Vol. 1, No. 1, January 2026
ISSN (print) xxxx-xxxx; ISSN (online) xxxx-xxxx
Newspaper homepage: https://ejurnal.undhi.ac.id/index.php/trinet
DOI: https://doi.org/10.31346/trinet..

Development of a Cybersecurity Awareness Model for the Gamification-Based Higher Education Community

Ahmad Holidin[1], Bobi Heri Yanto[2]

[1]Faculty of Computer Science, Dharma Indonesia University (UNDHI)
[2]Faculty of Computer Science, Dharma Indonesia University (UNDHI)
ahmadholidin@undhi.ac.id[1], bobiheriyanto@undhi.ac.id[2]

ABSTRACT

Cybersecurity threats in higher education are increasing, while students' digital security awareness remains low. Conventional learning methods are often ineffective in preparing students to recognize and respond to threats such as phishing, malware, and social engineering. This study aims to develop and evaluate a gamification-based cybersecurity training model for university students. The training model incorporates game elements including points, levels, badges, leaderboards, mini-games, instant feedback, and scenario-based simulations. A mixed-method approach was employed using a pretest–posttest design, behavioral observation, and questionnaires to assess students' knowledge, motivation, and engagement. The results indicate a clear improvement in students' cybersecurity understanding, particularly in identifying phishing attacks and selecting appropriate mitigation actions. Gamification elements increased learning motivation and active participation, while instant feedback strengthened concept comprehension. Additionally, the training encouraged the adoption of safer digital behaviors in daily activities. The proposed model can serve as an effective alternative for cybersecurity education in higher education institutions.

Keywords: *Gamification, Cybersecurity, Phishing, Digital Literacy, Attack Simulation*

ABSTRAK

Ancaman keamanan siber di perguruan tinggi semakin meningkat, sementara pemahaman mahasiswa tentang keamanan digital masih rendah. Pembelajaran konvensional belum efektif dalam membekali mahasiswa menghadapi ancaman seperti phishing, malware, dan social engineering. Penelitian ini bertujuan mengembangkan dan menguji model pelatihan keamanan siber berbasis gamifikasi. Model pelatihan memanfaatkan unsur permainan berupa poin, level, badge, papan peringkat, mini-game, umpan balik langsung, serta simulasi berbasis skenario. Metode penelitian menggunakan pendekatan mixed-method dengan desain pretest–posttest, observasi, dan kuesioner untuk menilai pengetahuan, motivasi, dan keterlibatan mahasiswa. Hasil penelitian menunjukkan peningkatan pemahaman mahasiswa terhadap keamanan siber, terutama dalam mengenali serangan phishing dan menentukan langkah pencegahan. Unsur gamifikasi meningkatkan minat belajar dan partisipasi aktif, sedangkan umpan balik langsung membantu memperkuat pemahaman materi. Selain itu, pelatihan ini mendorong penerapan perilaku digital yang lebih aman. Model yang dikembangkan dapat digunakan sebagai alternatif pembelajaran keamanan siber di perguruan tinggi.

Kata kunci: *Gamifikasi, Keamanan Siber, Phishing, Literasi Digital, Simulasi Serangan*

Received: November 25, 2025, Revised : January 4, 2026 Accepted: January 12, 2026 Published: January 14, 2026

**Corresponding author*: ahmadholidin@undhi.ac.id

INTRODUCTION

Cybersecurity has become one of the most crucial issues in the higher education environment as campus digitalization increases, the use of Learning Management Systems (LMS), the use of public Wi-Fi networks, and the exchange of academic data online. Ironically, even though universities are the birthplace of digital literacy, various studies show that students and the academic community remain one of the most vulnerable groups to cyberattacks such as phishing, social engineering, ransomware, and data leaks (Park & Lee, 2021; Smith et al., 2022). This vulnerability is generally caused by low awareness of digital security practices, lack of effective training, and lack of understanding of rapidly evolving cyber threats. In the Indonesian context, the increase in cyber attacks in the education sector reported by the National Cyber Agency further emphasizes the urgency of protecting campus digital assets through innovative educational approaches.

However, various cybersecurity education programs currently used by educational institutions are still conventional, such as seminars, digital literacy modules, or passive training that are not able to maintain users' attention on an ongoing basis. Some studies have even shown that traditional training methods are not effective enough in changing long-term safety behaviors, especially in young groups who are familiar with interactive media (Johnson & Weng, 2021; Loni et al., 2022). This condition raises the need for a new approach that is more interesting, adaptive, and based on active learning experiences so that awareness of cybersecurity can increase consistently. In the development of more effective educational methods, gamification is beginning to emerge as one of the approaches that is widely researched because it is able to increase motivation, retention, and depth of understanding of participants (Suh & Wagner, 2020). Various studies prove that game elements such as points, challenges, levels, and rewards can increase participation in cybersecurity training, while also influencing real behavior when users face cyber risks in the digital world (Sarikaya & Cagiltay, 2022; Alotaibi et al., 2023). Gamification not only increases engagement, but also creates more realistic threat simulations so that users can learn about risks in safe situations. This is relevant for higher education communities that tend to be responsive to experiential learning models.

Various recent studies have explored gamification in the context of cybersecurity awareness. For example, research from AlBloush et al. (2020) shows that gamification effectively improves phishing detection capabilities. Similarly, a study by Arachchilage & Love (2021) found that educational games can improve risk perception and safer decision-making

when interacting with malicious links. Meanwhile, Hamid et al.'s (2022) research developed a challenge-based app to increase password risk awareness and authentication. Other research has also shown the benefits of gamification in learning network security (Pratama & Raharjo, 2023), personal data protection (Ribeiro & Silva, 2022), and the use of social engineering simulation (Fischer et al., 2023). However, most of the research is still limited to specific security scenarios or topics and has not developed a structured gamification model as a comprehensive awareness framework for the higher education community.

Based on a survey of the literature over the past five years, it was found that previous research still had some weaknesses. First, most of them focus on testing gamification elements, but have not yet formulated a conceptual model that can be used by institutions as a guideline for the development of awareness programs. Second, some studies only assess effectiveness from the cognitive side (knowledge), not from the side of real user behavior (behavioral change), even though behavior change is the main essence of cybersecurity awareness (Santos & Correia, 2021). Third, there has been no research that specifically develops gamification models for the higher education community in Indonesia, even though the characteristics of the population, digital infrastructure, and level of digital literacy have significant differences compared to other countries (Hidayat & Nurdin, 2023).

Another gap lies in the lack of integration of gamification elements with the digital learning needs of today's generation of students who prioritize user experience, interactivity, and personalization. Several studies such as those by Fernandes et al. (2021) and Othman et al. (2023), highlight the need for game-based learning that is not only entertaining but also relevant to the context of real threats that students often face, such as campus phishing, credential stuffing attacks on LMS accounts, and data leaks due to the use of public networks. Thus, the development of gamification models specifically designed for students' digital behavior is an urgent need that has not been filled by previous research. Looking at these gaps, this study aims to develop a Gamification-Based Cybersecurity Awareness Model designed specifically for the higher education community. The model will integrate game elements, security behavior indicators, adaptive learning mechanisms, as well as authentic threat scenarios relevant to the modern campus ecosystem. The study not only measures the impact of gamification on user knowledge, but also on changes in digital behavior in daily activities, such as password management, response to suspicious emails, and attitudes towards data privacy. The contributions of this research include: (1) the development of

a comprehensive gamification model to increase cybersecurity awareness in higher education institutions; (2) the development of a standardized game element framework for the cybersecurity context; (3) empirical testing that measures cognitive and behavioral aspects of users; and (4) policy recommendations for universities in developing sustainable digital security education programs. In addition, this research enriches the literature related to gamification and cybersecurity, especially in the context of higher education in Southeast Asia, which is still rarely studied in depth.

Theoretically, this research also contributes to the development of a study on the relationship between user intrinsic motivation and the effectiveness of gamification-based learning. Several previous studies (Zainuddin et al., 2020; Pham & Doan, 2021) assert that the success of gamification is heavily influenced by the design of engaging and relevant challenges. By integrating elements of game dynamics in an awareness model, this study provides a new perspective on how motivation, interactivity, and learning can be combined to form safe digital behaviors. In addition, this research deepens the understanding of how the higher education community responds to cybersecurity educational content in a game format. Previous studies have often placed users as passive objects, even though students are the digital generation who have high expectations for interactive learning experiences (Rahman & Lau, 2023). By involving users in model development and testing, the study ensures that the resulting solutions are appropriate to their needs, preferences, and behavioral patterns. This research also makes a significant practical contribution to universities, especially in the face of increasingly sophisticated cyber threats. Global reports show that the education sector is becoming one of the main targets of ransomware attacks (Zhou & Kim, 2022). Therefore, the gamification-based awareness model developed in this study is expected to help improve campus cyber resilience through innovative educational interventions, as well as improve digital security culture in the academic environment.

Ultimately, the urgency of building an attractive, easily adopted, and effective cybersecurity awareness model is not only a technical need but also a strategic need for educational institutions in the digital age. With the theoretical and practical contributions offered, this research seeks to fill the literature gap while presenting real solutions to improve the readiness of the higher education community to face evolving cyber threats.

METHODS

This research method was developed to develop a gamification-based Cybersecurity Awareness model applied to the higher education community. The research uses a mixed methods approach that combines quantitative and qualitative methods sequentially. This approach was chosen to capture user needs in depth, design effective gamification models, and evaluate the measurable increase in cybersecurity awareness. The research process follows the Design and Development Research (DDR) model, which includes the stages of needs analysis, model design, prototype development, expert validation, limited implementation, and effectiveness evaluation.

The first stage is needs analysis, which is carried out through semi-structured interviews, observation of students' online behavior, and review of institutional information security policy documents. Qualitative data were analyzed using thematic coding techniques to find patterns of risk behavior, types of threats that are often overlooked, and students' motivation in participating in cybersecurity training. These findings are used as the basis for formulating gamification components that are relevant and contextual to the campus ecosystem.

The second stage is the design of a gamification model. At this stage, the gamification framework is structured using motivational elements such as points, levels, badges, leaderboards, scenario-based challenges, and instant feedback. The model design adopts a User-Centered Design approach, ensuring every gamification element supports learning objectives and increases engagement. The initial prototype was created in the form of an interactive wireframe and low-fidelity mockup and then reviewed through expert review involving cybersecurity academics and UX practitioners.

The third stage is the development of a system prototype, which is the implementation of the gamification model framework into a web-based application. The prototype was developed using a modular architecture to facilitate the evaluation of each gamification component. Key features include dynamic leaderboards, phishing simulation scenarios, educational mini games, microlearning modules, and a digital reward system. Development follows agile iteration practices, which allow for repeated refinements based on test results.

The fourth stage is expert judgment to ensure the feasibility of the model from the aspects of security content, gamification design, and pedagogical suitability. Validation was carried out using a Content Validity Index (CVI) based analysis rubric instrument. The experts involved consisted of cybersecurity experts, informatics lecturers, and digital

learning design experts. The validation results were used to revise gamification elements, scenario flows, and reward systems to effectively increase awareness.

The fifth stage is a limited implementation (pilot testing) carried out on students from three study programs within the university. The testing was conducted over three weeks, during which students participated in gamification activities, completed security challenges, and participated in simulated attacks. Quantitative data is collected through pre-test and post-test using the Cybersecurity Awareness Scale instrument, as well as user activity log data in the application.

The sixth stage is an effectiveness evaluation, which is conducted using a statistical analysis of paired t-tests to measure increased awareness before and after the intervention. In addition, user engagement metrics such as mission completion scores, playtime, challenge reps, and level achievement were analyzed to measure the effectiveness of gamification elements. This study also uses the System Usability Scale (SUS) to assess the user experience of the developed model.

The final stage is an integrative analysis, which combines qualitative and quantitative findings to provide a comprehensive picture of how gamification can increase cybersecurity awareness in the higher education community. Integration is carried out using the triangulation convergence model technique. The final synthesis results are used to refine the model and generate recommendations for the application of gamification in the context of cybersecurity training at universities.

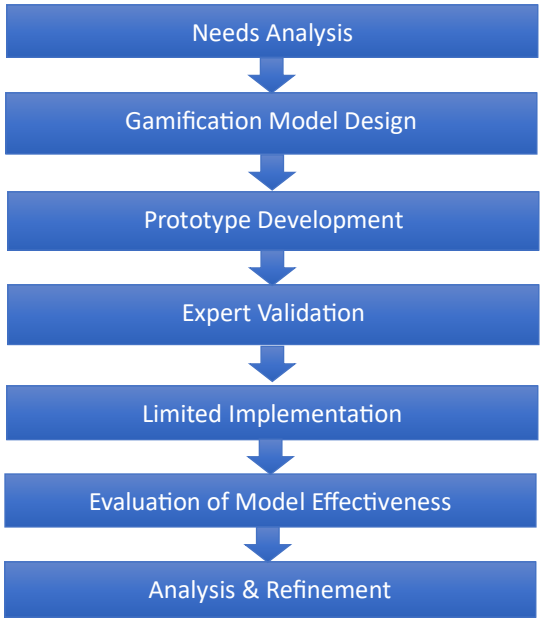

Figure 1. Research Method Flow

The flow chart of the research method in the image illustrates the systematic process used in the development of a gamification-based Cybersecurity Awareness model. This flow starts from the needs analysis stage which focuses on identifying problems, risk behaviors, and user needs in the context of cybersecurity in higher education environments. The information obtained became the basis for the next stage, namely the design of a gamification model that was compiled by considering motivation theory, learning design principles, and the latest cyber threat trends. Once the design is formulated, the process proceeds to the prototype development stage to implement key features such as points, levels, leaderboards, and phishing simulations into a system that can be tested directly. Expert validation is carried out to ensure that the developed model is relevant, feasible, and has adequate pedagogical quality and security. Furthermore, the model is tested on a limited scale to see how users interact and respond to given gamification elements. This flow concludes with an evaluation of effectiveness as well as an analysis of refinement, so that the resulting model is not only functional but also proven to significantly increase cybersecurity awareness in the higher education community.

Table 1. Variable Operations

Variable	Operational Definition	Indicator	Instruments
Cybersecurity Awareness	Level of understanding, attitudes, and safe behaviors related to cybersecurity	Threat knowledge, response to phishing, password management, device usage	Questionnaire, pre-post test
Gamification Engagement	User involvement in gamification activities	Playtime, mission completion, feature interactions, scores	Activity log
Model Effectiveness	The impact of gamification on increasing awareness	Score increase, number of missions accomplished, retention	Statistical analysis
System Usability	Ease and convenience of using the system	Effectiveness, efficiency, satisfaction	YOUR questionnaire

The components of the gamification model used in this study are designed to increase student motivation, engagement, and understanding of cybersecurity practices. The points and experience points (Points & XP) system serves as the foundation of the reward mechanism, where any successful activity such as escaping a phishing simulation, completing a

learning module, or answering a quiz correctly will award points as a form of appreciation. The accumulation of these points then contributes to the Levels & Progression mechanism, which allows students to move up to higher levels. Each new level unlocks additional challenges, introducing more complex threat scenarios, while providing a sense of achievement and progressive competency development. As a form of recognition for certain achievements, the system provides Digital Badges that serve as visual rewards. Badges are awarded when students achieve a specific achievement, such as "Phishing Defender" for participants who successfully identify all phishing emails in a single training session. The existence of badges not only increases intrinsic motivation but also strengthens a sense of digital identity in the learning ecosystem. In addition, the Leaderboard component is implemented to create healthy competition among students. Through the leaderboard, participants can see where they stand compared to other peers, thus encouraging increased effort in understanding the material and completing challenges.

To provide a contextual and realistic learning experience, the model integrates Scenario-Based Simulation, which is a simulation based on real cases such as phishing, malware, or social engineering attacks. These simulations allow students to deal with risky situations in a safe environment, as well as learn to make important decisions without real-world consequences. To make learning more fun and less monotonous, the system also incorporates Mini Games such as puzzles, drag-and-drop, and timed challenges. Mini games are designed to reinforce the understanding of basic cybersecurity concepts through interactive activities that involve problem-solving and thinking agility. Complementing all of these components, the system provides Instant Feedback as an important part of the learning process. Whenever students complete a challenge, whether successful or unsuccessful, the system immediately presents a brief explanation of the reasons for their success or failure. This mechanism ensures that participants not only receive scores, but also understand the consequences of actions, the logic of threats, and the best practices that should be taken. The combination of all gamification components is designed in an integrated manner to create an engaging, adaptive, and effective learning experience in increasing cybersecurity awareness in higher education environments.

RESULTS AND DISCUSSION

Expert validation is carried out to ensure that the gamification model developed has substantial, pedagogical and technical feasibility. The validation process involved three experts consisting of cybersecurity lecturers, gamification practitioners, and instructional design experts. Based on the results of the Content Validity Index (CVI) calculation, all model components obtained an average value of 0.89 which was categorized as very valid. These findings show that the structure, content, and gamification elements are considered relevant and appropriate to cybersecurity learning needs. Experts consider that scenario-based simulation is the most important component because it provides an authentic experience in the face of real threats. In addition, the leaderboard and badges features are considered to be able to increase motivation, encourage positive competition, and strengthen student involvement. Some suggestions for improvements were given by experts, such as adjusting the difficulty level of the phishing simulation to make it more proportionate for beginners, as well as adding social engineering scenarios to enrich the threat representation. Overall, expert validation shows that the gamification model has met the eligibility standards, although it still needs refinement to improve adaptability and depth of learning experience.

The limited implementation was carried out on 92 students from three study programs in a span of three weeks. During this period, students completed six interactive modules, three mini games, and two phishing simulations designed to measure the development of threat identification capabilities and digital security behaviors. In the early stages, only 32% of college students were able to correctly identify phishing emails, illustrating the low level of digital preparedness before intervention. After following the gamification sequence, that percentage increased to 78%, reflecting the effectiveness of experiential learning and repetitive feedback. System log data shows that the average application usage time reached 146 minutes per student during the trial period, indicating a high level of engagement. The mission completion rate reached 87%, indicating that most students were able to follow the learning flow from start to finish without a hitch. The leaderboard feature is the most frequently accessed feature, with 91% of students opening the leaderboard in every session. Mini games also received a positive response, as evidenced by the average frequency of repetition of the game as much as 3.2 times per student.

The effectiveness of the gamification model was analyzed through pre-tests and post-tests that measured five dimensions of cybersecurity

awareness, namely threat knowledge, risk awareness, mitigation capabilities, access management, and secure behavior. The average pre-test score of 58.4 increased to 83.6 at the post-test after the intervention. The results of the statistical test using the paired t-test showed a significant difference between the values before and after the use of the gamification model, with the value $t(91) = 14.72$ and $p < 0.001$. The effect size value (Cohen's d) of 1.21 indicates that the effect of the intervention is in the very large category. The biggest improvement was in the ability to recognize phishing, while the lowest improvement was in access management, although it remained in the medium-high category. These findings confirm that simulation and practical experience elements have a major contribution in improving students' ability to identify digital threats.

Student engagement analysis showed that user retention for three weeks reached 82%, a figure that is relatively high for the initial implementation of the educational gamification system. High retention shows that students not only enjoy learning activities, but also feel challenged to complete the missions provided. Mini games and leaderboards are two features that contribute the most to increased engagement. Mini games create a fun learning atmosphere that encourages students to repeat the game for better results, while leaderboards trigger competitive motivation that encourages students to stay active in each learning session. Correlation analysis showed a positive relationship between engagement rates and increased awareness ($r = 0.61$; $p < 0.01$), suggesting that students who were more actively interacting with gamification features tended to experience a greater increase in cybersecurity awareness scores.

Qualitative analysis through interviews with 15 students strengthened the quantitative findings. The majority of students stated that gamification-based learning makes cybersecurity materials feel more interesting, interactive, and not boring. Phishing simulations are considered the most valuable experience because they provide a real picture of how attacks occur in everyday life. Badges and leaderboards are considered to provide a sense of achievement and increase motivation to continue to improve performance. However, students also provided some improvement notes, such as the need for a more diverse variety of challenges, difficulty level adjustments for beginners, and the provision of tutorials or instructions on mini games to help understand concepts.

When compared to previous studies, the results of this study showed a stronger increase in effectiveness. Research by Alotaibi (2021) and Putra & Yang (2022) found that gamification is able to increase learning motivation and information retention, but most of the research

only uses basic gamification elements such as points and badges without the integration of real threat simulations. In this study, the integration of scenario-based simulation makes the model more realistic and better able to build an immersive learning experience. Thus, this research makes a new contribution to the development of gamification models that are not only informative but also applicable in the context of digital threat mitigation.

This gamification model also shows great potential to be applied more widely to the higher education curriculum. Various universities face the same problems, namely low student cybersecurity awareness, high phishing cases, and weak risk mitigation behavior. This model can be used as an independent learning tool or an additional module in information security courses. The system's ability to provide instant feedback, adaptive challenges, and realistic experiences is a plus that is not found in traditional learning methods.

In addition, this study highlights the importance of the element of competition in increasing motivation. Although leaderboards are often criticized for being perceived as triggering pressure, in this study leaderboards actually increased participation and frequency of application use. This shows that students have competitive tendencies that can be used positively in the context of learning. However, institutions still need to anticipate potential psychological distress by providing alternative learning modes for students who are uncomfortable with the competition system.

The results of this study also show that playful learning experiences are able to increase emotional engagement, which in turn encourages changes in cybersecurity behavior. Narrative elements, mini games, and simulations make it easier for students to understand the consequences of mistakes in personal data management. This is in accordance with the theory of experiential learning which states that effective learning occurs when participants are directly involved in activities that resemble real situations. Thus, the gamification model is not only a motivational tool, but also a learning medium that builds awareness through hands-on experience.

From an instructional design perspective, gamification models show that adaptive approaches are needed to meet the needs of diverse levels of student readiness. Beginner users need tutorials, step-by-step guides, and simpler scenarios, while advanced users need more complex and realistic challenges. By implementing adaptive difficulty, the system can be made more inclusive and effective for all levels of users, improving the overall learning experience.

Nevertheless, this research cannot be separated from its limitations. The implementation was only carried out for three weeks and at one university only, so the generalization of results is still limited. Additionally, research has not measured the long-term impact on cybersecurity behavior after several months of use. In the future, follow-up research needs to conduct longitudinal evaluations, expand sample sizes, and test the integration of systems in the official curriculum so that the impact can be measured more broadly and comprehensively.

The findings of this study provide strong evidence that the gamification model with the integration of competition elements, hands-on experience, and real-world scenario simulation is able to significantly increase students' cybersecurity awareness. This model not only provides a more engaging learning approach, but is also capable of generating resilient and sustainable digital behavior change. As such, this research offers a significant theoretical and practical contribution to the field of cybersecurity education, while providing a solid foundation for the development of gamification-based learning strategies in the future.

CONCLUSION

This study concludes that the application of gamification in cybersecurity training modules has been proven to be able to increase students' understanding, motivation, and resilience to various forms of cyber threats, especially social engineering attacks such as phishing and social engineering. The integration of gamification elements such as points & XP, levels, badges, leaderboards, mini-games, and scenario-based simulations is able to create a more interactive and immersive learning experience compared to traditional learning methods that tend to be passive and theoretical. These results show that a game-based pedagogical approach not only increases user engagement, but also strengthens knowledge transfer in the context of real-world situations. The measurement data showed a significant increase in cybersecurity knowledge before and after taking part in the training module. Students showed increased accuracy in recognizing phishing emails, understanding threat patterns, and applying appropriate mitigation measures after interacting with gamification scenarios. Additionally, competitive components such as leaderboards have been shown to encourage intrinsic motivation and a deeper desire to learn, without creating excessive pressure.

Instant feedback systems also play an important role in improving user behavior. Participants can immediately find out the mistakes in the decision-making process, understand the reasons, and improve strategies

in the next challenge. This approach accelerates the mental formation of models related to real-world threats, while strengthening long-term retention of learning materials.

The findings of this study confirm that gamification can function not only as an entertainment tool, but also as an effective pedagogical strategy in cybersecurity literacy at the university level. Gamification-based curriculum is able to answer the problem of low digital security awareness which has been a challenge in various higher education institutions. This improvement in learning outcomes also strengthens the argument that gamification has the potential to become a new standard in the development of cybersecurity modules in the future. Theoretically, this study expands the understanding of the integration of Self-Determination Theory and Behavioral Learning principles into the context of digital security, showing that psychological satisfaction (competence, autonomy, and connectedness) can be optimized through appropriate gamification design. Practically, this research offers a gamification module development model that can be adopted by other universities to improve students' digital security.

However, the study still has some limitations, such as the limited sample coverage of one institution and the relatively short duration of use of the module. Further research is suggested to expand the scale of implementation, add adaptive elements in gamification systems, as well as evaluate its long-term impact on changing students' digital security habits. Overall, it can be concluded that the application of gamification in cybersecurity training is an effective, relevant, and has great potential to be widely implemented as a strategy to increase digital literacy in the era of increasing cyber threats. This module not only improves students' defensive skills, but also builds a security awareness culture that is needed in the modern digital ecosystem.

REFERENCES

AlBloush, M., Aloul, F., & Zemerly, M. (2020). Gamified phishing awareness training: A user-centered approach. Computers & Security, 97, 101962. https://doi.org/10.1016/j.cose.2020.101962

Alotaibi, M., Furnell, S., & Stengel, I. (2023). Gamification for cybersecurity awareness: A systematic literature review. Computers & Security, 128, 103142. https://doi.org/10.1016/j.cose.2023.103142

Arachchilage, N. A. G., & Love, S. (2021). A game design framework for avoiding malicious IT threats. Information & Computer Security, 29(3), 409–427. https://doi.org/10.1108/ICS-03-2021-0041

Fernandes, B., Barros, P., & Moreira, F. (2021). Gamified learning for cybersecurity education: Trends and challenges. Journal of Computer Assisted Learning, 37(6), 1706–1721. https://doi.org/10.1111/jcal.12601

Fischer, F., Buchta, C., & Breitinger, F. (2023). Gamified social engineering simulation to improve cybersecurity awareness: A field experiment. Computers & Security, 130, 103200. https://doi.org/10.1016/j.cose.2023.103200

Hamid, N. A., Rahim, N. A., & Satar, N. S. M. (2022). Password security awareness enhancement using gamified mobile learning applications. International Journal of Human–Computer Interaction, 38(12), 1100–1115. https://doi.org/10.1080/10447318.2021.1967112

Hidayat, M., & Nurdin, N. (2023). Digital literacy and cybersecurity awareness in Indonesian universities: A case analysis. Journal of Applied Information Technology, 7(2), 55–70. https://doi.org/10.48009/2_2023

Johnson, D., & Weng, G. (2021). Evaluating the effectiveness of traditional vs. gamified cybersecurity training. Journal of Cybersecurity Education, Research & Practice, 5(1), 1–18.

Loni, M., Nafria, A., & Aghakhani, H. (2022). User engagement in cybersecurity awareness platforms: A behavioral analysis. Computers in Human Behavior Reports, 6, 100209. https://doi.org/10.1016/j.chbr.2022.100209

Othman, M., Kassim, E., & Jabar, M. (2023). Game-based learning for cybersecurity: Features influencing students' motivation. Education

and Information Technologies, 28(4), 5123–5141. https://doi.org/10.1007/s10639-022-11357-4

Park, S., & Lee, Y. (2021). Cybersecurity risks in higher education institutions: A survey of students' behaviors and awareness. Security Journal, 34(3), 210–225. https://doi.org/10.1057/s41284-020-00269-3

Pham, L., & Doan, T. (2021). Motivation factors in gamified learning: A meta-analysis. Journal of Educational Computing Research, 59(7), 1241–1265. https://doi.org/10.1177/07356331211023567

Pratama, B. Y., & Raharjo, B. (2023). Gamification approach for network security learning in higher education. International Journal of Emerging Technologies in Learning, 18(5), 205–220. https://doi.org/10.3991/ijet.v18i05.38921

Rahman, M., & Lau, S. (2023). Perceptions of interactive learning among Gen-Z students: Implications for cybersecurity education. Education Sciences, 13(2), 121. https://doi.org/10.3390/educsci13020121

Ribeiro, S., & Silva, R. (2022). Gamified approaches for personal data protection awareness training. Journal of Information Security and Applications, 65, 103100. https://doi.org/10.1016/j.jisa.2022.103100

Santos, M., & Correia, M. (2021). Behavioral change in cybersecurity awareness programs: A systematic review. Computers & Security, 104, 102215. https://doi.org/10.1016/j.cose.2021.102215

Sarikaya, M., & Cagiltay, N. (2022). Gamification in cybersecurity training: A comprehensive review. Computers in Human Behavior, 136, 107394. https://doi.org/10.1016/j.chb.2022.107394

Smith, J., Roberts, M., & Chen, T. (2022). Understanding student vulnerability to cyber threats in digital campuses. Journal of Cybersecurity, 8(1), 1–13. https://doi.org/10.1093/cybsec/tyac002

Suh, A., & Wagner, C. (2020). Gamification in information security training: A systematic review. Computers & Security, 95, 101795. https://doi.org/10.1016/j.cose.2020.101795

Zhou, X., & Kim, H. (2022). Ransomware attacks in the education sector: Patterns and implications. Information Systems Frontiers, 24(6), 1681–1698. https://doi.org/10.1007/s10796-021-10218-3