

Gamification on Cybersecurity Awareness Training for Adolescents: A Systematic Literature Review

Andang Wijanarko
Department of Information Systems
Universitas Bengkulu
Indonesia
andang@unib.ac.id

Aan Erlanshari
Department of Information Systems
Universitas Bengkulu
Indonesia
aan_erlansari@unib.ac.id

Abstract—This systematic literature review aims to synthesize empirical evidence on the effectiveness, gamification elements, and implementation challenges of gamification in cybersecurity awareness training for adolescents. This study follows the PRISMA guidelines with a literature search on the Scopus academic database. Of the 124 studies identified, 14 studies met the inclusion criteria for further analysis. The synthesis results show that gamification significantly increases engagement, intrinsic motivation, and knowledge retention among adolescents on the topic of cybersecurity. The most effective gamification elements are points, badges, and leaderboards (PBL). However, key challenges such as framework usage, ensuring long-term engagement, and integration between game mechanics and learning outcomes must be considered for future research.

Keywords— Gamification, Cybersecurity, Cybersecurity Awareness, Adolescent, PRISMA.

I. INTRODUCTION

The digital world has become an integral part of the daily lives of modern adolescents. This generation, which has grown up as digital natives, uses the internet as their primary space for learning, socializing, accessing entertainment, and forming their identity. Recent surveys indicate that adolescents spend an average of 6-8 hours per day in the digital world, with usage intensity increasing post-pandemic [1]. However, behind the convenience and connectivity it offers, the digital space also harbors the complexity of evolving cybersecurity threats.

Today's adolescents face a variety of sophisticated cybersecurity risks, ranging from phishing that is increasingly difficult to distinguish from legitimate communication and cyberbullying that affects mental health to digital identity theft and massive data privacy violations [1]. Worryingly, adolescents' vulnerability to these threats stems not only from their lack of experience but also from neurocognitive developmental factors specific to adolescence. The adolescent period is characterized by a tendency towards risk-taking behavior and a perception of invulnerability, which often leads adolescents to ignore the potential consequences of their actions in the digital world [2], [3]. In addition, the immature development of the prefrontal cortex affects their ability to assess risks and make appropriate decisions in complex situations [2], [3].

Efforts to raise cybersecurity awareness through traditional training methods—such as one-way seminars, static text-based modules, or monotonous video presentations—have proven increasingly ineffective in reaching the teenage population [4], [5], [6]. These methods fail to capture the learning characteristics of the digital native

generation, who are more stimulated by visual, interactive, and reward-based content [4], [5], [6]. More than just being considered boring, these conventional approaches are deemed irrelevant to the dynamic and personal digital ecosystem of adolescents. As a result, knowledge conveyed through traditional methods has low retention and fails to transform into safer internet behavior [4], [5], [6].

In this context, gamification offers an innovative solution. Gamification is defined as the application of game elements and game design in non-game contexts [7]. The aim is to increase user motivation, engagement, and participation. In education, gamification has been proven to improve learning outcomes in various fields [8].

Although interest in gamification in cybersecurity training has been increasing, there have been few systematic literature reviews specifically focusing on the adolescent population. Most existing reviews are more general in nature or focus on adults in corporate environments. In addition, many reviews also focus on student populations in the field of education. Therefore, this Systematic Literature Review (SLR) was conducted to consolidate existing empirical findings on the application of gamification for cybersecurity awareness training among adolescents.

This study will answer the following research questions (RQs):

RQ1: How effective is gamification in improving adolescent knowledge, attitudes, and safe cyber behavior?

RQ2: What gamification elements are most commonly and effectively used in this context?

RQ3: What are the challenges and opportunities in applying gamification to cybersecurity awareness training for adolescents?

II. METHODOLOGY

A systematic and comprehensive literature search was conducted to identify all relevant studies discussing the application of gamification in cybersecurity awareness training for adolescents. This process was designed to minimize publication bias and ensure the widest possible coverage of the existing literature. This literature review was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a transparent, systematic, and replicable process [9], [10].

A. Search Strategy

The publication time frame was set from January 2020 to October 2025. This time limit was applied to ensure that this literature review only covered findings that were up-to-date and relevant to the latest developments in gamification technology and the cybersecurity threat landscape.

Keywords were developed taking into account the variety of terminology used in the literature. The main search strings were developed using Boolean operators (AND, OR) to combine the core concepts of this study, namely:

- Concept 1: Gamification -> ("gamification" OR "gamify" OR "gamified")
- Concept 2: Cybersecurity Awareness -> ("cybersecurity awareness training")
- Concept 3: Adolescent Population -> ("adolescent" OR "teen" OR "youth" OR "young people")

The combination of keywords used was as follows: ("gamification" OR "gamify" OR "gamified") AND ("cybersecurity awareness training") AND ("adolescent" OR "teen" OR "youth" OR "young").

B. Inclusion and Exclusion Criteria

The inclusion and exclusion criteria were considered during the research selection process to identify relevant studies that aligned with the study's aim. The criteria for selecting primary studies were shown in Table 1.

Table 1. Inclusion and exclusion criteria
(Source: Author's concept)

No.	Inclusion Criteria
1	Articles written in English
2	Articles released between 2020 and 2025
3	Articles published in the field of Computer Science
4	Articles published in open access
No.	Exclusion Criteria
1.	Books, book reviews, conference proceedings, editorial material
2	Duplicated studies

C. Selection Criteria

The selection process was conducted in three stages, as illustrated in the PRISMA diagram below. First, all search results were collected, and duplicates were removed. Second, researchers evaluated the titles and abstracts based on inclusion and exclusion criteria. Finally, full-text articles that passed the second stage were reassessed for eligibility. This process was carried out by two researchers independently to avoid bias, and any differences are resolved through discussion.

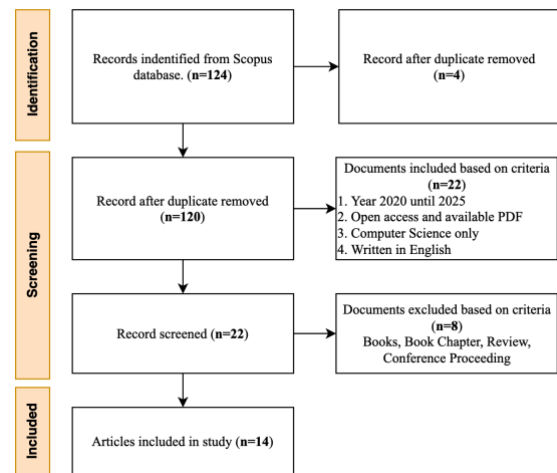


Figure 1. PRISMA flowchart

A systematic literature search was conducted in the Scopus database, resulting in the identification of 124 initial records. After checking for duplicates, 4 records were identified as duplicates and deleted, leaving 120 records to proceed to the screening stage. From the 120 available records, screening was carried out based on the established inclusion criteria: publication year 2020 to 2025, open access and PDF available, only in the field of computer science, and written in English. After the screening process, 22 articles met the criteria and proceeded to the eligibility assessment stage. The 22 articles were then assessed in depth based on their eligibility. From this process, 8 documents were excluded because they were books, book chapters, review articles, and conference proceedings. Subsequently, 14 articles finally met all eligibility criteria.

Although the selection process was conducted rigorously using clear criteria, it must be acknowledged that there were several limitations to this process. First, the search was only conducted in one database (Scopus), which meant that relevant studies from other databases may have been overlooked. Second, the restriction to open access articles may have resulted in some high-quality studies that are not openly available being excluded from this review.

Nevertheless, this systematic selection process has successfully identified 14 studies that are most relevant to the topic of gamification in cybersecurity awareness training for adolescents, which will be analyzed in depth in the results and discussion section.

This process ensures that the included studies are truly representative and meet the established quality standards so that the synthesized results of this systematic literature review are scientifically accountable.

D. Data Extraction

Data from each included study were extracted into a standardized template. The variables extracted included author and year, study design, participant characteristics, gamification intervention (elements used), outcomes measured (knowledge, engagement, and behavior), and key findings. Data analysis was conducted using narrative synthesis to synthesize findings and answer research questions.

III. RESULTS AND DISCUSSIONS

A total of 14 empirical studies met the inclusion criteria. The majority of studies used quantitative research designs. Participants in the studies described in the given context were mostly young adults, with ages generally ranging from adolescents to early thirties. Although some studies covered a wider age range, the majority of participants were in the younger age group. The intervention platforms used varied, ranging from web applications and mobile apps to games.

A. Research Question 1 (RQ1)

How effective is gamification in improving adolescents' knowledge, attitudes, and safe cyber behavior?

Gamification shows considerable promise in enhancing cybersecurity education, training, and awareness, particularly for students, by making the learning process more engaging and enjoyable compared to traditional methods [11], [12]. While its effectiveness is not universally guaranteed and depends on various factors, studies consistently affirm its positive impact on several key areas [12], [13], [14].

1. Enhancing Knowledge and Comprehension

Gamification has been shown to increase knowledge and improve the comprehension of cybersecurity concepts. In addition, specific frameworks, like Cyber-Hero, have demonstrated measurable results in cybersecurity awareness training for high school students [13]. Subsequently, an interactive video game, Cyber Shield, resulted in a 51.4% increase in workers' cybersecurity awareness across various topics, including password complexity, social engineering, phishing assaults, and physical security, indicating its potential for knowledge transfer [15].

The implementation of gamification in cybersecurity awareness training has been proven to significantly improve knowledge mastery and conceptual understanding among adolescents. Empirical studies show that the gamification approach is not only successful in transferring information but also in building a comprehensive understanding of various aspects of cybersecurity [12], [13], [16], [17], [18].

Gamification mechanisms serve as catalysts in the learning process through several approaches. First, elements such as progress bars, levels, and badges create a step-by-step learning structure that makes it easier for adolescents to systematically digest complex cybersecurity concepts. Second, the immediate feedback system integrated into the gamification design allows participants to immediately correct misunderstandings and reinforce correct understanding [11], [18].

This evidence of effectiveness can be observed in the application of the Cyber-Hero framework, which is specifically designed for secondary school students [13]. This framework not only presents cybersecurity content in an engaging format but also integrates reward and challenge mechanisms that are tailored to the developmental characteristics of adolescents. Evaluation results show a marked improvement in participants' conceptual understanding and practical ability to identify cybersecurity threats.

Furthermore, a study on the interactive video game Cyber Shield revealed quite astonishing results [15]. Its implementation among workers showed a 51.4% increase in

cybersecurity awareness across various critical topics, including password complexity, social engineering, phishing attacks, and physical security. These findings indicate the strong potential for knowledge transfer through gamification, which can be adapted for adolescent populations.

The learning process through gamification also facilitates better contextual understanding. Unlike traditional lecture methods, which tend to be abstract, gamification presents real-life scenarios in a controlled environment [13], [19]. Young people not only learn theory but also experience firsthand the consequences of their actions in simulations, thereby building a deeper understanding of cause-effect relationships in cybersecurity practices.

Thus, gamification not only improves test scores but, more importantly, builds a strong cognitive foundation for a comprehensive conceptual understanding of cybersecurity, which can ultimately translate into safer behavior when interacting in the digital world.

2. Impact on Attitudes and Engagement

Gamification introduces elements of fun and interactivity, making learning more captivating and enjoyable for participants [13], [19], [20], [21], [22], [23]. For example, in the context of students, including those in secondary school, they often cite fun and enjoyment as reasons why gamification positively affects the learning process in cyber ranges [11], [16], [17]. In addition, the studies have shown that gamification effectively enhances engagement and interest in cybersecurity awareness [13], [24]. Therefore, gamification is a valuable strategy for improving motivation in cybersecurity education [12].

The application of gamification in cybersecurity awareness training brings a new dimension to shaping the attitudes and engagement levels of learners. The game elements introduced not only add fun and interactivity but also fundamentally change learners' perceptions of the learning process, which was previously considered monotonous, into an exciting and engaging experience [13], [19], [20], [21], [22], [23].

In the context of learners, including secondary school students, gamification successfully creates a learning environment that is free from pressure but still challenging. Field studies show that students consistently cite fun and enjoyment as the main reasons why gamification has a positive impact on the learning process, especially in cyber ranges [11], [16], [17]. This element of fun is not merely entertainment but serves as a catalyst that facilitates better acceptance of the material and forms positive associations with the topic of cyber security.

Empirical evidence from various studies shows that gamification is not only effective in increasing interest and engagement in cybersecurity awareness [13], [24], but also successfully builds sustainable intrinsic motivation. Participants who were initially involved due to external factors (such as tasks or obligations) gradually developed a genuine interest in cybersecurity material.

Therefore, gamification has proven to be a valuable strategy for increasing motivation in cybersecurity education [12]. This approach not only changes attitudes temporarily but also has the potential to shape a long-lasting cybersecurity

mindset. By creating a positive and engaging learning experience, gamification instills the values of cyber awareness as part of natural digital habits, rather than simply obligations that must be obeyed.

This transformation in attitudes and increased engagement is a critical foundation for building a strong cybersecurity culture among the younger generation, which will ultimately contribute to a safer and more secure digital ecosystem.

3. *Promoting Safe Cyber Behavior*

Previous studies have consistently highlighted the effectiveness of gamification in promoting positive behavioral change in the cyber realm [24]. This approach does not merely focus on knowledge transfer but successfully penetrates the level of behavioral change by placing strong emphasis on motivation as the main driver [13]. Gamification has great potential to encourage behavioral transformation through its three main pillars: increased motivation, optimized engagement, and practical skills development [13].

The process of behavioral change through gamification occurs in several interrelated stages. First, gamification creates a safe practice environment where young people can directly experience the consequences of their actions without having to bear the actual risks. This experiential learning enables the formation of digital muscle memory that will carry over into everyday internet behavior [15], [18].

Second, the immediate feedback system integrated into the gamification design provides real-time behavioral correction. When an adolescent makes a mistake in the simulation, such as choosing a weak password or falling for a phishing scheme, instant feedback helps them immediately understand the impact of their actions and how to correct them [15], [18].

Third, progression dynamics in gamification, such as leveling systems and mastery challenges, encourage adolescents to continue honing their cybersecurity skills. Each level successfully completed represents not only cognitive achievement but also behavioral proficiency in applying safe internet practices [15], [18].

In summary, gamification is a very promising approach to improving adolescents' cybersecurity knowledge, fostering positive attitudes, and encouraging safe internet behavior thanks to its ability to increase engagement, motivation, and understanding through interactive and enjoyable learning experiences. The resulting transformation is not merely superficial change but the formation of a safe and responsible digital culture among the younger generation.

The key to success lies in a user-centered design approach, a deep understanding of adolescent psychology, and seamless integration between game elements and substantive educational content. With proper execution, gamification not only teaches young people about cybersecurity but also shapes them into resilient digital citizens who are responsive to today's cyber challenges.

B. *Research Question 2 (RQ2)*

What gamification elements are most commonly and effectively used in this context?

Gamification, defined as the integration of game-like elements and interactive activities, is recognized as an educational method that can provide motivation, mental

relaxation, and habit reinforcement to learners [13]. These elements offer visible indicators of effort, motivating progress in learning journeys.

Gamified elements consistently yield measurable results, such as increased knowledge, improved engagement, and behavior changes, effectively aligning with specific learning goals [13]. By intentionally incorporating game elements that fulfill needs for autonomy, competence, and relatedness, gamification influences motivation, leading to desired outcomes like improved learning, productivity, participation, and behavior change [12].

Specific elements identified as effective in increasing motivation, engagement, and information retention among students include points, badges, and leaderboards (PBL) [15].

Additionally, competitive elements such as leaderboards, team-based competitions, challenges, and time pressure have been associated with increased engagement, motivation, and short-term participation [13].

While many elements show positive impacts, some gamification elements have demonstrated context-dependent and sometimes contradictory effects [12]. Researchers and practitioners are advised to apply certain game elements with caution, as studies have often failed to assess their potential negative effects [12], [13]. Elements recommended for cautious application include [12]:

1. Leaderboards
2. Competition
3. Time pressure
4. Narratives
5. Challenges
6. Points
7. Extrinsic rewards

Future research should aim to report both the benefits and negative effects of game elements, considering context and participant demographics, to contribute to more inclusive and adaptive gamified initiatives [12].

In summary, while a wide array of gamification elements are commonly used and can be effective in boosting engagement and learning outcomes, competitive elements, points, badges, and leaderboards are frequently cited for their positive impact. However, a nuanced approach is necessary, as several elements, including points, leaderboards, and competitive aspects, also warrant cautious application due to their context-dependent nature and potential for negative effects.

C. *Research Question 3 (RQ3)*

What are the challenges and opportunities in applying gamification to cybersecurity awareness training for adolescents?

Applying gamification to cybersecurity awareness training for adolescents presents both unique challenges and significant opportunities. Gamification offers a way to make a traditionally dull subject engaging, but its effective implementation requires addressing several gaps.

1. Opportunity

a. Enhanced Engagement and Enjoyment

Gamification introduces elements of fun and interactivity that create a fundamental transformation in the learning experience. For adolescents who find traditional methods uninteresting, this approach successfully changes negative perceptions into positive engagement [13]. Game-based learning mechanisms utilize the natural psychological principles of adolescents to play and explore, thereby creating a learning environment that does not feel like formal learning but remains substantive.

More than just making the learning process enjoyable, gamification can influence early behavioral change by emphasizing intrinsic and extrinsic motivation [13]. Structured reward systems, visual progress tracking, and challenges tailored to ability levels create psychological incentives to stay engaged and internalize learning material.

b. Improved Learning and Knowledge Retention

Empirical evidence shows that gamification is effective in fostering participant engagement and knowledge retention [15]. Through spaced repetition mechanisms disguised as levels and repeated challenges, cybersecurity knowledge is not only understood cognitively but also embedded in long-term memory.

Gamification has proven to be a valuable strategy for increasing cybersecurity awareness and making the learning experience more engaging [13]. This approach allows young people to directly experience the consequences of their actions in a safe environment, thereby building a more contextual and applicable understanding. Scenario-based learning simulations in a gamified format help transfer theoretical knowledge into practical competencies that are ready to be applied in real-life situations.

c. Proven Effectiveness with Adolescents

Specialized frameworks such as Cyber-Hero have demonstrated measurable results when used for information security awareness and training targeted at secondary school students [13]. The successful implementation of this framework proves that, with a design tailored to the characteristics of adolescent development, gamification can be a highly effective tool.

Several key factors that make gamification effective for adolescents include:

- 1) The ability to adapt to the learning preferences of the digital native generation
- 2) Flexibility in presenting content that is relevant to the digital world of adolescents
- 3) The capacity to provide immediate feedback, which is much needed in the adolescent learning process
- 4) The ability to create experiential learning without facing real risks

2. Challenge

a. Lack of Specific Targeting

Previous studies have often examined gamification in general without specifically targeting individuals based on different educational backgrounds [13]. This one-size-fits-all

approach limits our understanding of how gamification can actually improve learning for specific groups such as adolescents. The unique developmental characteristics of adolescents—including cognitive patterns, motivation, learning preferences, and emotional maturity levels—require a different design approach than other populations.

Without proper segmentation, gamification risks failing to address the pain points actually experienced by adolescents in the context of cybersecurity. Effective game design elements for university students or adult professionals may be irrelevant or even counterproductive when applied to secondary school students. This gap requires more in-depth research on better-defined adolescent personas based on age, socio-economic background, and level of technological literacy.

b. Absence of Theoretical Framework:

There is a significant gap in the lack of an established theoretical framework specifically designed to integrate game design elements into cybersecurity awareness programs [13]. Many gamification implementations are ad hoc and not supported by a strong theoretical foundation from the fields of educational psychology, game theory, or cognitive science.

The development of a comprehensive framework must consider the integration of adult learning theory (andragogy) and child learning theory (pedagogy), given that adolescents are in a transitional phase between the two approaches.

c. Ensuring Long-Term Engagement

A critical limitation is ensuring long-term engagement rather than just short-term participation. Without addressing these temporal dynamics, gamified solutions may fail to deliver lasting motivation and undermine the objective of sustained awareness [12].

d. Unclear Connection to Learning Goals

While various interactive gamification elements are used to motivate participants, their direct connection to achieving specific learning goals in cybersecurity awareness programs remains unclear [12].

Overall, gamification does show great potential in transforming cybersecurity awareness training for adolescents from monotonous material into an interactive and engaging learning experience. However, the full realization of this potential is still hampered by several fundamental challenges that require a more strategic approach.

Although gamification has been proven to increase engagement and motivation in the short term, its long-term effectiveness still requires more targeted development. Future research needs to be more specific in targeting the unique characteristics of adolescents by considering aspects of cognitive development, cultural background, and diverse digital learning preferences.

There is also a need to develop a comprehensive theoretical framework that integrates principles from developmental psychology, learning theory, and game design. This framework will be an important foundation for designing gamification interventions that are not only attractive but also pedagogically sound.

Equally important is the need for a closer alignment between game mechanics and specific learning outcomes. Each element of gamification must have a clear correlation

with measurable improvements in knowledge, attitude changes, and improvements in cybersecurity behavior.

To achieve this, an adolescent-centered design approach is key, whereby young people are actively involved in the process of designing solutions. Integration with other learning methods and the development of a comprehensive evaluation system will create a more effective and sustainable learning ecosystem.

By addressing these challenges through a systematic approach, gamification will not only become an effective educational tool but can also serve as a catalyst in shaping a generation of digital citizens who are more resilient and responsible in facing the ever-evolving landscape of cyber threats.

IV. CONCLUSION

Based on a synthesis of 14 empirical studies that have been analyzed, it can be concluded that gamification is a highly effective approach with great potential for improving the quality of cybersecurity awareness training for adolescents. The success of this approach lies primarily in its proven ability to increase learning engagement, motivate active participation, and strengthen knowledge retention among adolescents.

Gamification elements such as points, badges, and leaderboards (PBL) have proven to be the most popular and positively impactful mechanisms in increasing participants' intrinsic and extrinsic motivation. However, behind this success, the implementation of gamification also faces complex challenges that need to be overcome. Game design elements that are overly focused on competition can potentially cause anxiety and pressure among participants who lack confidence, while improper integration of game mechanisms with learning materials risks distracting attention from essential educational content.

For future research and development, this field still faces several significant limitations. More studies are needed that focus on the specific developmental characteristics of adolescents, given that this population has unique learning needs and preferences compared to other age groups. The development of a comprehensive theoretical framework is also urgently needed to provide a strong conceptual foundation for designing effective gamification interventions.

Equally important is the need to build stronger connections between game mechanics and specific learning objectives. Each element of gamification must be designed to directly support the achievement of the desired cybersecurity competencies, rather than merely being a decoration that adds excitement without educational meaning. By overcoming these challenges, gamification will not only be an effective tool for cybersecurity awareness education but can also contribute to shaping a sustainable digital security culture among the younger generation.

Going forward, the success of gamification implementation in the context of cybersecurity education for adolescents will greatly depend on a holistic design approach that considers the psychological aspects of adolescent development, the learning characteristics of the digital native generation, and the social interaction dynamics unique to this age group. Thus, gamification can fully realize its potential as

a transformative educational approach that is relevant to the times and effective in shaping safe internet behavior.

REFERENCES

- [1] Dr. S. G. Dhawad, "Cybercrime in the Era of Social Media and the Digital Age: Threats, Challenges, Societal Implications, and Preventive Strategies," *Gurukul International Multidisciplinary Research Journal*, Apr. 2025, doi: 10.69758/GIMRJ/250313IIVXIIIP0037.
- [2] R. M. MacHado Fernandes, L. F. Rust Da Costa Carmo, and C. L. Rebello Da Motta, "A taxonomy proposal of cyber threats involving children and adolescents," *2022 17th Latin American Conference on Learning Technologies, LACLO 2022*, pp. 01–08, Oct. 2022, doi: 10.1109/LACLO56648.2022.10013466.
- [3] V. Nakta and E. Sood, "The Vulnerability of Children in Cyberspace," *Handbook of Research on Cyber Law, Data Protection, and Privacy*, pp. 313–331, Jan. 2022, doi: 10.4018/978-1-7998-8641-9.CH019.
- [4] G. Tempestini, S. Merà, M. Pietro Palange, A. Bucciarelli, and F. Di Nocera, "Improving the Cybersecurity Awareness of Young Adults through a Game-Based Informal Learning Strategy," *Information*, vol. 15, no. 10, pp. 607–607, Oct. 2024, doi: 10.3390/INFO15100607.
- [5] R. Al-Kuwari, "Enhancing Cybersecurity Awareness Training for Mitigating Human-Induced Cybersecurity Breaches," *International Journal of Engineering and Computer Science*, vol. 13, no. 10, pp. 26498–26503, Oct. 2024, doi: 10.18535/IJECS/V13I10.4917.
- [6] Diana Ussher-Eke, "From awareness to action: Designing effective cybersecurity training programs," *International Journal of Science and Research Archive*, vol. 16, no. 2, pp. 494–504, Aug. 2025, doi: 10.30574/IJSRA.2025.16.2.2348.
- [7] N. Danilina, "Gamification As A New Interpretation Of The Game In The Digital Economy: Theoretical And Practical Rationale," *Obščestvo i ekonomika*, no. 12, pp. 104–104, Jan. 2022, doi: 10.31857/S020736760023431-3.
- [8] M. Ahmad and R. W. Khan, "Gamification in Education: Enhancing the Students Engagement and Learning Achievements through the Integration Use of Game based Learning," *The eKnowledge*, vol. 3, no. 1, pp. 23–37, Nov. 2024, doi: 10.63062/TK/2K24A.31016.
- [9] L. Hijriyah, A. Alias, and M. F. Mohd Sahabuddin, "Exploring walkability research trends based on systematic literature review (SLR) by applying PRISMA," *Open House International*, vol. 49, no. 1, pp. 63–121, May 2023, doi: 10.1108/OHI-02-2023-0031.
- [10] B. Kitchenham and S. M. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," 2007. [Online]. Available: <https://www.researchgate.net/publication/302924724>
- [11] W. Lazarov *et al.*, "Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education," *Technology, Knowledge and Learning*, 2025, doi: 10.1007/s10758-025-09840-y.
- [12] A. K. Gwenthure and S. Nam, "GAMIFIED CYBERSECURITY INITIATIVES: THE TREND, LIMITS, AND LESSONS," *Journal of Information Technology Education: Research*, vol. 24, pp. 1–34, 2025, doi: 10.28945/5601.

- [13] A. K. Gwenthure and F. S. Rahayu, "Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review," *International Journal of Serious Games*, vol. 11, no. 1, pp. 83–99, 2024, doi: 10.17083/ijsg.v11i1.719.
- [14] K. Khadka and A. B. Ullah, "Human factors in cybersecurity: an interdisciplinary review and framework proposal," *Int J Inf Secur*, vol. 24, no. 3, 2025, doi: 10.1007/s10207-025-01032-0.
- [15] H. Taherdoost, "Towards an Innovative Model for Cybersecurity Awareness Training," *Information (Switzerland)*, vol. 15, no. 9, 2024, doi: 10.3390/info15090512.
- [16] T. Keller, J. Guggemos, and J. Warwas, "Digital educational escape rooms as a novel approach to cybersecurity education: An empirical study on learner perceptions of usefulness and usability," *Computers in Human Behavior Reports*, vol. 20, 2025, doi: 10.1016/j.chbr.2025.100785.
- [17] E. T. Al-Shammari, "Integrating Protection Motivation Theory With Cultural Context: A Framework for Cybersecurity Education," *Journal of Cases on Information Technology*, vol. 27, no. 1, 2025, doi: 10.4018/JCIT.368146.
- [18] G. Tempestini, S. Merà, M. P. Palange, A. Bucciarelli, and F. Di Nocera, "Improving the Cybersecurity Awareness of Young Adults through a Game-Based Informal Learning Strategy," *Information (Switzerland)*, vol. 15, no. 10, 2024, doi: 10.3390/info15100607.
- [19] T. van Steen and J. R. A. Deeleman, "Successful Gamification of Cybersecurity Training," *Cyberpsychol Behav Soc Netw*, vol. 24, no. 9, pp. 593–598, 2021, doi: 10.1089/cyber.2020.0526.
- [20] H. Alqahtani and M. Kavakli, "Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)," *Information (Switzerland)*, vol. 11, no. 2, 2020, doi: 10.3390/info11020121.
- [21] T. Georgiou, L. Baillie, O. Chatzifoti, and S. C. Chan, "Future forums: A methodology for exploring, gamifying, and raising security awareness of code-citizens," *International Journal of Human Computer Studies*, vol. 169, 2023, doi: 10.1016/j.ijhcs.2022.102930.
- [22] M. T. Parvez, A. M. Alsuhibani, and A. H. Alamri, "Educational and Cybersecurity Applications of an Arabic CAPTCHA Gamification System," *Ingenierie des Systemes d'Information*, vol. 28, no. 5, pp. 1275–1285, 2023, doi: 10.18280/isi.280516.
- [23] T. M. Tran, R. Beuran, and S. Shinobu Hasegawa, "Gamification-Based Cybersecurity Awareness Course for Self-regulated Learning," *International Journal of Information and Education Technology*, vol. 13, no. 4, pp. 724–730, 2023, doi: 10.18178/ijiet.2023.13.4.1859.
- [24] C. Moumouh, J. A. García-Berná, M. Y. Chkouri, and J. L. Fernández-Alemán, "Serious Games to Improve Privacy and Security Knowledge for Professionals: a Systematic Literature Review," *International Journal of Serious Games*, vol. 12, no. 1, pp. 3–24, 2025, doi: 10.17083/ijsg.v12i1.825.