suggests a multi-dimensional assessment system comprising pre-training baseline evaluations, immediate post-training evaluation, and long-term behavioural and financial monitoring at 3, 6 and 12 months.

2 LITERATURE REVIEW

2.1 Cybersecurity Training Challenges

Developing cybersecurity training has proven difficult because of the rigid nature of traditional teaching methods. (Pramod, 2025), standard cybersecurity awareness training is not possible to be effective to ensure user attention and essential convert into behavioural change This reflects a broader issue in cybersecurity education where passive learning methods cannot be relied upon to develop practical skills. According to Amjad et al., (2025), engagement and effectiveness assessment systems are often absent in many cybersecurity training programs. Their systematic review reveals that both active and learner-centred strategies should be used to achieve better results in the behavioural and awareness outcomes. The interaction between users plays a significant role in determining training tool effectiveness, as shown by Singh, (2025) According to that study, performance feedback systems in which students participate proactively perform better than those in which participation is minimal. This implies that, in addition to content delivery, the extent of interaction between learners and the system determines the effectiveness of the training.

2.2 Gamification in Cybersecurity

Gamified methods have become a promising solution to improving cybersecurity training practice, as they enhance engagement and knowledge retention. It has been demonstrated that the inclusion of game elements such as points, leaderboards, badges, narrative structures, and progression levels positively affects time-on-task and voluntary engagement, though much of this evidence comes from student-based research, which may limit its applicability to the workplace context (Okhae Joel Ojugo & Nse-obot Peter Afaha, 2025). Gamified security awareness programs have proven to be more engaging than traditional compliance-based training programs in organisational settings, although their effectiveness largely relies on well-designed challenges, instant feedback, and social competition (Williams et al., 2024; Zola et al., 2024). The presence of properly designed gamified training frameworks is usually characterised by clear learning goals, an upwardly challenging difficulty level, and social recognition mechanisms all of which are consistent with the design of Capture the Flag (CTF) competitions. This correspondence supports the appropriateness of CTF-based solutions as realistic and interactive approaches to cybersecurity education, as they naturally involve competitive problem-solving, progressive skill development, and active learner engagement (Singh, 2025). Empirical evidence also confirms that CTF-based learning environments are among the most effective gamified methods for enhancing knowledge acquisition, practical skills, and learners' attitudes in cybersecurity training (Jean Tirstan T et al., 2022)**.**

2.3 Capture The Flag (CTF) as Training Application

Capture the Flag (CTF) competitions are seen as a potentially viable method of cybersecurity training, since they offer both theoretical and practical training in a controlled, scenario-based context. In contrast to conventional teaching approaches, CTF platforms allow active learning by involving participants in problem-solving activities that cut across various cybersecurity areas, thus promoting the development of skills aligned with professional competency models (Cole, 2022). Experience shows that these settings greatly improve technical expertise in fields such as web security, cryptography, and digital forensics, largely due to their interactive and challenge-based format (Qolomany et al., 2024). In addition, the design of the platform is tightly linked to the pedagogical effectiveness of CTF training, with the introduction of adaptive difficulty, real-time feedback, and performance monitoring mechanisms that support long-term engagement and enhanced learning outcomes(Okhae Joel Ojugo & Nse-obot Peter Afaha, 2025; Singh, 2025). In addition to technical skills, user awareness and behavioural intention have also been positively affected by the incorporation of gamification components into CTF structures, supporting their use as a comprehensive method of cybersecurity training (Razack & Saad, 2024).

2.4 ROI in Cybersecurity Training

The challenge of measuring the return on investment (ROI) of cybersecurity training programs is another major research problem because of the mainly indirect and preventive benefits that are experienced. Unlike traditional investments, the value of such training can only be measured in terms of the rate of security incidents that can be prevented, or risk mitigated in an organisation, which is again difficult to measure. Therefore, the need for developing systematic systems for evaluation of such training is greatly needed to be able to measure the training process in terms of performance and competence improvement (Qolomany et al., 2024). Present-day approaches focus on the correlation between the outcomes produced as a result of CTF training implementation and tangible improvements in technical skills and user behaviour. Integration of assessment-based measures in the evaluation process—for example, reflective activities—enhances the reliability and validity of the measurement of cybersecurity training effectiveness, thereby making ROI calculation possible (Khoo et al., 2025). Moreover, the use of analytical tools capable of isolating the impact of the intervention in the learning process on organisational factors improves the evaluation foundation and facilitates attributing the achieved outcomes to particular training initiatives (Arduin & Costé, 2026).

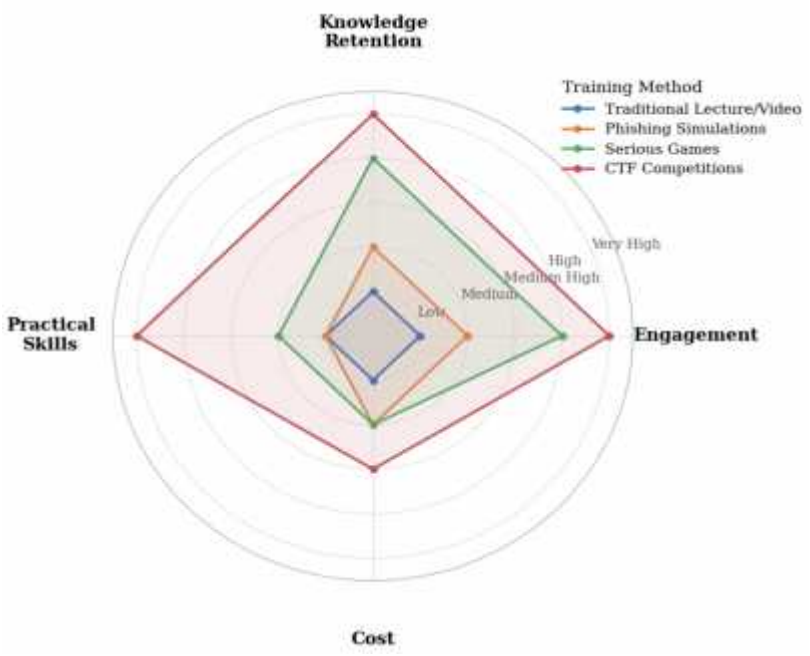
Borneo International Journal eISSN 2636-9826; Vol. 9 (2); 2026; 16-22
Published by *Majmuah Enterprise*
www.majmuah.com

2.5 Research Gap

Although the literature on Capture The Flag (CTF)-based cybersecurity training has been expanding, there still are several aspects, which are critical, that restrict its use in corporate settings. An impressive percentage of the literature has been carried out in an academic environment with majority of the research being done in student populations hence providing scanty evidence on efficacy in full time professionals and organizational (Khoo et al., 2025; Schafeitel-Tähtinen & Lazarov, 2025). This casts doubt on the validity of generalizations, as there are differences in the motivations, time limit, and performance expectations between academic and corporate training settings. Moreover, the existing studies are more focused on the short-term results, and the majority of them consider the immediate knowledge acquisition and involvement rates after the CTF participation, but little attention is paid to long-term knowledge retention and the long-term behavioural change (Okhae Joel Ojugo & Nse-obot Peter Afaha, 2025; Tan et al., 2025).Moreover, despite a range of frameworks that have been offered to evaluate the effectiveness of cybersecurity training, no standardized and validated models that are specifically designed to evaluate the return on investment (ROI) of CTF-based training in an actual organizational setting exist (Amjad et al., 2025; Qolomany et al., 2024).The limitations point to the necessity to consider a more holistic and longitudinal evaluation strategy, and this paper fills in these gaps by providing a multidimensional model of evaluating training efficacy and ROI within corporate cybersecurity settings.

Figure:1 gives a pictorial summary of the main features of the traditional, gamified, and CTF-based training modes to be discussed in this section.

Figure1: Comparison of Cybersecurity Training Methods.



3. METHODOLOGY

A systematic literature review (SLR) is used to explore and contrast the effectiveness of Capture the Flag (CTF)-based gamified cybersecurity training with conventional compliance-based cybersecurity awareness training within the context of organisations.

3.1 Research Design and Data Collection

A systematic search was carried out to identify relevant academic studies on cybersecurity training and gamification methods, published between 2021 and 2026. Academic databases, such as IEEE Xplore Scopus and ScienceDirect were used to retrieve relevant studies. A Boolean search strategy was used with the assistance of the following keywords: “Capture The Flag, gamifications, cybersecurity training, security awareness, behavioural change, and return on investment”.

3.2 Study Selection

The inclusion criteria were as follows: (i) peer-reviewed journal articles and conference papers, (ii) the studies focusing on the effectiveness of cybersecurity training, and (iii) the studies that report the results and outcomes linked to knowledge retention, behavioural change, or impact on organisations. Research that only involves general opinion articles or irrelevant issues was not included. The initial search yielded approximately 200 articles. After screening titles and abstracts for relevance, duplicate and irrelevant studies were removed. Having eliminated any duplicate materials and irrelevant research, it was found that a final list of 22 peer-reviewed articles was selected and to be analyzed in detail.

3.2 Data Analysis

Thematic synthesis was used to synthesize the research. This involved coding and classifying the findings to identify recurring themes across four categories: knowledge retention, behavioural change, user engagement, and return on investment (ROI). Comparison of findings revealed consistent performance differences between gamified training systems and non-gamified ones as well as important deficits in long-term evaluation. This synthesized knowledge was instrumental in the development of a comprehensive 12-month model for evaluating ROI, which is to be used to measure the effectiveness of cybersecurity training in companies.

4. Discussion

The discussion is based on the synthesis of the literature reviewed to provide the practical advice on the implementation and evaluation of CTF-based training in corporate settings. The thesis is that, when properly planned CTF programs are combined with a longitudinal ROI measurement program it is a better investment, as opposed to the conventional compliance based training models.

4.1 Strategic Implementation of CTF in Corporate Environments

To apply CTF events to a corporate environment, the format, platform, and integration should be taken into account. The best format to use in general corporate training is the Jeopardy-style format because it is easy to use and self-paced (Cole, 2022; Kaplan et al., 2022). Attack-Defense formatting, where the attack and defense are executed simultaneously, should only be used by special security operations units. The choice of platform is also important; open-source platforms such as CTFd can be deployed to scale, and analytics-based data-driven platforms can be shown to drive better skill development results (Singh, 2025). A CTF, however, should not be an independent activity. The hybrid CTF+LMS model, which can be integrated with the Learning Management System (LMS) of an organization, will allow tracking, competency mapping, and data collection that will be needed to calculate ROI (Karagiannis & Magkos, 2021; Razack & Saad, 2024)

Table 1. CTF Format Comparison and Corporate Suitability

Format	Target Audience	Key Benefit	Corporate Suitability
Jeopardy Style	Beginners & mixed teams	Accessible, self-paced, multi-domain	High Ideal for general workforce
Attack Defense	Advanced SOC teams	Adversarial thinking, incident response	Medium Requires infrastructure
King of the Hill	Intermediate teams	System hardening, live defense	Medium-High
Hybrid CTF+LMS	All skill levels	Trackable, scalable, integrated	Very High Best for ROI

Note. Data synthesized from Amjad et al. (2025) , Mohamad Fadli bin Zolkipli (2026) , Jean Tirstan T et al. (2022) , and Williams et al. (2024)

4.2 A Consolidated Framework for Measuring ROI

The return on investment (ROI) of Capture The Flag (CTF) cybersecurity training is challenging to assess because the "return" is largely in the form of preventing security incidents. As a result, a holistic and longitudinal approach to assessment is needed to not only measure immediate learning gains, but also the long-term behavioural and financial impact. The current research indicates that CTF-style and gamified cybersecurity training significantly improves engagement, learning retention and behavioural outcomes when compared to passive learning approaches (Amjad et

al., 2025; Pramod, 2025). In addition, empirical research shows that gamified cybersecurity training leads to decreased vulnerability to phishing and better security practices (Williams et al., 2024), with systematic reviews validating their impact on improving cybersecurity knowledge and skills (Tan et al., 2025). This study proposes a three-phase longitudinal approach to measuring the ROI for a 12-month period, combining knowledge assessment, behavioural diagnostics and financial analysis.

Phase I: Pre-training Assessment (Month 0)
Organizations need to set a baseline before training to facilitate comparisons. This phase includes:

- Knowledge Assessment: Assessing employees' technical and security awareness.
- Behavioural Diagnostics: Assessment of actual vulnerability with phishing click-through rates and compliance with security policies (A. St. Khadijah Ridwan et al., 2025).
- Cost Benchmarking: Establishment of the company's past cost per security incident as a cost benchmark.

This cost baseline helps overcome a common challenge in training evaluation by providing a way to measure change.
Phase II: Test and Technical Analytics (Months 1-3)
The emphasis during the CTF-based training phases is on measuring "active ROI" via platform analytics.

- Engagement Metrics: Measuring participation rate, time-on-task, and voluntary participation, which tend to be higher with games (Singh, 2025; Uluç & Eyüpoğlu, 2025).
- Learning: Tracking learner advancement through platform metrics such as flags and hints, and considering competency models such as those of National Institute of Standards and Technology.
- Post-Training Assessment: Assessing knowledge gain (delta change) via post-training quizzes on cognitive and technical skills.

This period aligns with the learning and immediate result levels of existing training evaluation models, capturing immediate benefits.
Phase III: Long-term Impact and Return on Investment (ROI) (Months 3-12)
The success of CTF training is measured by the sustainability of behavioural change and its impact on the organisation.

- Knowledge Retention: 3, 6 and 12-month follow-up testing to measure retention of knowledge, given evidence of its decline in traditional training models.
- Impact on Behaviour and Incidents: Ongoing analysis of security logs to detect decreases in human-error-based incidents, such as phishing and password breaches (Williams et al., 2024).
- Return On Investment (ROI): Calculating the financial gains by comparing the cost of training against the value of the incidents that could have happened without the training, which can be found in industry reports such as Ponemon.

The ROI is based on the financial formula:

$$R = \frac{\text{Cost of CTF Training Value of Prevented Incidents} - \text{Cost of CTF Training}}{\text{Cost of CTF Training}} * 100$$

Framework Contribution
The methodology in this approach can be used to systematically and empirically evaluate the effectiveness of CTF cybersec training by looking at how technical, behavioural and economic factors combine to impact the results. This evaluation framework is multi-dimensional and longitudinal; it captures not only short-term knowledge retention, but also long-term behaviour change, by linking the impact of training to the organizations' overall cybersecurity performance. Additionally, the evaluation framework provides a solid basis for making a case for investing in cybersec training, and it expands the body of research on gamified cybersecurity training.

4.3 Addressing Implementation Challenges

Using CTF for cybersecurity education has a lot of advantages in terms of user engagement and enhancing applicable skills; however, implementing CTF in an organizational setting presents many challenges. The first challenge is how to determine the proper level of difficulty of each challenge to use with users. If you create tasks that are too difficult, it could lead to discouraging those users who are not as experienced; however, tasks that are too easy will result in boredom for those who are more advanced (Jean Tirstan T et al., 2022; Taherdoost, 2024).Another issue to take into consideration, especially when looking to roll out CTF on a larger scale is scalability of how to provide continued training and support by way of providing quality and appropriate challenges, which can only be achieved with consistent access to qualified staff and relevant resources (Singh, 2025; Uluç & Eyüpoğlu, 2025). Moreover, performance evaluation can be undermined by the performance evaluation practices, including flag sharing, which can manipulate the results of performance evaluation and restrict the ability to measure real competencies (Cole, 2022; Kaplan et al., 2022). Inequalities in participation, especially the lack of women, also bring up questions about inclusivity in CTF settings (Schafeitel-Tähtinen & Lazarov, 2025). Taken together, these issues should underscore the need to implement strategies carefully that balance instructional design, assessment integrity, and inclusivity to make the training based on CTF effective and sustainable in the context of real organizations.

4.4 Proposed Solutions and Mitigations

There are several approaches that can help address these issues through targeted organizational interventions, including having tiered libraries of cyber challenge types (CTFs) with adaptive hint mechanism, which have been shown to result in sustained engagement among many different types of participants (Qolomany et al., 2024); using cloud-native, containerized CTF infrastructures to overcome limitations of scalability so organizations of various sizes can deploy cost-effective, reproducible training environments (Singh, 2025); and aligning CFT-based assessments with established competency frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Workforce Framework, so that there is a direct relationship between training outputs and the skills needed by organizations to perform their work, giving an evidence-based basis for calculating return on investment (ROI) (Amjad et al., 2025; Tan et al., 2025).Lastly, the application of collaborative/socio-historical/inclusive ideas in designing CTFs and offering participants team-based methods to compete has been demonstrated as potentially effective at minimizing the gender participation gap in CTFs and enhancing inclusiveness overall in the cybersecurity training setting(Schafeitel-Tähtinen & Lazarov, 2025).

5. Conclusion

This paper compared the effectiveness of Capture The Flag (CTF) competitions and conventional compliance-based cybersecurity training on corporate workforces. According to the analysis of peer-reviewed sources, CTF-based training shows better results in various aspects: better knowledge retention, more practical skills acquisition, better employee engagement, quantifiable behavioural change, and positive ROI (Amjad et al., 2025; Pramod, 2025; Singh, 2025; Tan et al., 2025; Williams et al., 2024). CTF competitions are aligned with professional competency models, including NICE, to allow standard evaluation and calculable ROI (Amjad et al., 2025; Tan et al., 2025). The multidimensional ROI measurement framework suggested in this paper (section 4.2) offers organizations with a systematic approach of measuring both financial and behavioural returns of CTF training investments, which is a major gap in the current literature (Qolomany et al., 2024; Taherdoost, 2024; Vineetha Harish et al., 2025). Although it has been shown to be effective, there are still a number of challenges to broad corporate implementation, such as that it is difficult to calibrate with heterogeneous groups of employees, is not easily scalable or cost-efficient to support, there is a risk of cheating, and little evidence of its use has been established on full-time employees (Cole, 2022; Jean Tirstan T et al., 2022; Kaplan et al., 2022; Uluç & Eyüpoğlu, 2025). The next step in research should be the longitudinal studies of CTF outcomes during 12-months or more in real corporate environment and the creation of automated analytics dashboard that will be integrated with organizational LMS and incident reporting systems (Khoo et al., 2025; Ridwan et al., 2025; Schafeitel-Tähtinen & Lazarov, 2025).

Acknowledgments

The authors would like to express their sincere appreciation to the School of Computing, Universiti Utara Malaysia, for their support and guidance throughout this study. The authors also acknowledge the contributions of researchers whose work has informed and supported this research.

References

Ambrosio, J., Burghardt, M. D., & Hecht, D. (2021). Authentic Engineering Design Assessment. *2021 ASEE Virtual Annual Conference Content Access Proceedings*, 36735. https://doi.org/10.18260/1-2--36735

Amjad, K., Ishaq, K., Nawaz, N. A., Rosdi, F., Dogar, A. B., & Khan, F. A. (2025). Unlocking Cybersecurity: A Game-Changing Framework for Training and Awareness—A Systematic Review. *Human Behavior and Emerging Technologies*, *2025*(1), 9982666. https://doi.org/10.1155/hbe2/9982666

Arduin, P.-E., & Costé, B. (2026). Learning to Hack, Playing to Learn: Gamification in Cybersecurity Courses. *Journal of Cybersecurity and Privacy*, *6*(1), 16. https://doi.org/10.3390/jcp6010016

Cole, S. V. (2022). Impact of Capture The Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class. *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*, 470–476. https://doi.org/10.1145/3502718.3524806

Jean Tirstan T, Joy Gilbert A, & Nelmiawati Nelmiawati. (2022). Analysis of Cyber Security Knowledge and Skills for Capture the Flag Competition. *JURNAL INTEGRASI*, *14*(1), 14–22. https://doi.org/10.30871/ji.v14i1.3986

Kaplan, Z., Zhang, N., & Cole, S. V. (2022). A Capture The Flag (CTF) Platform and Exercises for an Intro to Computer Security Class. *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 2*, 597–598. https://doi.org/10.1145/3502717.3532153

Karagiannis, S., & Magkos, E. (2021). Adapting CTF challenges into virtual cybersecurity learning environments. *Information & Computer Security*, *29*(1), 105–132. https://doi.org/10.1108/ICS-04-2019-0050

Khoo, L. J., Mohamad Yatim, M. H., & Wong, Y. S. (2025). Research on Capture the Flag Exercises for Cybersecurity Skill Training Among Malaysian Undergraduates. *Journal of Human Centered Technology*, *4*(1), 1–9. https://doi.org/10.11113/humentech.v4n1.87

Okhae Joel Ojugo & Nse-obot Peter Afaha. (2025). Impact of AI-Enhanced Capture the Flag (CTF) competitions on student learning outcomes in cybersecurity training: A qualitative study. *Open Access Research Journal of Engineering and Technology*, *8*(2), 073–080. https://doi.org/10.53022/oarjet.2025.8.2.0044

Pramod, D. (2025). Gamification in cybersecurity education; a state of the art review and research agenda. *Journal of Applied Research in Higher Education*, *17*(4), 1162–1180. https://doi.org/10.1108/JARHE-02-2024-0072

Qolomany, B., Calay, T. J., Hossain, L., Mulahuwaish, A., & Bou Abdo, J. (2024). CCTFv2: Modeling Cyber Competitions. *Entropy*, *26*(5), 384. https://doi.org/10.3390/e26050384

Razack, A. K. A., & Saad, M. F. M. (2024). Enhancing Cybersecurity Awareness through Gamification: Design an Interactive Cybersecurity Learning Platform for Multimedia University Students. *Journal of Informatics and Web Engineering*, *3*(3), 21–40. https://doi.org/10.33093/jiwe.2024.3.3.2

Ridwan, A. St. K., Radiyah, U., Malik, M. I., Pattiroi, M. N., Fajri, N. U., & Amir, N. (2025). The Effectiveness of Capture The Flag as a Network Security Practical Intervention on Students' Self-Efficacy and Learning Outcomes. *Information Technology Education Journal*, 811–824. https://doi.org/10.59562/intec.v4i4.11191

Schafeitel-Tähtinen, T., & Lazarov, W. (2025). Capture the Flag as a Learning Tool to Improve Cybersecurity Education. *SEFI 53rd Annual Conference Proceedings (or Leave Blank If Not Specified)*. SEFI 53rd Annual Conference. https://doi.org/10.5281/ZENODO.17631277

Schafeitel-Tähtinen, T., & Lazarov, W. (2025). Teaching and Learning Cybersecurity Using Capture the Flag: Effectiveness Comparison Between University Students in Finland and Czechia. *Computer Applications in Engineering Education*, *33*(5), e70082. https://doi.org/10.1002/cae.70082

Singh, H. (2025). An Analysis on Data-Driven Capture the Flag (CTF) Platforms for Cybersecurity Education. *International Journal for Research in Applied Science and Engineering Technology*, *13*(11), 380–389. https://doi.org/10.22214/ijraset.2025.75084

Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. *Information*, *15*(9), 512. https://doi.org/10.3390/info15090512

Tan, T., Abdullah, R. S., & Mas'ud, Z. (2025). Cybersecurity Education Using Gamification: Systematic Literature Review. *International Journal of Academic Research in Business and Social Sciences*, *15*(10), Pages 743-760. https://doi.org/10.6007/IJARBSS/v15-i10/26583

Uluç, C., & Eyüpoğlu, C. (2025). *Development of Capture the Flag Platform for Cyber Security Education*. *18*(1), 1–42. https://jast.hho.msu.edu.tr

Vineetha Harish, A., Tam, K., & Jones, K. (2025). Generating training events for building cyber-physical security skills. *The Computer Journal*, *68*(5), 445–459. https://doi.org/10.1093/comjnl/bxae123

Williams, L., Anthi, E., Cherdantseva, Y., & Javed, A. (2024). Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students. *Journal of The Colloquium for Information Systems Security Education*, *11*(1), 8. https://doi.org/10.53735/cisse.v11i1.186

Zola, F., Echeberria, X., Petisco, J., Vakakis, N., Voulgaridis, A., & Votis, K. (2024). KINAITICS: Enhancing Cybersecurity Education Using AI-Based Tools and Gamification. *Proceedings of the 2024 16th International Conference on Education Technology and Computers*, 138–147. https://doi.org/10.1145/3702163.3702183