Analyzing the Design and Impact of Digital Serious Games in Digital Security: Challenges and Emerging Trends

Lucas de O. Fratus[1], **Felippe F. da Silva**[1], **Alisson R. Svaigen**[1]

[1]Department of Informatics – State University of Maringa (UEM)
Maringa – PR – Brasil

{lucasdeoliveirafratus, felippefernandes10}@gmail.com, arsvaigen@uem.br

Abstract. Introduction: *Over the years, cybercrimes have increasingly affected society. The development of digital serious games (SGs) has been explored as assistant tools to raise awareness about digital security. However, there is a lack of studies that analyze the scientific rigor of such games in a comprehensive manner.* ***Objective:*** *Analyze the design and impact of digital SGs in the context of digital security through a systematic literature review (SLR).* ***Methodology****: We developed and applied an SLR protocol to summarize and analyze recent developments of SGs in this context, focusing on the challenges and emerging trends.* ***Results:*** *Our main results are twofold: from the SLR, we raise five fundamental challenges and three main trends in this research area; and we propose a set of guidelines for the development of digital SGs in digital security.*
Keywords *Digital Security, Serious Games, Systematic Literature Review, Digital Crimes*

1. Introduction

On the last decades, technological devices and social networks have become omnipresent in the daily life of society. Although this popularization has contributed to informing and bringing people closer, it has increased the challenges related to digital security [Ng e Hasan 2025]. Different aspects (e.g., data protection, safe use of online platforms, and safe virtual behavior) have emerged as major challenges of awareness, both for tech companies and public authorities. In the Brazilian context, 24% of Brazilians suffered from cybercrimes in 2024 [DataSenado 2024]. In 2025, the Federal Police carried out 1241 operations countering cybercrimes across the country, resulting in 502 arrests and 1512 search and seizure warrants [Polícia Federal 2025]. These data highlight the deep impact of cybercrimes in the country and, therefore, in society, reinforcing the need for educational actions aimed at raising public awareness about digital security.

Over the years, educational initiatives focused on digital security awareness have emerged, mainly due to their potential to promote the safe use of digital technology [Ahmed et al. 2024]. In this context, the development of digital serious games (SGs) has been explored as assistant tools, engaging people, stimulating reasoning and problem-solving. Commonly, digital security-related SGs are designed for a specific target audience [Abu-Amara e Tamimi 2021, Berisford et al. 2022]. However, cybercrimes affect different age groups equally. Furthermore, there is a lack of studies that analyze the scientific rigor of the proposed games. Considering this scenario, this study is guided by the following question: *How have digital serious games been designed, evaluated, and made available to promote digital security awareness, and what challenges, trends, and guidelines can be derived from the literature?*

Table 1. Summarization of the Related Studies

Reference	Main Scope	Type of Analysis			Propose Guidelines?
		Genre/platform	Audience profile	Evaluation approach	
[Hill Jr et al. 2020]	Cybersecurity SGs	◐	◐		No
[Coenraad et al. 2020]	General Cybersecurity games	●	◐	◐	No
[Ahmed et al. 2024]	Online cybersecurity courses	◐		◐	No
[Luccas et al. 2025]	SGs in higher education	◐		●	No
[Ng e Hasan 2025]	Cybersecurity SGs	◐			No
Ours	**Cybersecurity SGs**	●	●	●	**Yes**

Bearing these questions in mind, the main goal of this study is to analyze the design and impact of digital SGs in the context of digital security. To address this goal, we carry out a systematic literature review (SLR) to summarize the recent developments of SGs in this context. This study provides a comprehensive overview of the current state of digital serious games for digital security by systematically analyzing their design, implementation, and evaluation. Based on this analysis, we identify key research gaps, discuss emerging trends, and derive practical guidelines to support future research and game development in this domain.

This paper is organized as follows: Section 2 discusses the related studies to our SLR; Section 3 describes the SLR protocol; Section 4 presents the results obtained from the SLR, providing a comprehensive discussion addressing the research questions involved in this study; Section 5 presents the proposed guidelines; finally, our final remarks and future directions are presented in Section 6.

2. Related Studies

In this section, we discuss recent works in the literature that converge on a structured analysis of digital games focused on digital security. Table 1 presents a summarization of these studies, highlighting the aspects involved in our study. A filled circle indicates that the study discusses the key aspect properly; a half-filled circle indicates that the study covers the topic partially; the absence of a circle means the study does not discuss the related aspect.

Considering the specific scope of cybersecurity, some recent studies analyzed the development of SGs. Hill Jr et al. (2020) surveyed SGs in education, categorizing them into four different topics. Coenraad et al. (2020) performed a systematic review to understand how players are being introduced to cybersecurity in game-based contexts. Likewise, Ng and Hasan (2025) focused on the development of SGs for cybersecurity training. As noted in Table 1, these studies did not cover a comprehensive analysis considering the development and evaluation process, ranging from the observation of genre/platform to the evaluation approach used. Furthermore, they did not propose any guidelines to researchers/developers, considering the performed analysis.

In a broader scope, dos Santos et al. (2025) investigated the application of playful and interactive SGs in the educational environment, conducting a systematic mapping of the use of SGs. In this work, the authors found that, although the adoption of games shows consistent benefits for student motivation and engagement, the study highlights methodological gaps, such as the scarcity of empirical evaluations and the lack

of development frameworks. However, the authors did not focus on the audience profile and its relation to the evaluation approach. Furthermore, there is no proposal of guidelines related to the development of SGs in the educational context.

Regarding methodological approaches in the academic environment, Ahmed et al. (2024) reviewed how universities have structured cybersecurity education for the distance learning model. The study indicated that gamification and virtual laboratories are essential technological resources to promote active learning and mitigate the engagement challenges inherent to remote education. The adoption of simulated environments, virtual *Escape Rooms*, and competitions in the *Capture The Flag* (CTF) format proved to be highly effective. However, the authors still neglect the analysis of the influence of the target audience and their profile on game development and evaluation.

Overall, existing SLRs did not cover important dimensions of digital SGs for cybersecurity. On one hand, none of them provide a comprehensive discussion that connects different game development dimensions while also proposing guidelines for this research field. In contrast, our work differs from previous reviews by analyzing these aspects in an integrated manner. Moreover, we propose a set of guidelines to support the development of digital SGs in digital security.

3. Systematic Literature Review Protocol

The SLR protocol adopted in this study was based on the well-known procedures proposed by Kitchenham et al. (2004) . The main purpose of carrying out this SLR lies in the need to understand the impact of digital SGs on the audience's awareness of digital security. We present a summary of the SLR protocol in the following sections.

3.1. Formulation of Research Questions

Considering the general questions of this study (presented in section 1) and the goal of the SLR, we raise the following research questions:

- **RQ1:** Which digital security aspects are addressed by the related games?
- **RQ2:** What are the genres of the related games?
- **RQ3:** Which development platforms are used for the related games?
- **RQ4:** Which related games are currently freely available?
- **RQ5:** What are the target audiences of the related games?
- **RQ6:** What was the evaluation approach defined by the authors?

These RQs can lead to a structured understanding of how such solutions are designed and evaluated. They also support the identification of research challenges, trends, and opportunities for improvement.

3.2. Search Strategy

Aiming to embrace a wide range of potential studies, we planned a search strategy considering four different digital libraries: IEEEXplore[1] , ACM Digital Library[2] , SBC

[1] https://ieeexplore.ieee.org/
[2] https://dl.acm.org/

OpenLib[3] , and Scopus[4] . The first three were selected due to their relevance in digital-based educational studies. SBC OpenLib was considered to capture studies in Portuguese. Scopus was included as a comprehensive indexing database that aggregates publications from a wide range of venues, enabling the identification of relevant studies that may not be directly indexed in the aforementioned ones.

Based on the research questions and the empirical analysis of similar studies (see Section 2), we defined a generalist search string, which was subsequently adapted according to the specific syntax and requirements of each digital library. The general search string is presented as follows.

```
( "cybersecurity education" OR "information security education" ) AND ( "educational games" OR "game-based learning" OR "gamification")
```

We also defined inclusion and exclusion criteria, since they are essential to refine the set of studies retrieved by the search string, ensuring that only relevant and high-quality research studies are considered in the SLR. The temporal cutoff from 2020 onward was adopted to prioritize recent studies, considering the fast evolution of digital technologies, cybersecurity threats, game development platforms, and educational practices. In this context, older studies may reflect technological constraints, platforms, or threat scenarios that are less representative of the current state of the field. They are listed as follows.

- **Inclusion Criteria**:
  - **IC1**: Articles published from 2020 to the present;
  - **IC2**: Authors developed an original electronic game in the context of digital security;
  - **IC3**: Evaluations were conducted with a sample population composed of real participants.
- **Exclusion Criteria**:
  - **EC1**: The study is based on the improvement or adaptation of an existing electronic game;
  - **EC2**: The study aims to propose methodologies or frameworks related to gamification in digital security in such a way that the game development and evaluation are not relevant;
  - **EC3**: The study falls into one of the following categories: systematic review, systematic mapping, surveys, work-in-progress, call for papers, or book chapters;
  - **EC4**: The study reports only incremental improvements or focuses solely on game design aspects;
  - **EC5**: The proposed game is not digital (e.g., *unplugged* games);
  - **EC6**: The main goal of the proposed game is not related to cybersecurity/digital security;
  - **EC7**: The study is not written in English or Portuguese.

[3] https://sol.sbc.org.br/index.php/indice
[4] https://www.scopus.com/

Table 2. Number of studies filtered in the selection process

Digital Library	1st round	2nd round	3rd round	Final round
IEEEXplore	182	154	10	10
ACM DL	169	155	5	5
SBC Openlib	12	12	2	2
Scopus	129	129	11	9
Total	**492**	**450**	**28**	**26**

3.3. Study Selection Process

The study selection process was carried out from January to March 2026, aiming to refine the set of retrieved works and ensure their alignment with the research scope. To increase the methodological reliability of the review, the study selection process was conducted by three researchers. In the third and final screening rounds, the researchers independently assessed the studies according to the inclusion and exclusion criteria. Disagreements were first discussed among the researchers, and final decisions were made through consensus. This procedure aimed to reduce individual bias and ensure a more consistent application of the selection criteria. The selection process was conducted in four screening rounds, described as follows.

- **1st round**: Application of the search string in the digital libraries, using the "age range" filter *a priori* to limit the search from 2020 to the present (IC1);
- **2nd round**: Removal of duplicated studies, considering the following priority order: Scopus, IEEEXplore, ACM DL, and SBC Openlib;
- **3rd round**: Studies filtering based on the inclusion and exclusion criteria, considering the reading of publication titles, keywords, and abstracts;
- **Final round**: Studies filtering by considering the detailed reading of the remaining studies, once again applying the inclusion and exclusion criteria.

4. Results

Table 2 presents the results of the study selection process, from the first to the final round. We report the entire SLR protocol and its execution in an online Annex[5]. Considering the inclusion and exclusion criteria, we selected 26 studies to analyze, aiming to answer the research questions (Section 3.2). Due to the limited space, we also provide a summarization of the selected studies through an online Annex[6]. To improve readability and reduce the repetition of long citation lists, each selected primary study was assigned a unique identifier, ranging from S1 to S26. These identifiers are reported in the online Annex, and they are used throughout the following subsections when referring to the selected primary studies. Figure 1 shows the numerical highlights regarding the main findings for each research questions, which we discuss as follows.

4.1. Digital Security Aspects

In this section, we discuss the aspects to answer RQ1. A comprehensive analysis of the selected studies reveals that a wide range of cybersecurity topics are explored. However, there is a concentration around some topics. The majority of the developed games (about

[5]Available at: `https://tinyurl.com/fratusetal2016`
[6]Available at: `https://zenodo.org/records/19834636`

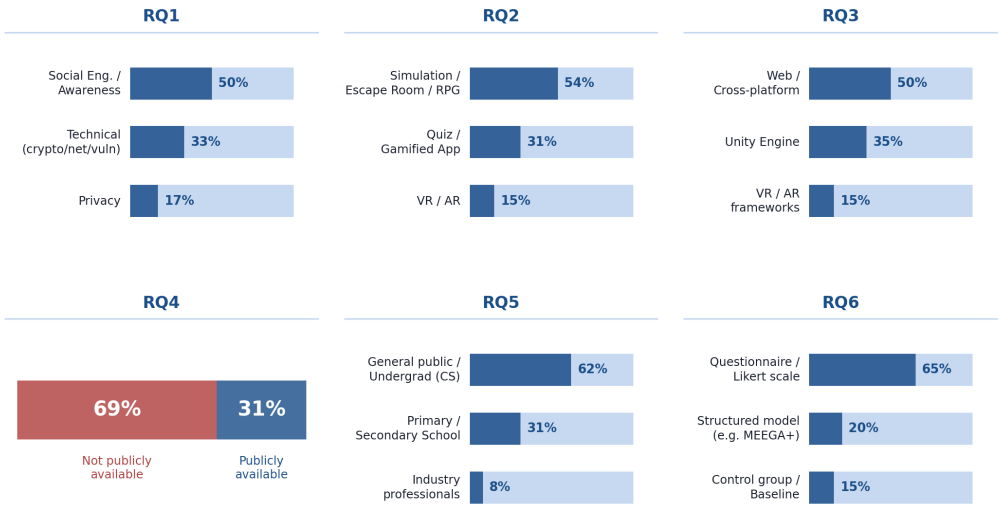

Figure 1. Numerical highlights of SLR results (the generation of the infographic was supported by the tool Jupyter Notebook)

half of them) focus on social engineering and user awareness [S2, S8, S19, S20, S22, S25] typically targeting the general public or younger audiences. From a scientific point of view, this aspect reflects a deep concern, being related to the weakest link in cybersecurity: the user.

Furthermore, around $1/3$ of the games involve technical aspects of cybersecurity. It includes topics such as cryptography and system vulnerabilities[S2, S8, S19, S20, S22, S25]. They are explored through more complex game mechanics, such as simulations or adversarial interactions. In general, these games are designed for undergraduate students, indicating their alignment with educational concerns. In contrast, a smaller portion of the studies involves privacy-related aspects[S5, S10, S16]. Despite their relevance, this topic appears comparatively underexplored when contrasted with more traditional security issues. Besides the analysis from a topic-related point of view, we can note that most games tend to address isolated cybersecurity topics, rather than integrating different cybersecurity topics in a unified game. Furthermore, topics related to emerging threats (e.g., AI-based attacks) are rarely explored.

4.2. Game Genres, Platforms of Development and Availability

In this section, we discuss the aspects to answer RQ2, RQ3, and RQ4. In general, most of the designed games adopt well-known game genres, combined with platforms that facilitate deployment and environments “ready-to-go”.

Regarding the game genres, a significant portion of the studies adopts simulation-based and role-playing experiences, which include escape rooms[S6, S8, S11], adversarial role-playing games [S12, S13, S26], and scenario-based simulations [S15, S16, S20, S25]. It suggests an increasing interest in “experiential” learning approaches, where users actively explore problems rather than passively receive information. Gamified applications and quiz-based games also represent a relevant group [S4, S21] . These environments typically focus on reinforcing conceptual knowledge through challenges, questionnaires, or point-based systems. Although easier to develop and deploy, these approaches tend to emphasize memorization rather than deeper understanding.

From the perspective of development platforms, there is a majority of web-based and cross-platform solutions [S1, S5, S6, S7, S9, S12, S14, S16, S17, S23, S26] , which appear in approximately half of the studies. These platforms are attractive to users due to their accessibility and low level of hardware requirements, making them suitable for large and diverse audiences. Similarly, the Unity game engine is widely used[S4, S8, S18, S21, S22, S24] , indicating that developers use popular environments, since Unity is a reference in the development of digital games, simulations, and interactive experiences. On the other hand, immersive technologies, such as Virtual Reality (VR) and Augmented Reality (AR), are less common[S3, S11, S18, S25] . This aspect may occur due to higher development costs and hardware constraints, indicating that, although immersive approaches are promising, their adoption in this context is limited.

When considering the availability of the developed games, we can note an important challenge: more than half of them do not provide public access to play. In many cases, it is unclear whether the game is just a prototype or restricted to the general public. On the other hand, the studies that provide access[S7, S9, S12, S20, S24] are predominantly associated with web-based platforms or simpler applications, reinforcing the relationship between accessibility and dissemination.

Analyzing these three dimensions jointly, we can note a "synergy" between popular genres, accessible platforms, and higher availability. Games based on quizzes, simulations, or lightweight interactions are more likely to be web-based and publicly accessible, which facilitates their adoption in real-world educational scenarios. On the other hand, more complex genres tend to be less accessible and not publicly available, limiting their impact on society.

4.3. Target Audience and Evaluation Approach

In this section, we discuss the aspects to answer RQ5 and RQ6. In a nutshell, the majority of studies focus on the general public or undergraduate students (typically in Computer Science or related technological fields) [S2, S4, S6, S9, S10, S11, S12, S13, S17, S18, S20, S21, S22, S23, S25, S26]. Similarly, students from primary and secondary education are considered to introduce cybersecurity aspects[S3, S5, S7, S8, S15, S16, S19, S24]. In a specific case, industry professionals are targeted considering specialized training contexts[S3, S5, S7, S8, S15, S16, S19, S24].

However, when analyzing the participant profiles considered in evaluations, an impactful discrepancy emerges: although most studies claim to target broad or heterogeneous audiences, the evaluation samples rely on "convenience groups", predominantly composed of undergraduate students. Even in cases where the game is designed for the general public or younger audiences, the evaluation is often conducted with a limited and homogeneous group [S2, S6, S20, S25]. This aspect can be explained by the difficulty of gathering a plurality of profiles as the evaluation public. This challenge directly impacts the scientific rigor of the results, whose findings may not accurately reflect the effectiveness of the games for their intended users. Moreover, the sample sizes are often relatively small. From a statistical point of view, this problem increases when participant profile diversity is limited. In many cases, evaluations involve a single group of students from a specific course or institution, without considering other aspects, such as age, gender, and educational background.

Regarding the evaluation approaches, there is a lack of standardization. Most studies are based on self-reported instruments, such as questionnaires, surveys, or Likert-scale assessment [S3, S5, S13, S26]. While these methods are useful for capturing subjective experiences, they provide a limited understanding of audience knowledge acquisition. A smaller group of studies applies well-known structured evaluation approaches (e.g., MEEGA+ model), aiming to evaluate learning aspects rigorously[S7, S9]. However, even in these cases, the evaluation designs are often not standardized, varying, for instance, in terms of instruments, duration, and analysis methods. Another outcome is the limited use of controlled experimental designs. Few studies adopt control groups or comparative baselines [S7, S9], which makes it difficult to isolate the actual impact of the game-based intervention. As a result, many conclusions are based on perceived effectiveness rather than robust empirical evidence.

4.4. General Discussion

The aforementioned discussion allows us to identify a set of recurring challenges as well as emerging trends in the design and impact of digital serious games in digital security. In a nutshell, the findings suggest that, although the area has evolved considering the plurality of approaches and technological adoption, there are still important issues that limit both the scientific rigor and the practical impact of the proposed solutions. The main identified challenges are listed as follows.

- **Limited scope of digital security topics:** Most games focus on social engineering and basic user awareness, while more advanced or emerging threats remain underexplored. In addition, most games address isolated topics rather than integrated digital security concepts, resulting in a fragmented learning experience;
- **Trade-off between complexity and accessibility:** On one hand, sophisticated game genres tend to provide better learning experiences, but are often associated with higher development and application costs. On the other hand, accessible approaches are more scalable, but may lack in providing a deep impact in terms of digital security awareness;
- **Lack of coherence between target audience and evaluation samples:** Although many studies propose solutions for broad or heterogeneous audiences, evaluations are frequently conducted with small and homogeneous groups, typically undergraduate students. This issue impacts the scientific rigor of the results;
- **Lack of standardization in evaluation approaches:** Most studies rely on self-reported instruments, with limited use of objective metrics and control groups. This aspect also impacts scientific rigor and makes it difficult to compare results across studies;
- **Limited availability of the developed games:** A wide range of developed games is not publicly accessible. This limitation reduces the potential impact and reuse of these games in learning environments, also hindering replication and validation by other researchers.

Although there are important challenges, we can identify some potential trends in the design and impact of digital serious games in digital security:

- **Adoption of experiential learning approaches:** There is a growing use of simulations and highly interactive environments, such as escape rooms. These scenarios promote active learning and higher levels of engagement from users;

- **Preference for accessible platforms:** Web-based and cross-platform solutions are widely adopted, reflecting a concern with scalability and ease of access for broader audiences;
- **General public-oriented audience:** Many games aim to target the general public or non-expert users, indicating a growing concern with "democratizing" digital security awareness. However, this trend is not consistently reflected in the evaluation procedures, which still rely predominantly on homogeneous samples.

Furthermore, we observed a worrying issue related to the studies (although not directly related to the proposed RQs): **there is a lack of ethical approval reporting**. A considerable number of studies do not explicitly mention approval by an ethics committee or institutional review board when conducting experiments with human participants. Considering that these studies involve data collection from real-world participants, the absence of such information raises concerns about compliance with ethical standards.

5. Proposal of Guidelines for the Development of Digital Serious Games in Digital Security

In this section, we propose guidelines to support the design, development, and evaluation of digital serious games in the context of digital security, aiming to overcome the main challenges discussed previously. We categorize the guidelines into three groups: for game design, for game development, and for game evaluation. They are described as follows.

- **Guidelines for game design:**
  - *Integration of multiple security topics:* Instead of focusing on isolated aspects, it is preferable to embrace different topics of digital security;
  - *Incorporation of emerging security threats:* Game developers should consider emerging threats, based on security reports from competent public entities or existing state-of-the-art studies;
  - *Design oriented to the target audience:* The game mechanics, language, and difficulty level should be aligned with the intended audience, increasing the potential user experience and learning level.
- **Guidelines for game development:**
  - *Accessibility-oriented design platforms:* Developers should ensure that the game remains accessible in terms of usability and infrastructure, aiming to reach a broader audience;
  - *Open availability:* Games should be made publicly available whenever possible to maximize their educational impact and allow replication and use by other researchers.
- **Guidelines for game evaluation:**
  - *Alignment between evaluation samples and target audience:* The evaluation's participant profile must reflect as closely as possible the intended audience of the game, ensuring that results are representative;
  - *Standardization of evaluation procedures:* Game evaluations must include well-known and structured evaluation methodologies/frameworks (e.g., the MEEGA+ model), providing stronger evidence and the possibility of further comparisons;
  - *Ethical compliance:* Research involving human participants must report approval by an ethics committee or institutional review board, ensuring the required ethical standards.

6. Final Remarks and Future Research Directions

In this study, we analyzed the design and impact of digital SGs in the context of digital security. As main contributions, we applied an SLR protocol, aiming to answer six different related research questions. As a direct result of the SLR, we conducted a comprehensive analysis of 26 studies, raising five fundamental challenges and three main trends in this research area. Based on these challenges and trends, we also proposed a set of guidelines for the development of digital SGs in digital security based on three fronts: game design, game development, and game evaluation.

Overall, our analysis highlighted that, despite the growing diversity of approaches, this research field still faces important challenges, for instance, the homogeneous groups considered in the game evaluation process, even when the game is proposed for a general audience, and the limited availability of the developed games. At the same time, some trends can be observed, including the adoption of experiential learning approaches, such as virtual escape rooms. Furthermore, the lack of ethical approval reporting in several studies highlights a critical issue regarding research transparency and compliance with ethical standards.

Despite the contributions of this study, some limitations must be acknowledged regarding the SLR. Initially, the search process was restricted to a set of four digital libraries. This may lead to the exclusion of relevant studies indexed in other sources. Also, the definition of the search string and the inclusion/exclusion criteria may lead to biases by omitting studies that address the topic using different terminologies. In particular, the term “serious game” was not explicitly included in the search string, which may have excluded studies that use this terminology exclusively. This choice was made because the search strategy prioritized broader expressions commonly associated with educational digital games (e.g., educational games and game-based learning). The study selection and data extraction processes also involve a degree of subjectivity, particularly in the categorization of aspects such as game genre, platform, and cybersecurity topics. Last but not least, the relatively limited number of studies and their strong association with academic contexts may restrict the generalization of the findings.

As future research directions, we intend to develop a game system focused on raising digital security awareness among the general public, following the guidelines proposed in this study. In fact, the scope addressed in this work and the future development of the game are already part of a research project whose protocol has been approved by the ethics committee of Universidade Estadual de Maringá, under Certificate of Presentation for Ethical Appraisal (CAAE) 90043225.0.0000.0104.

Declaration of Use of Artificial Intelligence Tools

The authors declare that ChatGPT 5.4 was used to support the generation of the infographic presented in Figure 1, specifically by assisting with the visual organization and chart-generation process. ChatGPT was also used for grammatical revision of the manuscript. Jupyter Notebook was used as a computational tool to generate the final version of the infographic. All textual content, data interpretation, analyses, and conclusions are the authors’ own formulation and responsibility.

References

Abu-Amara, F. e Tamimi, H. (2021). Cyber shield security awareness program. In *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 422–425. IEEE.

Ahmed, A., Watterson, C., Alhashmi, S., e Gaber, T. (2024). How universities teach cybersecurity courses online: a systematic literature review. *Frontiers in Computer Science*, 6:1499490.

Alma'ariz, S., Hadiprakoso, R. B., Qomariasih, N., et al. (2022). Soceng warriors: Game-based learning to increase security awareness against social engineering attacks. In *2022 IEEE 8th Information Technology International Seminar (ITIS)*, pages 124–129. IEEE.

Asif, S. A., Cao, Y., Veng, S., Chisholm, K., Posthumous, R. P., Rutherford, T., Shen, C.-C., e Mouza, C. (2025). Augmentwall: An ar firewall game for concretizing cybersecurity concepts and examining student engagement, learning, and motivation. In *2025 IEEE Integrated STEM Education Conference (ISEC)*, pages 1–8. IEEE.

Berisford, C. J., Blackburn, L., Ollett, J. M., Tonner, T. B., Yuen, C. S. H., Walton, R., e Olayinka, O. (2022). Can gamification help to teach cybersecurity? In *2022 20th International conference on information technology based higher education and training (ITHET)*, pages 1–9. IEEE.

Chattopadhyay, A., Sharma, S., Mbaya, E., e Rice, J. (2024). Vpet: A novel visual privacy themed cybersecurity educational game. In *2024 IEEE Frontiers in Education Conference (FIE)*, pages 1–9. IEEE.

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., e Weintrop, D. (2020). Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simulation & Gaming*, 51(5):586–611.

Costa, G., Lualdi, M., Ribaudo, M., e Valenza, A. (2020). A nerd dogma: introducing ctf to non-expert audience. In *Proceedings of the 21st Annual Conference on Information Technology Education*, pages 413–418.

DataSenado (2024). Panorama político 2024: Apostas esportivas, golpes digitais e endividamento. Technical report, Instituto de Pesquisa DataSenado.

de Abreu, J. M., Miani, R. S., e Nomura, S. (2024). " encrypta: A missão da liga dos robôs"-um jogo educacional para aprendizagem em cibersegurança. In *Simpósio Brasileiro de Jogos e Entretenimento Digital (SBGames)*, pages 1327–1338. SBC.

DeCusatis, C. a., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., Maloney, M., Avitable, D., e Mah, B. (2022). A cybersecurity awareness escape room using gamification design principles. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0765–0770. IEEE.

dos Santos, E. E., Junior, M. M. C., da Silva, F. F., e Aylon, L. B. R. (2025). Cyber defender: desenvolvimento e avaliação de um jogo educativo para ensino de segurança cibernética. In *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 289–304. SBC.

Fu, J., Lu, Y., Yang, Z., Nah, F., e LC, R. (2025). Cracking aegis: An adversarial llm-based game for raising awareness of vulnerabilities in privacy protection. In *Proceedings of the 2025 ACM Designing Interactive Systems Conference*, pages 639–662.

Hasan, K. F., Hughes, W., Rahman Tory, A., Campbell, C., e Turkay, S. (2026). Game on: A developmental approach to unsw cyber escape room for cybersecurity governance and policy education. *Education Sciences*, 16(1):133.

Hill Jr, W. A., Fanuel, M., Yuan, X., Zhang, J., e Sajad, S. (2020). A survey of serious games for cybersecurity education and training. *KSU Proceedings on Cybersecurity Education, Research and Practice*.

Huang, S., Herman, G. L., Olano, M., Oliva, L., e Sherman, A. T. (2025a). Meetingmayhem: A web-based educational game focused on adversarial thinking. In *Proceedings of the 30th ACM Conference on Innovation and Technology in Computer Science Education V. 2*, pages 735–736.

Huang, S., Herman, G. L., e Sherman, A. T. (2025b). Cyberguardian: A role-playing educational game for learning cryptographic primitives in authentic cybersecurity scenarios. In *Proceedings of the 30th ACM Conference on Innovation and Technology in Computer Science Education V. 2*, pages 745–746.

Jayakrishnan, G. C., Banahatti, V., Lodha, S., Sirigireddy, G., e Nivas, S. (2022). Housie: A multiplayer game for cybersecurity training and evaluation. In *Extended abstracts of the 2022 annual symposium on computer-human interaction in play*, pages 17–23.

Kido, Y., Tou, N. P., Yanai, N., e Shimojo, S. (2020). sd&d: Design and implementation of cybersecurity educational game with highly extensible functionality. In *Future of Information and Communication Conference*, pages 857–873. Springer.

Kitchenham, B. et al. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26.

Luccas, M. d. S., Pereira, L. T., e Branco, K. C. (2025). Um mapeamento sistemático da literatura sobre jogos sérios no ensino superior em ciência da computação. *Simpósio Brasileiro de Jogos e Entretenimento Digital (SBGames)*, pages 1231–1245.

Maqsood, S. e Chiasson, S. (2021). Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):1–37.

Mohanty, A., Murarisetty, P., Nguyen, N. D., Bahamon, J. C., Ramaprasad, H., e Sridhar, M. (2021). Criminal investigations: an interactiveexperience to improve student engagement and achievement in cybersecurity courses. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, pages 1276–1276.

Ng, C. Y. e Hasan, M. K. B. (2025). Cybersecurity serious games development: A systematic review. *Computers & Security*, 150:104307.

Pantaliano, M. E., Rabano, A. N. M., Villaalba, H. B., Blanco, M. C. R., Co, J. D. C., Sison, A. A. R. C., e Centeno, C. J. (2024). Forenseek: Gamifying learning experiences in digital forensics using unity engine and augmented reality technology. In *2024 IEEE International Conference on Computing (ICOCO)*, pages 196–201. IEEE.

Pérez, J., Torres, R., e Von Brand, S. (2020). Cyberkids: video game for raising cyber security awareness in children. In *2020 39th International Conference of the Chilean Computer Science Society (SCCC)*, pages 1–8. IEEE.

Polícia Federal (2025). Dados de crimes cibernéticos – janeiro a dezembro de 2025. Relatório Operacional. Disponível nos registros da Polícia Federal do Brasil.

Raturi, Y., Saini, S., Singh, Y., Saini, V., Balyan, Y., e Dhaka, R. (2025). Cyberclash: Cybersecurity awareness game. In *2025 IEEE 6th India Council International Subsections Conference (INDISCON)*, pages 1–5. IEEE.

Salman, O. H., Alawida, M., Hazeem, R. M. A., Zeyadeh, M. S., e Alameri, M. R. (2023). Cybersafe: A gamified cyber security training method. In *2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, pages 1–6. IEEE.

Silva, C., Serra, A., Folgado, D., Santos, H., Oliveira, Â., e Lopes, A. (2022). It's a fraud: learning about cybersecurity. In *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6. IEEE.

Susanto, H. Y. e Arifin, Y. (2024). The learning outcomes achievement and user experience analysis of a cryptography education web game. In *2024 10th International HCI and UX Conference in Indonesia (CHIuXiD)*, pages 30–35. IEEE.

Toledo, W., Louis, S. J., e Sengupta, S. (2022). Netdefense: A tower defense cybersecurity game for middle and high school students. In *2022 IEEE frontiers in education conference (FIE)*, pages 1–6. IEEE.

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., e Catarci, T. (2020). Cybervr: an interactive learning experience in virtual reality for cybersecurity related issues. In *Proceedings of the 2020 International Conference on Advanced Visual Interfaces*, pages 1–8.

Weeratunge, N. H. e Hjelsvold, R. (2025). Enhancing cybersecurity learning with in-game feedback. In *European Conference on Games Based Learning*, volume 2, pages 883–891. Academic Conferences International Limited.