



REVIEW

A Systematic Literature Review on the Application of Gamification in the Field of Information Security

Indre Grigaraviciute and Nikolaj Goranin*

Department of Information Systems, Vilnius Gediminas Technical University, Vilnius, Lithuania

*Corresponding Author: Nikolaj Goranin. Email: nikolaj.goranin@vilniustech.lt

Received: 08 May 2026; Accepted: 27 July 2026; Published: 15 September 2026

ABSTRACT: Gamification has emerged as an effective approach to enhance user engagement and security awareness in the field of information security. This study presents a systematic literature review (SLR) of research published between 2012 and March 2026, analysing publications from two major databases, Scopus and Web of Science (WoS). The review was conducted following the PRISMA 2020 guidelines. A comprehensive set of seven keywords: “gamification”, “information security”, “cybersecurity”, “security awareness”, “business security and privacy training”, “security management”, and “incident response”, was used to retrieve relevant studies. A total of 1487 articles were initially identified, of which 955 remained after duplicate removal. Following screening based on predefined inclusion and exclusion criteria, 77 studies were included in the final systematic literature review. Bibliometric and descriptive analyses were conducted using Mendeley, VOSviewer, ResearchRabbit, and Microsoft Excel. The results show that research is predominantly published in Computer Science and Engineering journals, with the United States, Germany, and the United Kingdom contributing the most studies. Conference papers constitute the largest proportion of documents, and most journals fall within the top two SJR quartiles (Q1 and Q2). Key applications of gamification include security awareness training, cybersecurity education for non-IT professionals, incident response, and privacy management, while future research directions emphasise adaptive gamification, integration with emerging technologies, longitudinal studies, and cross-cultural investigations. This study provides a comprehensive overview of the current state and future directions of gamification in information security, contributing to both academic understanding and practical implementation strategies. This article stands out for the research methods used, the novelty of the data, and the assessment of the included studies according to SCImago Journal Rank (SJR).

KEYWORDS: Information security; gamification; cybersecurity; security awareness; game-based learning; security education; human factors in cybersecurity; behavioral security; security training

1 Introduction

In the rapidly evolving field of information technology, the need for robust information security processes is becoming increasingly important. Organizations worldwide are continually battling cyber threats and data breaches that can result in substantial financial losses, reputational damage, and privacy violations. As a result, the need for innovative methods to increase information security and optimize the efficiency of security processes is increasing.

Addressing information security issues is a constant and complex challenge. Preventing breaches requires a continuous effort to effectively address and manage these issues. Humans are often considered the

weak link in information security due to their susceptibility to cyber attacks, lack of awareness of potential threats, and potential human error in handling sensitive data or following security protocols.

Conducted studies have shown that the main problems and factors influencing the perception of information security by end users are related to user age, information security policy, user behavior, education, knowledge, culture, environment, rules, and monitoring [1]. To increase end-user information security awareness of self-protection against cyber threats, the following methods were explored: education, enabling methods, management involvement, training, security awareness, and incident reporting. Training, engaging and useful learning programs for employees is another way to communicate information security.

Gamification has emerged as a growing area of interest within ISA programs. It aims to apply game features such as points in non-game context to encourage participants to perform a task or set of tasks in order to promote their InfoSec knowledge and behavior [2]. Although gamification has great potential to improve the performance of ISA programs in areas where current efforts are not succeeding, it also has significant pitfalls that should be considered in its design and application [3].

One of the new strategies that has received a lot of attention is the application of game elements in information security processes. Gamification refers to the use of computer game logic and thought patterns in a non-game context to engage and motivate individuals to achieve specific goals. By integrating elements such as points, levels, rewards, challenges, and competition into security processes, gamification can increase user engagement, encourage desired security behaviors, and ultimately improve the effectiveness of information security measures [4–6].

Recent studies have increasingly explored the application of gamification in information security awareness. According to a study conducted by Sharif and Ameen [7], it was found that a game-based approach is most commonly used to increase information security awareness. Most of the articles present methods in which games are used to inform and teach, showing positive effects [7]. An article by Nguyen and Pham [8] states that game methods are applied in information security training, but the results are limited due to the lack of implementation examples or a weak theoretical base. For instance, the study by Pahlavanpour and Gao [9] conducted a systematic mapping analysis using the Scopus and Web of Science databases, applying keywords such as “gamification”, “game”, “gamified”, and “security awareness”, while intentionally excluding broader terms like “information” and “program” to improve search precision. Similarly, Gwenhure and Sapty Rahayu [10] performed a systematic literature review focusing on cybersecurity awareness for non-IT professionals, employing an extensive and complex keyword strategy within the Scopus database for publications between 2020 and 2023.

Although these studies provide valuable insights into gamification in information security, they mainly focus on specific topics such as security awareness, cybersecurity training, or particular target groups. In addition, previous reviews were conducted using a limited set of keywords, a single database, or a restricted publication period. Therefore, there is still a need for a broader and more up-to-date review that examines gamification across different areas of information security using multiple databases and an extended search period.

This research contributes to the body of knowledge on gamification in the field of information security by employing a broader set of keywords and analysing data from both Scopus and Web of Science databases, rather than relying on a single data source. It provides a systematic map of the topic keywords and provides an understanding of the main topics in the research area. This article is intended to help academic and industrial researchers working on semantically enriched and knowledge-based information security. In addition, the results of this study can help researchers and practitioners to better understand the body of knowledge on

gamification in information security, while also capturing more recent research trends, as the analysed period extends beyond 2023.

The remaining part of this article is organized as follows. In [Section 2](#), we described the materials and methods of this research. In [Section 3](#), we present the systematic mapping study results on the gamification in the field of information security. In [Section 4](#), we discuss our findings. Finally, [Section 5](#) summarizes this article.

2 Materials and Methods

A systematic literature review (SLR) of gamification in the information security domain was conducted using bibliometric analysis. The SLR was systematically organized following the PRISMA 2020 statement [11] for planning, conducting, and reporting. The main steps of the SLR are explained in the following sections. Although bibliometric techniques were used to analyse publication trends and structural patterns in the literature, the core of this study follows a systematic literature review approach. The final synthesis is based on the 77 studies that met the predefined inclusion criteria, ensuring that the review goes beyond descriptive mapping by focusing on eligible evidence-based studies.

2.1 Research Questions

This SLR aims to provide a framework for the field of interest in the gamification in the field of information security and to provide an overview of the main ideas in this field. This leads to the following main research question (MRQ): How does gamification contribute to information security? Based on the MRQ, the following RQs are defined:

- RQ-1: How has research on gamification in information security evolved over time?
- RQ-2: What are the topics of application of gamification in the field of information security that are being explored?
- RQ-3: What are the main future directions in the topic under analysis?
- RQ-4: What are the publication trends in terms of authors, countries, and journal quality in gamification research in information security?

2.2 Conducting the Search

The PICOC (Population, Intervention, Comparison, Outcome, Context) framework, as employed by Kitchenham and Charters [12], was created to aid in the identification of keywords and the development of search strings derived from the MRQ.

Population: In this study, the population consists of scientific articles on the application of gamification in the field of information security.

Intervention: In our context, we examine how gamification is related to the field of information security.

Comparison: This study does not perform a comparison.

Outcomes: Our focus is solely on the article results; therefore, measurable outcomes are not considered.

Context: This academic study analyzes existing articles concerning the application of gamification in information security.

The PICOC criteria presented in [Table 1](#) were used to guide keyword selection and the screening process.

The selection of keywords was guided by the aim to comprehensively capture research at the intersection of gamification and information security. Therefore, a combination of a core concept (“gamification”) and domain-specific terms related to cybersecurity practices, education, and organisational security processes

was used to ensure broad yet relevant coverage of the literature. The keywords were designed to reflect the main application areas where gamification has been reported, including security awareness, training, management, and incident response. This approach ensured that both technical and human-centric aspects of information security were included in the search strategy.

Table 1: PICOC inclusion and exclusion criteria.

PICOC Element	Inclusion Criteria	Exclusion Criteria
P	Scientific articles on gamification in information security	Non-security or non-gamification studies
I	Studies involving gamification approaches in information security	Studies without gamification elements
C	Not applicable	Not applicable
O	Studies contributing to understanding of gamification applications and effects in InfoSec	Studies without analytical or thematic relevance
C	Information security and cybersecurity domain	Studies outside information security domain

Consequently, we identified seven main terms: “gamification”, “information security”, “cybersecurity”, “security awareness”, “business security and privacy training”, “security management”, and “incident response”.

The keyword “BSP training” was excluded from the main keyword set, as it did not yield any results in either Scopus or Web of Science. To ensure the relevance and robustness of the keyword-based search, this abbreviated form was not used in subsequent analyses; instead, the full term “business security and privacy training” was employed.

Although during the last decade, there was a significant growth of available bibliographic data sources and metrics, Web of Science (WoS) and Scopus databases (DBs) still remain the two major and most comprehensive sources of publication metadata and impact indicators [13]. In this study, the two terms were combined into a single search string, which was then used in the Web of Science (WoS) and Scopus databases (See Table 2). The keyword “gamification” was chosen as the main term in this study. Gamification can be defined as the use of game designed elements in non-gaming situations to encourage users’ motivation, enjoyment, and engagement, particularly in performing a difficult and complex task or achieving a certain goal [14–16]. Although related terms such as “game-based approaches”, “serious games”, and “game elements” are used in the literature, they were not included as primary keywords, as they represent broader approaches. Therefore, the term “gamification” was selected to ensure a focused and consistent search strategy aligned with the scope of this study.

Seven key terms are used quite widely in the 1487 articles. 532 duplicate articles have been removed to make the data more accurate (See Table 3). Search restrictions, including search string, document type, language, and categories, were applied later after refining and comparing data in the WoS and Scopus databases. The Scopus search string is used as follows:

((TITLE-ABS-KEY (gamification) AND TITLE-ABS-KEY (information security))) OR ((TITLE-ABS-KEY (gamification) AND TITLE-ABS-KEY (security awareness))) OR ((TITLE-ABS-KEY (gamification)

AND TITLE-ABS-KEY (cybersecurity))) OR ((TITLE-ABS-KEY (gamification) AND TITLE-ABS-KEY (security management))) OR ((TITLE-ABS-KEY (gamification) AND TITLE-ABS-KEY (incident response))) OR ((TITLE-ABS-KEY (gamification) AND TITLE-ABS-KEY (business security & privacy training)))

Table 2: Search strings in Web of Science (WoS) and Scopus.

No.	Database	Keyword 1	Operator	Keyword 2	Result
1.	Scopus	“gamification”	And	“information security”	302
2.	Scopus	“gamification”	And	“security awareness”	212
3.	Scopus	“gamification”	And	“cybersecurity”	354
4.	Scopus	“gamification”	And	“business security and privacy training”	8
5.	Scopus	“gamification”	And	“security management”	152
6.	Scopus	“gamification”	And	“incident response”	23
7.	WoS	“gamification”	And	“information security”	116
8.	WoS	“gamification”	And	“security awareness”	109
9.	WoS	“gamification”	And	“cybersecurity”	153
10.	WoS	“gamification”	And	“business security and privacy training”	1
11.	WoS	“gamification”	And	“security management”	46
12.	WoS	“gamification”	And	“incident response”	11
Total					1487

Table 3: Data change after removing duplicates in Scopus and Web of Science (WoS).

No.	Database	Before	Removed Duplicates	Result
1.	Scopus	1051	389	662
2.	WoS	436	143	293
	Total	1487	532	955

The link to the search query performed in the Web of Science database: <https://www.webofscience.com/wos/woscc/summary/5f75e93b-03b3-4856-a954-7fc661b2fe86-01a4fa6fb2/relevance/1>.

2.3 Study Selection and Quality Assessment

A total of 1487 records were retrieved in the initial search. Following the removal of duplicates, 955 unique articles remained (662 from Scopus and 293 from Web of Science). These records were then screened based on predefined inclusion and exclusion criteria (see below), resulting in 77 studies included in the final systematic literature review. Considering the research questions, it was decided to analyze the document types, subject/research area, and country data, and define inclusion criteria (IC) and exclusion criteria (EC) based on recommendations given by Angela Carrera-Rivera, William Ochoa, Felix Larrinaga, and Ganix Lasa. Authors should define the inclusion and exclusion criteria before conducting the review to prevent bias, although these can be adjusted later, if necessary [17].

Inclusion criteria (IC) and exclusion criteria (EC):

- IC1: Include papers that are works on gamification in information security.
- IC2: Include articles that are written in the English language.

- EC1: Exclude duplicate articles identified across databases.
- EC2: Exclude articles that are not intended for global research.

The overall results of the paper's selection procedure are illustrated in Fig. 1 as a PRISMA flow diagram.

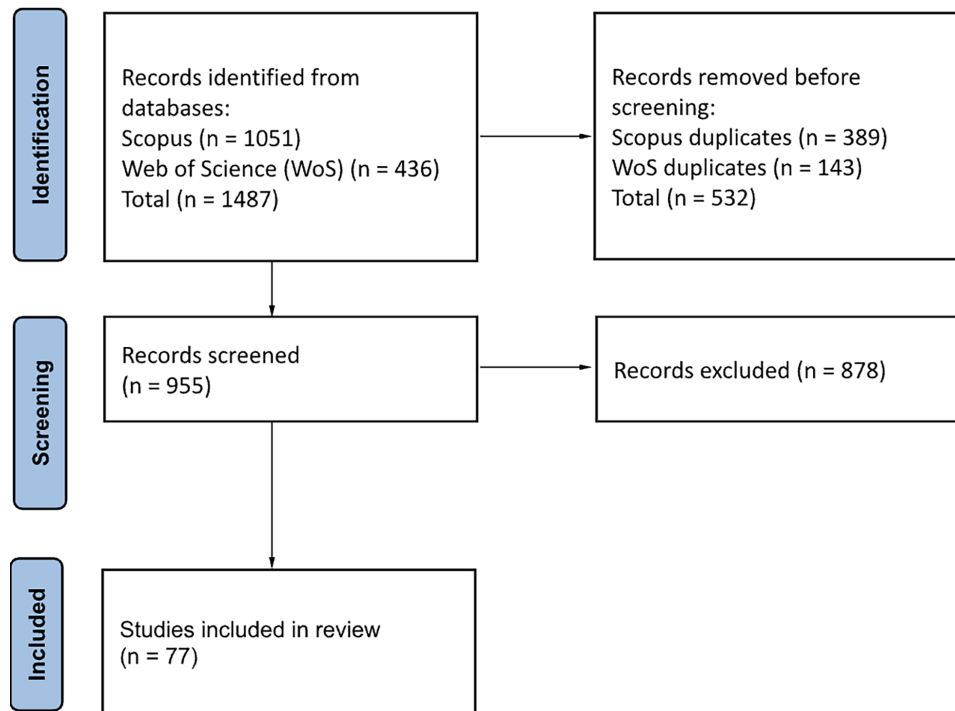


Figure 1: PRISMA 2020 flow diagram for new systematic reviews which included searches of databases.

Visualization and mapping tools (VOSviewer and ResearchRabbit) were applied to subsets of the final dataset to support bibliometric and thematic analysis; however, they did not affect the study selection process.

2.4 Used Tools

The following tools were employed in this study: (1) Mendeley (v2.142.0) was used for reference management and removal of duplicate records; (2) VOSviewer (1.6.20_mac) was applied for bibliometric analysis, including keyword co-occurrence mapping and visualisation of research clusters; (3) ResearchRabbit (2.0) was used as a supplementary tool for exploring citation networks and visualising temporal publication relationships, supporting contextual analysis rather than primary data selection; and (4) Microsoft Excel (16.0.20015.42303) was used for data organisation, descriptive statistical analysis, and preparation of tables, including SCImago Journal Rank (SJR) quartile classification.

2.5 Data Extraction

The data extraction process was conducted to systematically gather relevant information from two primary databases, namely Web of Science (WoS) and Scopus. Studies were selected based on predefined keywords and clearly defined inclusion and exclusion criteria.

The search used restricted categories (e.g., computer science or engineering), and inclusion and exclusion criteria to exclude irrelevant studies. Search results in the Web of Science (WoS) and Scopus databases, with inclusion and exclusion criteria added (See Table 4). At the identification stage, 293 records

from Web of Science (WoS) and 662 from Scopus were retrieved and screened according to the inclusion and exclusion criteria.

Table 4: Study selection and quality assessment in Web of Science (WoS) and Scopus.

No.	Criteria	Scopus	WoS
1.	Document Type: Scopus (Article, Review), WoS (Review article or Article)	148	135
2.	Subject/research area: Computer Science or Engineering, WoS: Education Educational Research Scopus: Social Science	124	86
3.	Language: English	118	85
4.	Open Access	76	51

Search results from Web of Science and Scopus were downloaded into Mendeley (<https://www.mendeley.com/> (accessed on 13 March 2026)) and subsequently deduplicated. After duplicate removal and manual screening for relevance to the study topic, 77 articles remained.

2.6 Method Used for the Results Analysis

The extracted data were subsequently analysed using Mendeley, VOSviewer, ResearchRabbit, and Microsoft Excel to ensure consistency, reliability, and to facilitate further statistical analysis. The results were analysed using a combination of bibliometric and descriptive statistical methods. Bibliometric analysis was performed using VOSviewer to examine keyword co-occurrence and to generate network, overlay, and density visualisations. In addition, Microsoft Excel was used for descriptive statistical analysis. The quality of the publication sources was assessed based on SCImago Journal Rank (SJR) quartiles.

2.6.1 Document Type Analysis

Articles can be included or excluded based on document type. One of the most popular document types in the Scopus and WoS databases is a conference paper, also known as conference proceedings. Based on the data provided by Dyba and Dingsoyr, it has been determined that a conference paper may fall into the grey literature category due to the lack of research details due to space limitations [18]. Moreover, conference papers are often expanded in journal papers [19].

The distribution of document types identified in the Scopus search results from 2012 to March 2026 is presented in Fig. 2. The analysis shows that conference papers constitute the largest proportion of publications, accounting for 50.2% of the total. This is followed by journal articles (19.6%) and conference reviews (18.6%). These findings indicate that research on gamification in information security is predominantly disseminated through conference venues, reflecting the dynamic and rapidly evolving nature of the field, where early-stage findings are frequently presented and discussed in academic conferences.

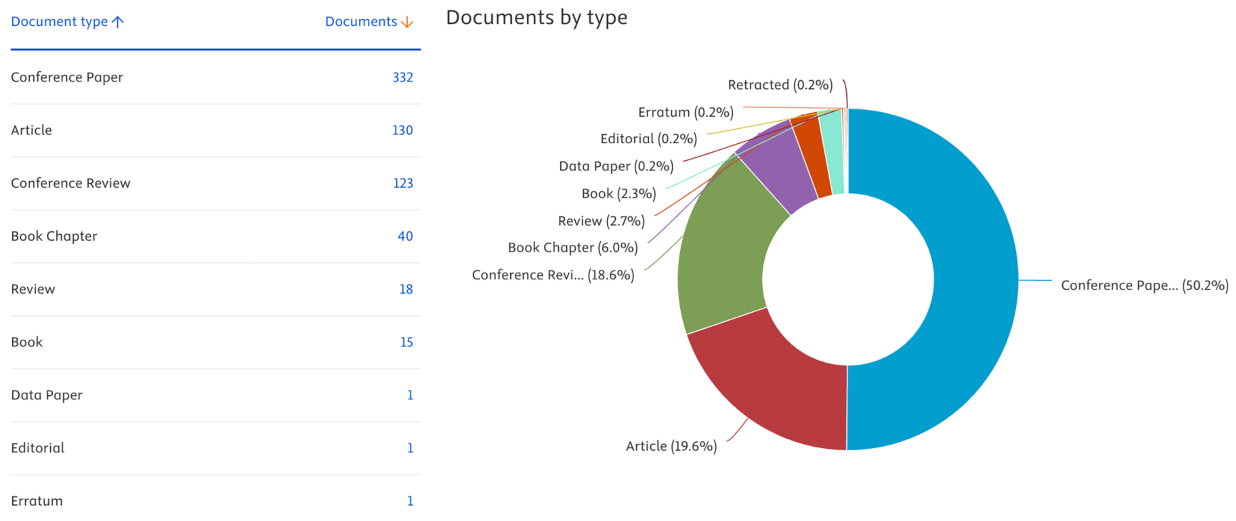


Figure 2: Overview of document types identified in the Scopus search results from 2012–March 2026.

The distribution of document types identified in the Web of Science (WoS) search results is presented in Fig. 3. Proceedings papers constitute the majority of publications, accounting for 53.58%, followed by journal articles at 41.98%, and review articles at 4.09%. Compared to the Scopus results (See Fig. 2), both databases show a predominance of conference/proceedings papers.

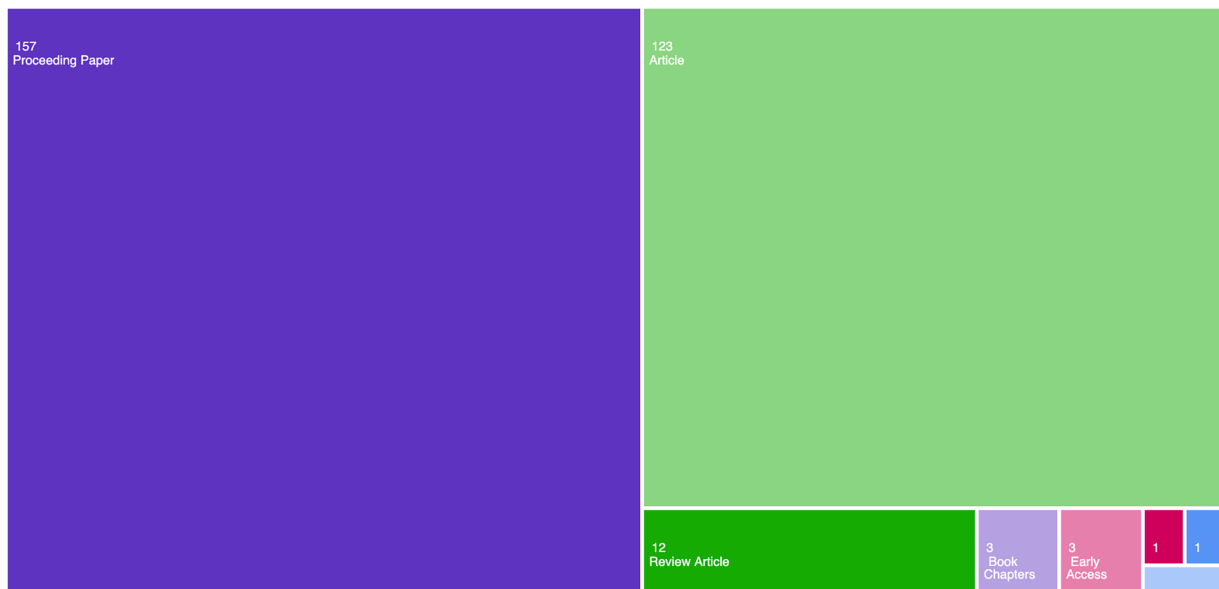


Figure 3: Overview of document types identified in the WoS search results.

A total of eight document types were identified in the Web of Science (WoS) search results. Proceeding papers represent the largest share (157), followed by journal articles (123) and review articles (12), while the remaining document types appear in smaller quantities. This distribution indicates that research in this field is primarily disseminated through conference proceedings and journal publications.

2.6.2 Subject Area Analysis

The subject area distribution of the selected studies is presented in Fig. 4, based on the Scopus search results from 2012 to March 2026. The analysis indicates that the majority of publications fall within the field of Computer Science, accounting for 38.4% of the total. This is followed by Engineering (17%) and Social Sciences (12.4%), which together represent the top three subject areas. These findings suggest that research on gamification in information security is predominantly driven by technical disciplines, while also maintaining a notable interdisciplinary presence.

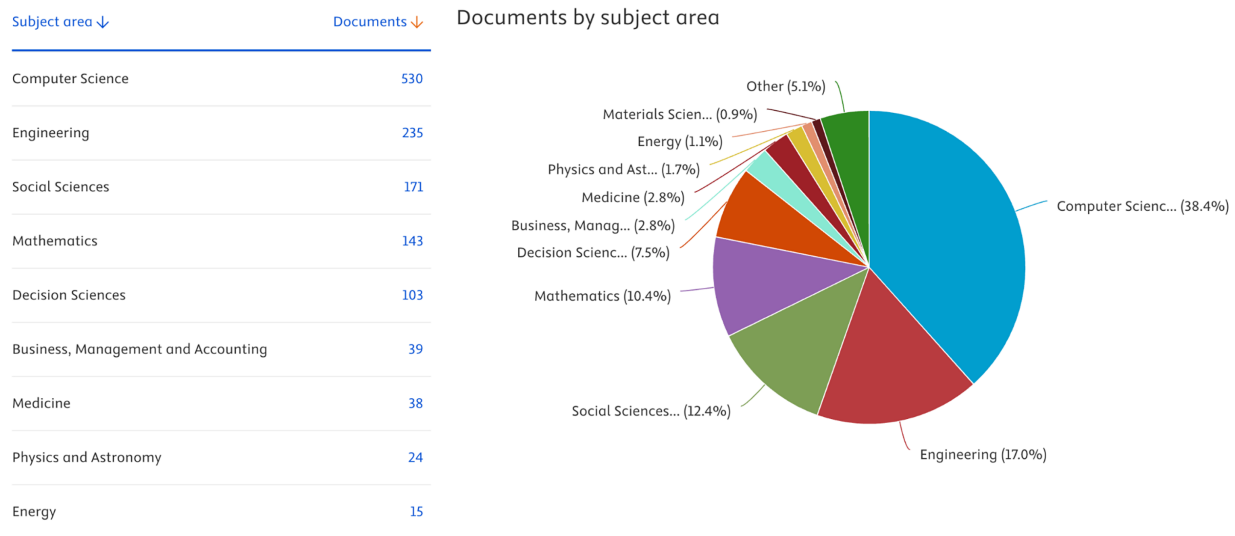


Figure 4: Overview of subject area identified in the Scopus search results from 2012–March 2026.

The distribution of research areas based on the Web of Science (WoS) search results is presented in Fig. 5. The findings show that Computer Science represents the dominant research area, accounting for 63.48% of the publications. This is followed by Education Educational Research (23.55%) and Engineering (18.09%), among the thirty-eight identified research areas. These results indicate a strong emphasis on technical and computational aspects, while also highlighting the growing importance of educational perspectives in the context of gamification in information security.

The analysis of research areas in the Web of Science (WoS) results shows that Computer Science dominates with 186 publications, followed by Education Educational Research (69) and Engineering (53). Telecommunications also represents a notable area with 27 publications, while other research areas appear with smaller contributions. This distribution highlights the strong technical focus of the field, while also indicating the growing importance of educational perspectives in gamification research within information security.

Overall, the analysis of subject and research areas across both Scopus and Web of Science databases reveals that gamification in information security is predominantly situated within the field of Computer Science, with Engineering and Social Sciences/Education also playing significant roles. This distribution highlights the technical foundation of the research area while emphasising its interdisciplinary nature, particularly the integration of educational approaches in promoting security awareness. This trend can be explained by the fundamentally technical nature of information security, which requires the development of secure systems and solutions, combined with the need to influence user behavior through training and

awareness programs. Therefore, the field naturally combines technical disciplines with educational and behavioral sciences.

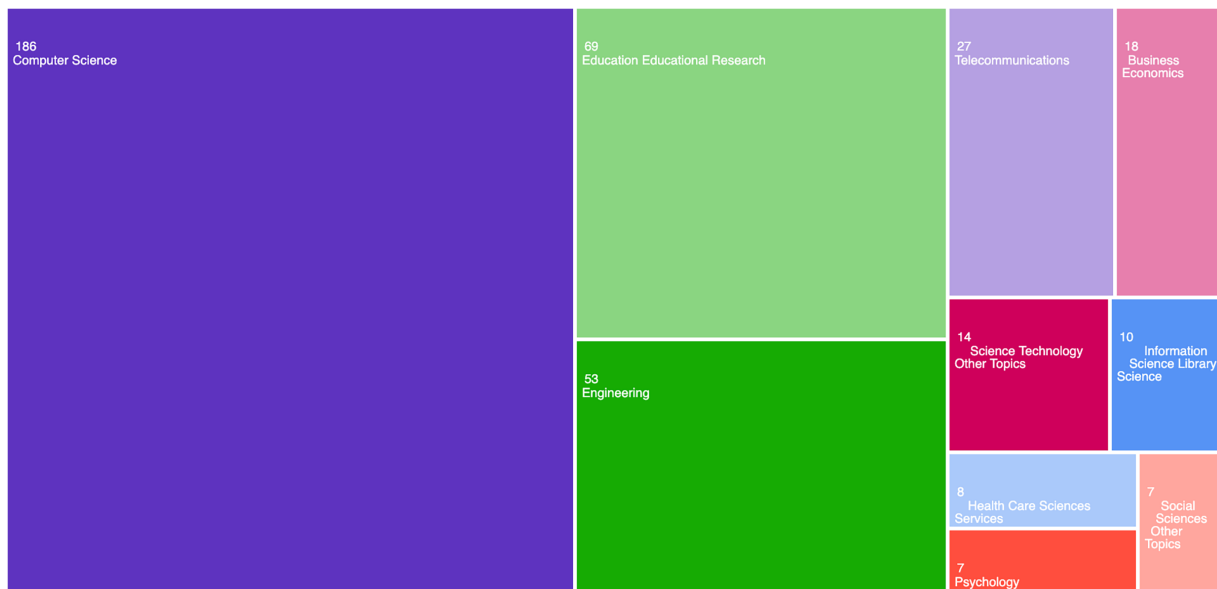


Figure 5: Overview of research area identified in the WoS search results.

2.7 Validity Evaluation

The validity of this systematic literature review was ensured through the use of a transparent and structured review process based on PRISMA guidelines. The study relied on two well-established databases, Scopus and Web of Science, which are widely recognised for their reliability and coverage of high-quality scientific publications. A predefined search strategy and clear inclusion and exclusion criteria were applied to ensure consistency and reduce selection bias during the study selection process.

To increase reliability, the review process followed a clearly documented and reproducible procedure, allowing the results to be systematically verified. However, limitations remain due to the exclusion of non-English publications and the restriction to two databases, which may have led to the omission of relevant studies indexed elsewhere.

A formal study-level methodological quality assessment (e.g., CASP) was not applied, as this review primarily focuses on bibliometric and mapping analysis rather than in-depth critical appraisal of individual studies.

3 Results

3.1 Chronological Distribution Analysis (RQ-1)

To address RQ-1, the publication timeline of the selected studies was analysed to determine when research on gamification in information security has been published. The analysis, based on publications from 2012 to March 2026, shows a gradual increase in research output over the years, with a marked growth from 2019 onwards. The peak in recent years highlights an accelerating scholarly interest in gamification approaches for enhancing information and cybersecurity awareness. Fig. 6 presents the annual distribution of publications, illustrating these trends and indicating that the topic has gained substantial momentum

in the last few years, reflecting both technological developments and the increasing importance of security awareness programs in organisations.

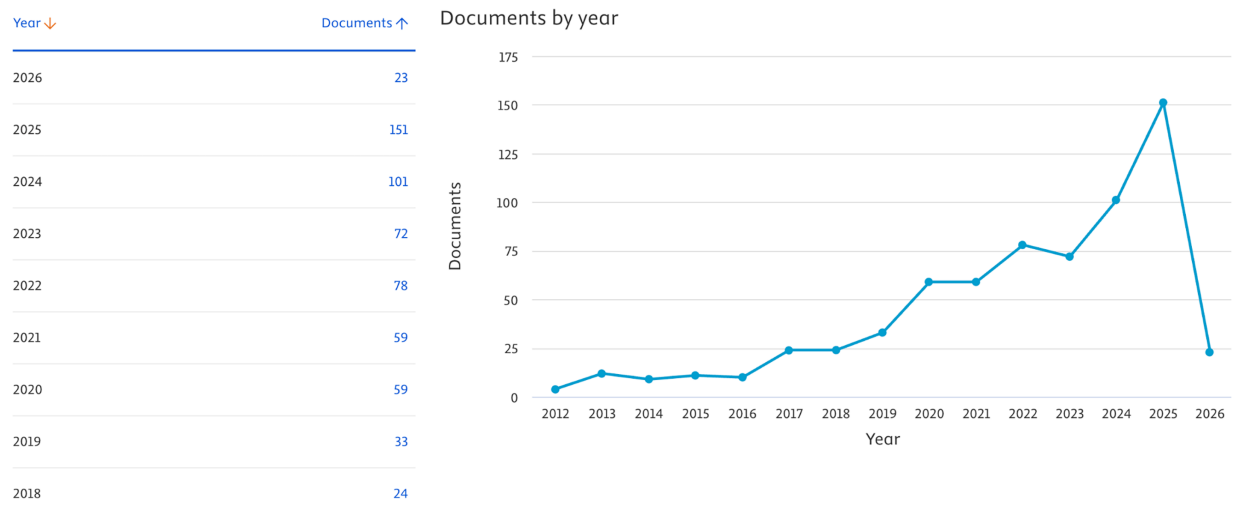


Figure 6: Annual distribution of Scopus documents by year (2012–March 2026).

The annual distribution of publications in the Web of Science (WoS) database is presented in Fig. 7. Between 2017 and March 2026, the number of publications on gamification in information security shows a gradual increase over time, reflecting a growing research interest, with a slight decrease observed in 2023. The highest output is observed in 2025, with 60 publications (20.13% of the total 298 records), followed by 2022 with 42 publications (14.09%) and 2024 also with 42 publications (14.09%). Moderate activity is seen in 2023 (32 publications, 10.74%), 2021 (29 publications, 9.73%), and 2020 (25 publications, 8.39%).

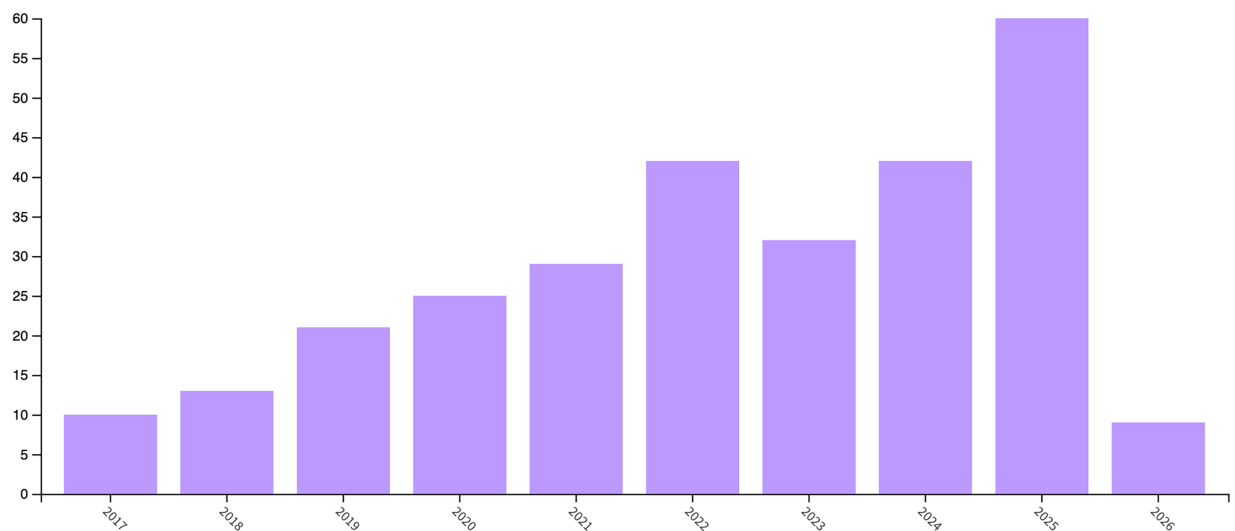


Figure 7: Annual distribution of Web of Science (WoS) documents by year (2017–March 2026).

Overall, these data indicate a growing interest in gamification applications in information security, peaking in the mid-2020s, which may correspond to increased awareness of cybersecurity challenges and the integration of gamified approaches in security training programs.

A slight decrease in publications observed in 2023 may be associated with a temporary slowdown in academic output, potentially influenced by the post-pandemic transition period, during which research priorities and funding structures were still adjusting after the COVID-19 disruption. Nevertheless, the overall trend remains upward, suggesting sustained and growing scholarly attention to the topic.

3.2 Keywords Occurrence Analysis (RQ-2 and RQ-3)

To address RQ-2, the selected studies were analysed to identify the specific areas in which gamification is applied within information security. The analysis indicates that gamification in information security is primarily applied in areas related to cybersecurity awareness, education, and training. The most dominant topics include security awareness programs, personnel training, e-learning environments, and cybercrime prevention. Additionally, gamification is frequently explored in the context of educational settings, particularly involving students and learning platforms, highlighting its role in improving engagement and knowledge retention.

Emerging application areas include domain-specific implementations such as healthcare, Internet of Things (IoT) environments, and organisational security practices. Furthermore, topics such as behavior change, user motivation, trust, and learning outcomes suggest a growing focus on human-centred and behavioural aspects. However, aspects related to performance evaluation, adoption, and real-world implementation remain less explored, indicating potential gaps in the literature.

To address RQ-3, the literature was examined to identify emerging trends and gaps for future research. The findings suggest that future research is likely to move towards more advanced, data-driven, and context-aware applications of gamification in information security. In particular, the emergence of keywords such as advanced analytics, machine learning, learning algorithms, and federated learning indicates an increasing integration of artificial intelligence and adaptive systems.

Future directions also point towards a stronger emphasis on personalised learning experiences, user behaviour analysis, and the effectiveness of gamified solutions in real-world environments. Additionally, there is a growing interest in domain-specific applications, including healthcare and IoT, as well as organisational contexts that require scalable and sustainable security awareness solutions.

Importantly, the limited focus on learning outcomes, user experience, and adoption highlights the need for more empirical and longitudinal studies. Therefore, future research should aim to evaluate the impact, usability, and long-term effectiveness of gamification approaches, as well as develop comprehensive frameworks that integrate technological, behavioural, and organisational perspectives.

The Most Occurring Keywords

Mendeley was used to remove duplicates after merging WoS and Scopus bibliographic data (955). Information about 611 articles was exported from Mendeley in RIS format and imported into VOSviewer. Type of analysis: Co-occurrence analysis, used to identify and visualise relationships between frequently occurring keywords in the selected literature. The minimum number of occurrences of a keyword was selected as 5. Of the 3531 keywords, 192 meet the threshold. There is no standard threshold for use in co-word analysis [20]. For each of the 192 keywords, the total strength of the co-occurrence links with other keywords was calculated. The keywords with the greatest total link strength were selected by VOSviewer. The number of keywords was selected: 192. 192 items grouped into 7 clusters. The network includes 4276 links, with a total link strength of 11,220, indicating a highly interconnected structure of terms within the literature. In the generated maps, nodes represent keywords, with sizes proportional to their frequency of occurrence, and the proximity between nodes reflects the strength of their co-occurrence relationships. The analysis highlights “cyber security” and “gamification” as the most prominent terms, while the clustering

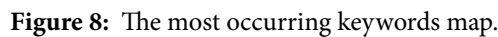
reveals distinct thematic groups, demonstrating how research on gamification in information security is organised around core topics such as security awareness, training, and incident response (See [Table 5](#)).

Table 5: Top 10 keywords extracted in the VOSviewer.

No.	Keyword	Occurrences	Total Link Strength
1.	gamification	375	2223
2.	cyber security	222	1571
3.	cybersecurity	197	1357
4.	students	91	701
5.	network security	74	554
6.	cyber-security educations	57	490
7.	personnel training	45	390
8.	computer crime	43	361
9.	e-learning	45	347
10.	education	49	319

VOSviewer was used to map and develop the keyword network, including co-occurrence, overlay, and density visualisations. In these maps, terms are represented as nodes of varying sizes, proportional to their frequency of occurrence. The terms are represented as nodes of varying sizes, proportional to the terms' recorded frequency. Additionally, the analysis indicates the frequency with which the terms appear in close proximity to one another [21]. The proximity of nodes on the map suggests the degree to which nodes were related in the literature [22].

Based on the co-occurrence map of the most frequently occurring keywords, particular attention can be drawn to less prominent terms such as “learning platform”, “cybersecurity training”, “online learning”, “performance”, “adoption”, “framework”, “healthcare”, “behavior change”, “cybersecurity gamification”, “trust”, “learning management systems”, “learning outcomes”, and “learning experiences” (See [Fig. 8](#)). The relatively lower frequency of these keywords suggests that, although they are present in the literature, they remain underexplored compared to core themes such as “cybersecurity” and “gamification”. This indicates that research has so far focused more on conceptual and awareness-related aspects, while practical implementation, evaluation of effectiveness, and user-centred outcomes have received comparatively less attention. In particular, the limited emphasis on learning outcomes, user experience, and adoption highlights potential research gaps, suggesting a need for more empirical studies assessing the impact and effectiveness of gamified approaches in real-world environments.



Early adopters in the literature shown in dark purple were concerned about cyber security, education computing, computer interaction, information systems, and computer games (See Fig. 9). Based on the overlay visualization of keywords, emerging trends can be observed in more recent publications, particularly around 2024. Keywords such as “advanced analytics”, “machine learning”, “learning algorithms”, and “federated learning” indicate a growing integration of artificial intelligence and data-driven approaches into gamification and information security research. At the same time, terms such as “cybersecurity awareness”, “organisational awareness”, “behavior change”, and “intrinsic motivation” suggest an increasing focus on user behaviour and human-centred security practices. The presence of application-oriented keywords, including “IoT”, “electronic health records”, “healthcare”, and “application”, highlights a shift towards domain-specific implementations of gamified solutions. Overall, these trends suggest that the field is evolving from general awareness and conceptual studies towards more advanced, personalised, and context-specific approaches that combine technological innovation with behavioural and organisational perspectives.

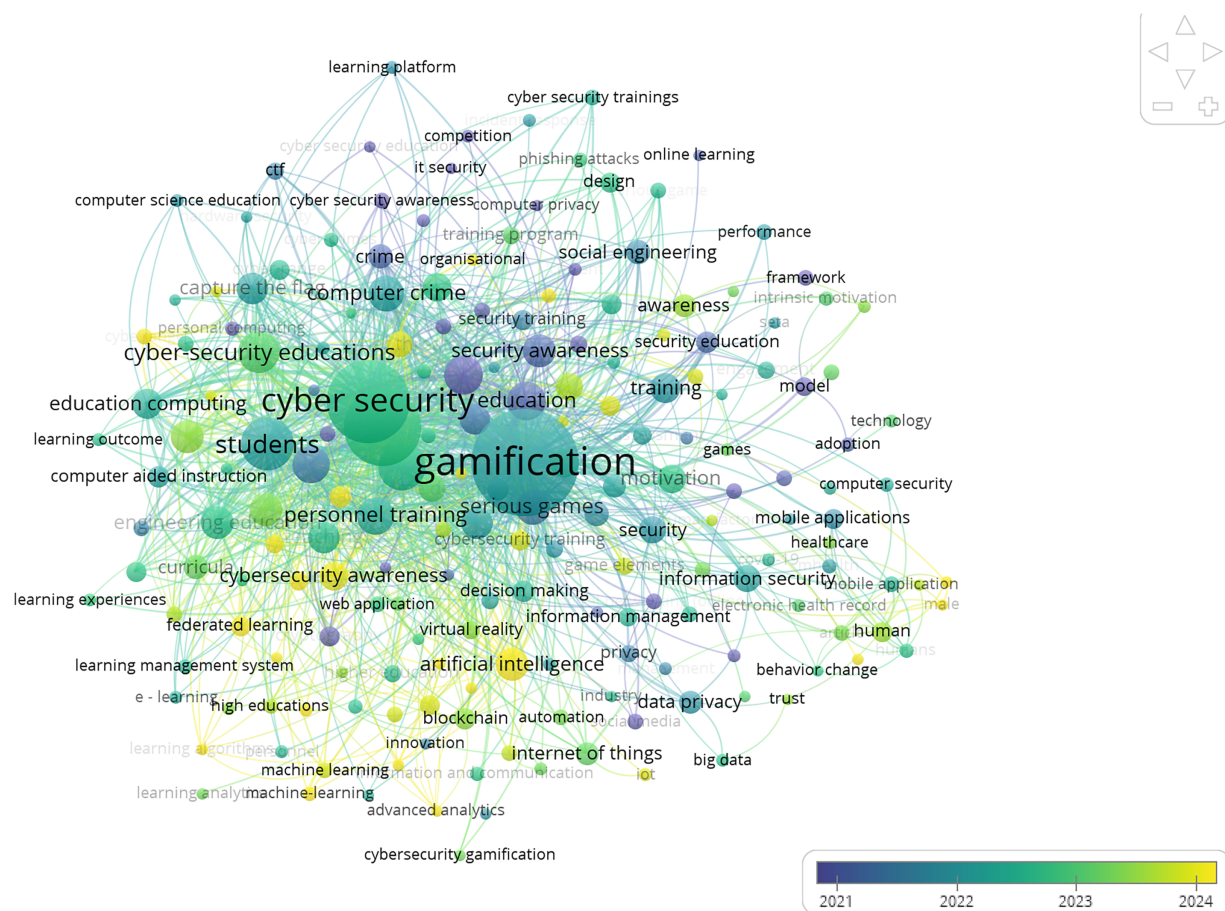


Figure 9: The overlay visualization of keywords.

Fig. 10 presents the density visualization of keywords, illustrating the most frequently occurring terms within the selected studies. The prominence of keywords such as “cybersecurity” and “gamification” confirms that the analysed articles are closely aligned with the defined search strategy. This serves as a validation of the study selection process, indicating that the applied keywords were appropriate and effective in identifying relevant literature. Furthermore, the concentration of related terms in the visualization highlights the consistency and coherence of the dataset. Overall, the results emphasise a strong focus on user engagement and behavioural aspects within information security research.

Overall, the keyword analysis demonstrates a well-structured and highly interconnected research landscape centred around core themes such as cybersecurity, gamification, and security awareness. The dominance of these keywords confirms the consolidation and maturity of the field, where research is strongly focused on improving user engagement and awareness through gamified approaches. At the same time, the presence of less frequent keywords highlights emerging and still underexplored areas, particularly related to practical implementation, user experience, learning outcomes, and the effectiveness of gamified solutions in real-world contexts.

of high-impact journals (Q1 and Q2 SJR quartiles), suggesting that influential research is largely produced in regions with well-established research infrastructures.

Key contributing authors, including Brilingaitė A., Di Nocera F., Gwenhure A. K., Lazarov W., Schafeitel-Tähtinen T., and Tempestini G., consistently appear across both databases, reflecting their central role in advancing the field. Analysis using ResearchRabbit confirmed that the most recent and conceptually related studies largely overlap with the selected dataset, further supporting the relevance of the identified countries and authors. Overall, these findings indicate that gamification research in information security is both globally relevant and concentrated among a network of leading researchers publishing in top-tier journals, highlighting areas of influence and potential collaboration for future studies.

3.3.1 Countries Participating in the Study

The distribution of publications by country or territory based on the Scopus search results from 2012 to March 2026 (See Fig. 11). The analysis shows that a substantial portion of records (129) is classified as undefined, indicating missing or unspecified country information. Among the identified countries, the United States leads with 99 publications, followed by India with 44 and the United Kingdom with 41 documents. These results suggest that, despite some limitations in data classification, research in this field is primarily concentrated in a few leading countries.

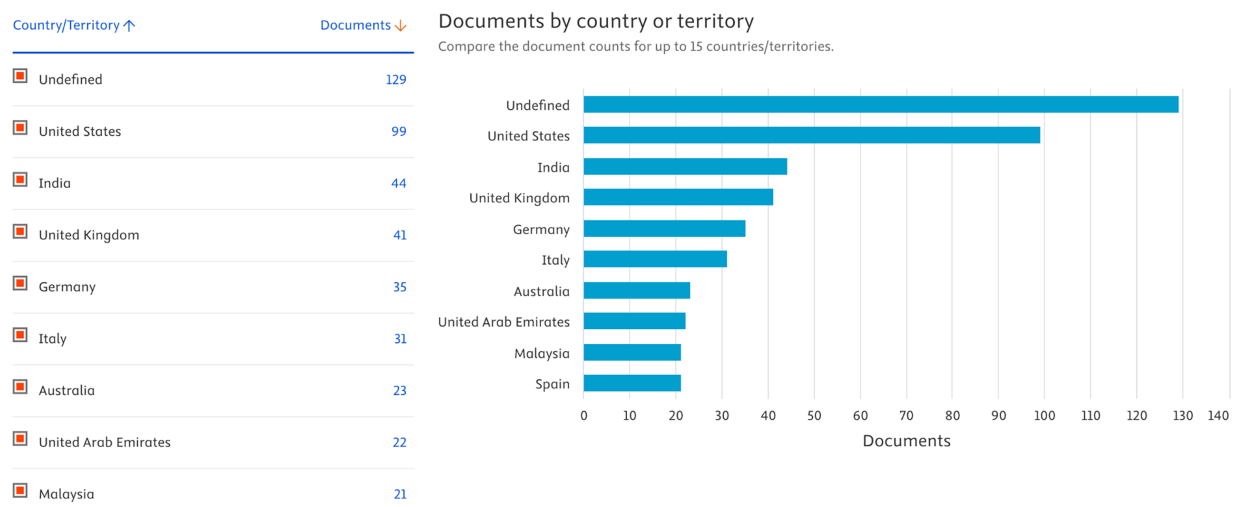


Figure 11: Overview of country or territory identified in the Scopus search results from 2012–March 2026.

The distribution of publications by country based on the Web of Science (WoS) search results from 2012 to March 2026 (See Fig. 12). The results indicate that the United States is the leading contributor with 58 publications, followed by Germany with 27 and England with 21 documents. A comparison with the Scopus data shows that both the United States and Germany demonstrate strong and consistent research output across both databases, with the United States also leading in Scopus and Germany contributing 35 publications. This highlights that research in this field is concentrated in countries with a well-established presence in both WoS and Scopus databases. This dominance can be explained by the strong research infrastructure, significant investment in cybersecurity, and the presence of leading academic and industrial institutions in these countries. Additionally, these countries place a high emphasis on cybersecurity awareness and education, which aligns closely with the application of gamification approaches in training and user engagement.



Figure 12: Overview of countries identified in the WoS search results from 2012–March 2026.

To address RQ-4, the selected articles were analysed to identify the countries contributing to research on gamification in information security. The analysis reveals a geographically diverse research landscape, with the United States leading in both Scopus (99 publications) and Web of Science (58 publications), followed by Germany (35 in Scopus, 27 in WoS) and the United Kingdom (41 in Scopus, 21 in WoS). Although some records were classified as undefined, the data indicate that research activity is concentrated in a few leading countries, reflecting established expertise and resources in cybersecurity and gamification. Overall, the trends suggest that while the field is attracting international attention, the majority of contributions originate from countries with strong research infrastructure and a focus on both technical and educational aspects of information security awareness. This pattern can also be associated with the presence of well-developed management schools, established standardisation frameworks, and advanced legal and regulatory environments in these countries, which support the development and implementation of structured cybersecurity practices.

It is noteworthy that although Japan is strong in the field of technology, research articles are selectively published in one database—WoS, while articles by Indian and Malaysian scientists appear in the Scopus database. This shows that data sharing depends not only on the research field, but also on the available article database.

3.3.2 *ResearchRabbit*

In addition to the keyword-based search conducted in Scopus and Web of Science, ResearchRabbit was used to analyse citation relationships between the selected publications. This platform supports the identification of influential studies, conceptually related publications, and additional research connected through citation networks. Therefore, this section presents the citation analysis of the retrieved studies, the analysis of conceptually related publications, and the evaluation of additional related studies identified through ResearchRabbit. The results provide additional evidence of the coverage and consistency of the selected literature.

ResearchRabbit utilized a citation-based approach, enabling users to explore research connections beyond keyword queries [23]. For data extraction, a total of 51 records were exported in BibTeX format from the Web of Science (WoS) database and 76 records from the Scopus database. The most relevant and representative studies were selected for further analysis in ResearchRabbit, and a total of 68 articles were transferred to the ResearchRabbit environment to explore citation relationships, research clusters, and emerging research trends related to gamification in information security.

Citation Analysis

The citation analysis revealed that the most highly cited publication is the 2017 article “Room escape at class: Escape games activities to facilitate the motivation and learning in computer science” by Borrego et al. [24], with 226 citations. This is followed by the 2021 article “Enhancing employees information security awareness in private and public organisations: A systematic literature review” by Khando et al. [25], which has received 218 citations. The third most cited study is the 2020 publication “Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling” by Dincelli and Chengalur-Smith [26], with 82 citations. The next most cited article is “Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)” by Alqahtani and Kavakli-Thorne (2020) [27], with 68 citations. These findings indicate that both early gamification applications in education and more recent studies focusing on security awareness have had a significant impact on the development of the field. It is noteworthy that, despite variations in the number of references (15–161), these studies are consistently used in research irrespective of their publication years (2017–2020), indicating their sustained relevance in the field.

Analysis of Conceptually Related Publications

The analysis of conceptually related studies identified through ResearchRabbit demonstrates that recent research on gamification in information security is characterised by a broad interdisciplinary scope. The identified publications cover not only cybersecurity education and awareness, but also human factors, digital learning environments, critical infrastructure protection, and the application of game-based approaches in different professional contexts. In addition, bibliometric approaches have been applied in related research areas to analyse emerging trends and the development of digital technologies across different domains [28].

Several recent studies indicate the growing interest in applying gamification principles to cybersecurity training and awareness development. Research has examined successful gamification approaches for cybersecurity training [29], the role of human factors in cybersecurity [30], and the use of gamified methods for improving information security awareness knowledge [31]. These studies demonstrate that gamification is increasingly considered as a complementary approach for addressing challenges related to user engagement, knowledge development, and security behaviour.

The identified literature also highlights the importance of educational approaches and learner-oriented environments. Studies have investigated gamification acceptance among learners with different levels of digital skills [32], game-based learning approaches in higher education [33], and gamified cybersecurity awareness courses supporting self-regulated learning [34]. In addition, research has explored the use of digital platforms and game-based environments for cybersecurity education, including approaches designed for younger learners and STEM-related education [35].

Beyond general cybersecurity awareness, recent research has expanded towards specialised security domains. Examples include the application of serious games for workforce development in critical infrastructure protection [36], cloud-based educational game platforms for cybersecurity learning [37], and serious games addressing hardware supply chain security through threat modelling approaches [38]. These studies

demonstrate that gamification is being adapted to different security contexts, ranging from general awareness training to specialised professional environments.

Research identified through the network analysis also reflects the connection between cybersecurity education and behavioural aspects. Several studies investigate how gamification can support learning experiences, user participation, and practical security skill development. For example, gamified approaches have been explored in software quality improvement contexts [39], cybersecurity concept learning among students [40], and informal learning strategies for improving cybersecurity awareness among young adults [41]. These findings indicate that gamification research is moving beyond simple reward-based mechanisms towards more complex learning experiences involving interaction, simulation, and practical engagement.

The ResearchRabbit analysis also identified studies demonstrating the expansion of gamification applications from general cybersecurity awareness towards more specialised training environments, practical exercises, and behavioural analysis. These publications indicate that researchers increasingly explore interactive approaches that combine cybersecurity knowledge acquisition with practical experience and user engagement.

A significant research direction focuses on cybersecurity training environments based on simulation, practical exercises, and scenario-based learning. Studies have investigated gamified cybersecurity awareness courses supporting self-regulated learning [34], serious games for hardware supply chain security using threat modelling approaches [38], and innovative cybersecurity awareness training models [42]. In addition, game-based training approaches have been explored in critical infrastructure protection and resilience contexts, demonstrating the potential of gamification for preparing users to respond to complex security situations [43].

Another emerging direction concerns interactive cybersecurity exercises and learning platforms. Research has examined technology-enhanced educational approaches for cybersecurity incident management [44], gamified approaches for mobile payment security adoption [45], and portable attack-and-defence cybersecurity exercises based on Capture-the-Flag concepts [46]. These studies highlight the movement towards practical learning environments where users can develop cybersecurity-related skills through active participation rather than traditional information delivery methods.

Recent publications also emphasise narrative-driven learning, usability evaluation, and user experience aspects of cybersecurity education. Research has explored story-driven gamified education for understanding security threats [47], cybersecurity educational game applications and their usability evaluation [48], and the role of immersive gamified platforms in understanding user behaviour during cybersecurity training [49]. These studies suggest that effective gamification requires not only the inclusion of game elements but also consideration of learner experience, interaction design, and contextual relevance.

Beyond educational settings, several studies investigate human behaviour and decision-making processes related to cybersecurity. Research has examined behavioural approaches to reducing the usability–security trade-off [50] and the use of board-game-based learning approaches to improve decision-makers’ understanding of cybersecurity complexity [51]. Furthermore, recent work has explored personalised and gamification-based cybersecurity approaches within organisational environments, including financial institutions [52]. These studies demonstrate increasing attention towards adapting gamification strategies to specific user groups and professional contexts.

The identified research network also indicates growing interest in applying gamification to different sectors and user populations. Studies have investigated the use of computer games for cybersecurity education in higher education institutions [53], showing that educational gamification remains one of the dominant application areas. Overall, the identified studies demonstrate a transition from basic awareness-oriented

gamification towards more complex approaches involving simulations, practical exercises, immersive environments, and context-specific cybersecurity learning scenarios.

Emerging Research Trends

The ResearchRabbit analysis further highlights the increasing role of gamification in cybersecurity education, professional training, and the development of practical security skills. The identified publications demonstrate that researchers are increasingly moving from theoretical discussions of gamification towards the design and evaluation of interactive learning environments.

Several studies focus on the integration of game-based approaches into educational processes. Research has examined the implementation of game-based learning strategies in higher education and the development of comprehensive processes for introducing game-based learning among educators [53,54]. In addition, gamification has been investigated as a method for improving cybersecurity concept learning among students, demonstrating its relevance for engaging younger generations in information security topics [40].

Another important research direction concerns cybersecurity exercises and practical skill development. Studies have explored Capture-the-Flag-based approaches as methods for teaching cybersecurity and investigated cyber ranges at different educational levels [46,55]. Furthermore, research has analysed scoring mechanisms and competition-based approaches in cybersecurity exercises, highlighting the importance of balanced evaluation methods in gamified security training environments [56].

Recent studies also indicate growing interest in applying gamification principles beyond traditional educational institutions. Research has explored gamification in software quality improvement contexts [39] and the use of game-based approaches for cybersecurity learning among students [40]. These studies demonstrate that gamification can support different forms of professional and academic skill development by creating interactive environments where users actively participate in problem-solving activities.

The literature identified through ResearchRabbit also includes studies focusing on awareness development among specific user groups. Research has investigated game-based informal learning strategies for improving cybersecurity awareness among young adults [57] with recent work further demonstrating the effectiveness of informal game-based learning for increasing cybersecurity awareness in this population [58]. In parallel, other studies have examined factors influencing information security awareness within organisational environments [59]. These studies emphasise that effective cybersecurity awareness requires consideration of users' characteristics, motivation, and learning context.

Further research directions include the development of innovative educational environments and adaptive learning approaches. Studies have explored digital educational escape rooms as novel approaches for cybersecurity education [41], cybersecurity training event generation for developing cyber-physical security skills [60], and balanced scoring approaches for cybersecurity exercises [56]. These works indicate that modern cybersecurity education increasingly combines gamification, simulation, and interactive technologies to create more engaging and realistic learning experiences.

The analysed literature identified through ResearchRabbit demonstrates a growing focus on adaptive, personalised, and context-aware learning approaches in gamification research for information security. These studies indicate that current research is increasingly focused not only on the implementation of game elements but also on improving the relevance, effectiveness, and adaptability of cybersecurity education.

Recent studies have investigated more advanced gamification approaches that incorporate adaptive learning and personalised training mechanisms. Research has explored multimodal and adaptive gamified systems designed to improve cybersecurity competence training [61], as well as broader analyses of gamification components and their application in organisational environments [62,63]. These studies suggest that

future gamification solutions may increasingly consider individual learner characteristics, professional roles, and specific security requirements.

Systematic reviews and broader frameworks identified in the research network further demonstrate the maturation of the field. Recent literature reviews have analysed serious games for improving privacy and security knowledge among professionals [64] and examined cybersecurity education frameworks from broader perspectives [65]. These studies contribute to understanding current research gaps and highlight the need for more structured evaluation of gamification effectiveness across different contexts.

The identified publications also show increasing attention towards specialised user groups and sector-specific cybersecurity challenges. Research has investigated cybersecurity education approaches for operational technology personnel in critical infrastructures [66], cybersecurity learning preferences among different populations [67], and professional training approaches based on cyberontological and gamification concepts [68]. These studies indicate that cybersecurity gamification is expanding beyond general awareness training towards targeted solutions for specific communities and professional environments.

Recent research has also explored innovative approaches for cybersecurity learning through narrative, competitive, and interactive methods. Studies have examined gamified cybersecurity education using narrative-driven approaches for teaching technical concepts [69], game-based assessment approaches for cybersecurity awareness among younger users [70], and tailored cybersecurity education frameworks developed for specific national or educational contexts [71]. These studies demonstrate the continuing diversification of gamification methods and their adaptation to different learning objectives.

The latest publications further highlight the importance of evaluating cybersecurity training effectiveness and understanding user engagement. Research has examined Capture-the-Flag-based cybersecurity education approaches [72], cybersecurity education frameworks incorporating behavioural and cultural aspects [71], and digital learning preferences for cybersecurity education among different user groups [67]. In addition, recent studies have explored gamification in cybersecurity courses and competitive learning environments, demonstrating the continued role of interactive approaches in developing cybersecurity competencies [73,74].

Additional publications identified through ResearchRabbit extend the research landscape towards broader cybersecurity education, interactive learning environments, and human-centred security approaches. Recent studies have investigated gamified cybersecurity learning environments by evaluating educational game usability, workload, and student engagement, demonstrating the importance of effective design and user experience in cybersecurity training [75,76]. Scenario-based approaches have also been explored as a method for developing professional information security skills by placing learners in realistic security situations [77]. In parallel, research on cybersecurity competitions, educational platforms, and supporting systems highlights the growing role of practical and collaborative approaches in developing cybersecurity competencies [78].

The analysed studies further demonstrate that gamification is increasingly combined with simulation, interactive technologies, and applied problem-solving activities. Research has examined gamified approaches for cybersecurity risk exploration in IT/OT infrastructures, showing the potential of game-based methods for professional security training beyond traditional educational environments [79]. Other studies have investigated gamification in computer science education, cybersecurity applications, and technology-supported learning environments, emphasising the role of motivation, engagement, and perceived usefulness in learning processes [80–83].

The literature also highlights the importance of human behaviour and awareness as key components of cybersecurity education. Research on social engineering attacks demonstrates the need to address human

vulnerabilities through effective awareness and training approaches [84]. Similarly, studies analysing digital technologies, behavioural impacts, and user interaction with emerging systems show that cybersecurity education increasingly requires consideration of user characteristics and technology adoption factors [85–87].

Furthermore, emerging cybersecurity challenges related to artificial intelligence, cyber-physical systems, and digital transformation indicate the growing complexity of security education requirements. Research on AI-related cybersecurity risks and explainable cyber-physical security solutions highlights the need for adaptive and multidisciplinary learning approaches that integrate technical knowledge with practical decision-making skills [88,89]. Studies addressing youth engagement and alternative educational approaches further demonstrate the expansion of cybersecurity learning towards broader audiences and innovative educational models [90].

Overall, the ResearchRabbit analysis indicates that research on gamification in information security is evolving from initial awareness-oriented applications towards more advanced, context-specific, and adaptive learning approaches. The identified studies demonstrate that gamification is primarily applied in three interconnected areas: cybersecurity awareness and training, educational environments, and practical security skill development through simulations, serious games, and interactive exercises. Recent research increasingly focuses on realistic scenarios, personalised learning, specialised user groups, and the evaluation of training effectiveness. Furthermore, the analysed publications reveal stronger connections between information security, education, human factors, and emerging technologies, indicating the interdisciplinary nature of this research field. Despite significant progress, the literature still shows a need for further empirical validation, long-term effectiveness evaluation, and the development of adaptive gamification strategies tailored to different organisational and educational contexts. The results were sorted by the most recent publications, displaying 68 records (See Fig. 13).

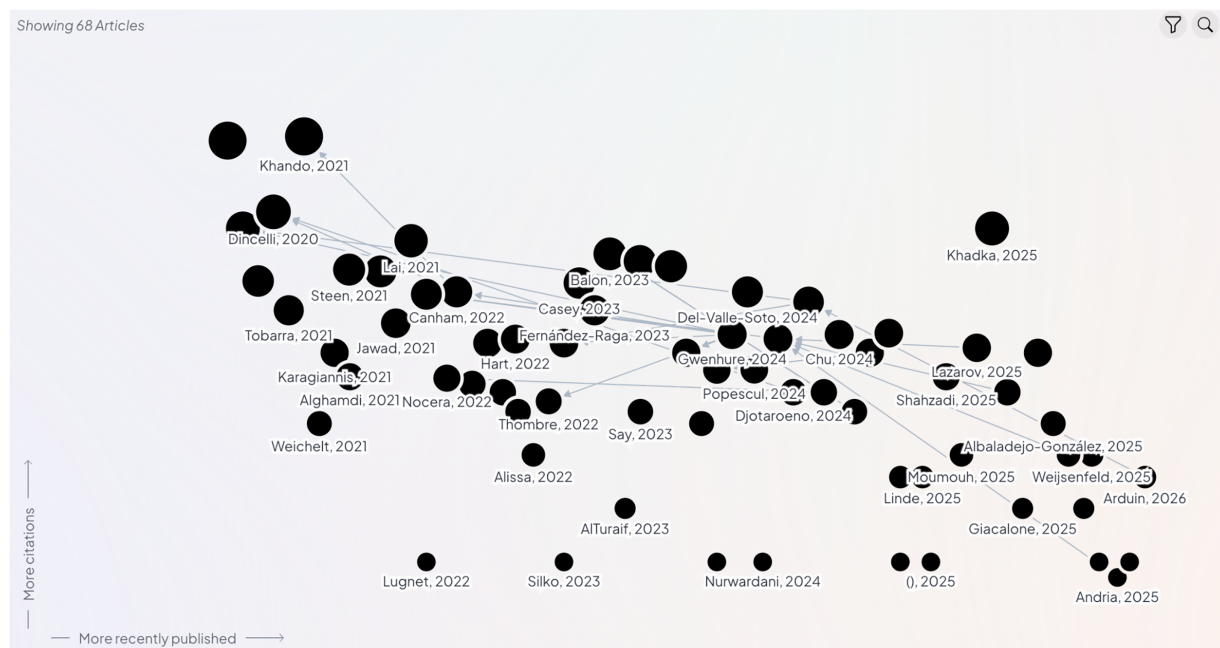


Figure 13: The most recent publications identified, with results limited to the 68 [10,24–90].

Additional Related Studies

The majority of conceptually related recent studies were already included in the selected dataset; therefore, no further analysis using the ResearchRabbit platform was conducted (See Fig. 14). In total, 18 additional “similar” studies were identified, confirming the coverage and completeness of the initial sample. One duplicate record was identified and removed. Several key works were both cited within the selected articles and identified as conceptually related. For instance, the study “From game design elements to gamefulness: defining “gamification” by Deterding et al. (2011) [14], was cited in 6 out of 68 selected articles and additionally identified among 3 similar studies. Other notable contributions include Gjertsen et al. article “Gamification of Information Security Awareness and Training” (2017) [3], Hendrix et al. article “Game Based Cyber Security Training: are Serious Games suitable for cyber security training?” (2016) [91], and Scholefield and Shepherd article “Gamification Techniques for Raising Cyber Security Awareness” (2019) [92], each cited in 3 selected articles and associated with 1–3 additional similar studies. The most recent study identified through this process is Hodhod et al. article “CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness” (2023) [93], which, although cited only once within the selected dataset, was linked to 2 additional similar studies. Overall, these findings demonstrate that both foundational and more recent studies are well integrated within the analysed sample. Considering the defined time frame and the applied inclusion and exclusion criteria, the identified “similar” studies that were not included in the final set of 68 articles fall outside the selected scope, further supporting the robustness and methodological consistency of the literature selection process.

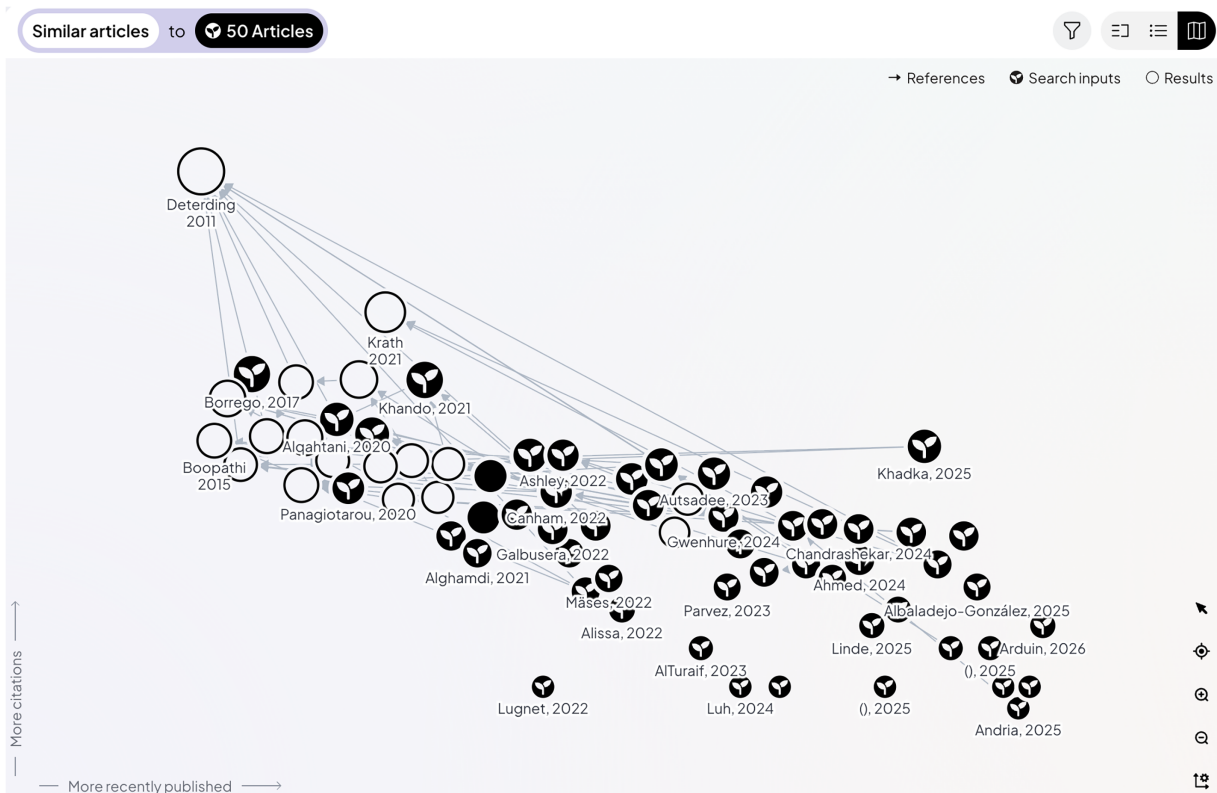


Figure 14: Identification of conceptually related studies based on the 50 most recent selected articles [3,14,91–105].

Additional conceptually related studies identified through ResearchRabbit further demonstrate the development of serious games and gamified approaches for cybersecurity awareness and education. These

publications, although not included in the final dataset, provide additional context regarding the evolution of gamification methods and their application in different learning environments. Several studies focus on the development of adaptive and serious game-based solutions designed to improve cybersecurity awareness. For example, CyberHero was proposed as an adaptive serious game aimed at promoting cybersecurity awareness [93], while other research has examined the theoretical foundations of gamification, serious games, and game-based learning, highlighting the importance of underlying motivational and educational principles [94].

The identified literature includes studies addressing cybersecurity education for students and young learners. Research has explored the use of gamification for teaching cybersecurity concepts [95], game-based cybersecurity training for high school students [96], and augmented reality-based approaches for cybersecurity education through interactive environments [97]. These studies indicate that gamification is increasingly applied at earlier educational stages to develop cybersecurity awareness and improve learners' engagement with security-related topics.

Other related publications investigate serious games designed for specific cybersecurity skills and awareness objectives. Studies have proposed serious games for improving software security awareness [98], educating users about cybersecurity requirements through dedicated learning games [99], and raising general cybersecurity awareness through simulation-based approaches such as Riskio [100]. In addition, gamified attacker-defender models have been explored as a method for cybersecurity assessment and education, demonstrating the potential of competitive and role-based learning scenarios [101].

Recent related research also highlights the growing use of immersive and narrative-based learning approaches. Virtual escape rooms have been developed to increase cybersecurity awareness by combining problem-solving activities with game mechanics [102]. Similarly, cybersecurity awareness frameworks based on gamification principles have been proposed for high school students and broader educational contexts [103,104]. Furthermore, detective-themed serious games have been investigated as alternative approaches for cybersecurity education, demonstrating the potential of storytelling and scenario-based learning to improve user engagement [105].

Overall ResearchRabbit Findings

Overall, the ResearchRabbit-related publications complement the findings of the main systematic literature review by providing an additional citation-driven perspective on the development of gamification in information security. The identified related studies demonstrate that the field is increasingly moving towards adaptive, immersive, and scenario-based learning environments, with a strong emphasis on serious games, simulations, and interactive experiences for improving cybersecurity awareness and developing practical security competencies. The analysis also confirmed that most influential and conceptually relevant studies were already captured within the selected dataset, indicating a high level of coverage and consistency of the review process. The identification of additional similar studies further supported the completeness of the sample, while their exclusion based on predefined time frame and inclusion/exclusion criteria demonstrates the methodological rigour of the study. Furthermore, the presence of both highly cited foundational studies and recent contributions highlights the continuity and evolution of research in this field. Taken together, these findings demonstrate that the analysed dataset provides a reliable and comprehensive basis for further systematic analysis of gamification applications in information security.

3.3.3 The Authors

The analysis of leading authors was conducted based on data extracted from both Web of Science (WoS) and Scopus databases, including 51 records from WoS and 76 records from Scopus. The comparison aimed to identify the most active contributors in the field of gamification in information security.

The results indicate that several authors consistently appear across both datasets, including Brilingaitė A., Di Nocera F., Gwenhure A. K., Lazarov W., Schafeitel-Tähtinen T., and Tempestini G. (See [Table 6](#)). The recurrence of these authors in both databases highlights their significant and continuous contribution to the research area.

Table 6: Overview of authors identified in the Web of Science (WoS) and Scopus search results.

No.	Authors	Count
1.	Brilingaitė A	2
2.	Di Nocera F.	2
3.	Gwenhure A. K.	2
4.	Lazarov W.	2
5.	Schafeitel-Tähtinen T.	2
6.	Tempestini G.	2

Overall, the findings suggest that while the field involves a broad range of researchers, a smaller group of authors demonstrates higher research productivity and visibility. This pattern reflects a developing research domain where key contributors play an important role in shaping the direction and advancement of gamification in information security studies.

3.3.4 SCImago Journal Rank

The selected studies were further evaluated based on SCImago Journal Rank (SJR) quartiles (Q1–Q4) to assess the quality and impact of the publication sources. The analysis focused on a total of 75 journals after duplicate removal. Among these, two journals were not indexed in the SCImago Journal & Country Rank (SJR) system and therefore were not assigned a quartile ranking. The distribution of the top 10 journals is presented in [Table 7](#).

Table 7: The distribution of the top 10 journals.

No.	Journal	Publisher	Count
1.	IEEE Access	IEEE	6
2.	Information (Switzerland)	MDPI	6
3.	Sustainability (Switzerland)	MDPI	4
4.	Applied Sciences (Switzerland)	MDPI	3
5.	Computers and Security	Elsevier	3
6.	International Journal of Serious Games	Serious Games Society	3
7.	Journal of Cybersecurity and Privacy	MDPI	2
8.	Frontiers in Education	Frontiers Media S.A.	2
9.	Ingenierie des Systemes d'Information	International Information and Engineering Technology Association	2
10.	Technology, Knowledge and Learning	Springer Science + Business Media	2

The selected studies were published across a variety of journals, with the distribution of articles shown in Table 7. The most frequent sources included IEEE Access and Information (Switzerland), each contributing 6 articles, followed by Sustainability (Switzerland) with 4 articles, and Applied Sciences (Switzerland), Computers and Security, and International Journal of Serious Games, each contributing 3 articles. Several journals, including Journal of Cybersecurity and Privacy, Frontiers in Education, Ingenierie Des Systemes d'Information, and Technology, Knowledge and Learning, contributed 2 articles each.

Analysis of the SCImago Journal Rank (SJR) quartiles revealed that the majority of these journals are ranked in Q1 and Q2, indicating that the selected studies are predominantly published in high- to mid-impact journals.

This distribution shows a strong dominance of open-access publishers such as MDPI, indicating a trend toward increased accessibility and rapid dissemination of cybersecurity and gamification research (See Table 7). Traditional publishers such as IEEE and Elsevier are also present, reflecting the technical foundation and established academic credibility of the field.

Fig. 15 shows the distribution of the selected journals based on their SCImago Journal Rank (SJR) quartiles. Of the 75 journals included in the analysis, 39 are classified as Q1, 24 as Q2, 9 as Q3, and 3 as Q4. The predominance of Q1 and Q2 journals indicates that the majority of research on gamification in information security is published in high-impact outlets, reflecting the academic relevance and quality of the field. The journals were selected following predefined inclusion and exclusion criteria, including document type (Scopus: articles and reviews; WoS: articles and review articles), subject areas (Computer Science, Engineering, Education Educational Research, and Social Sciences), language (English), and open access availability. As a result, the dataset includes both open-access journals from established publishers, ensuring a balance between accessibility and academic quality.

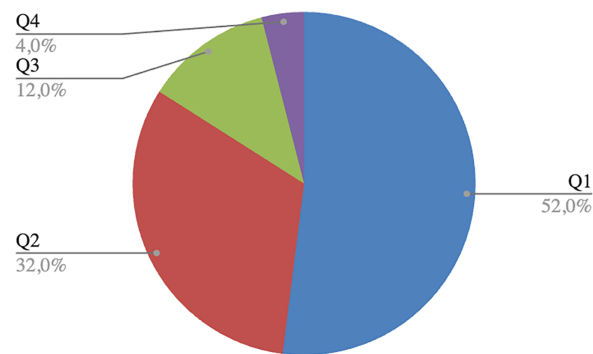


Figure 15: The distribution of selected journals by SJR quartile ranking.

Overall, the SJR-based evaluation demonstrates that the selected studies are predominantly published in high-quality and reputable journals, with a clear concentration in Q1 and Q2 quartiles. This distribution confirms the academic maturity and growing significance of research on gamification in information security. The presence of both leading open-access publishers and established traditional publishers further indicates a balanced publication landscape that supports both accessibility and scholarly rigour. Moreover, the application of well-defined inclusion and exclusion criteria ensured the consistency and reliability of the dataset. Taken together, these findings suggest that the analysed literature provides a robust and credible foundation for understanding current developments and future directions in the field.

4 Discussion

The findings of this study highlight the growing importance of gamification in the field of information security, particularly in the context of cybersecurity awareness and training. The dominance of keywords such as “gamification” and “cybersecurity” confirms that the research area is well-established and primarily focused on improving user engagement and awareness through interactive approaches. At the same time, the concentration of studies in Computer Science, Engineering, and Education reflects the interdisciplinary nature of the field, where technical solutions are closely integrated with educational strategies to address human-related security challenges.

The analysis also reveals a shift in recent research towards more advanced and data-driven approaches. The emergence of keywords related to machine learning, advanced analytics, and federated learning suggests that gamification is increasingly being combined with artificial intelligence to develop adaptive and personalized security awareness solutions. In addition, the appearance of domain-specific terms such as healthcare and IoT indicates that gamified approaches are being extended to more specialised and high-risk environments, where security awareness is particularly critical.

Despite these advancements, several gaps remain evident. Less prominent keywords related to learning outcomes, user experience, adoption, and performance evaluation indicate that the effectiveness of gamified solutions is still not sufficiently explored. This suggests that existing research has focused more on conceptual development and awareness-raising rather than on rigorous empirical validation in real-world contexts. Furthermore, the uneven distribution of publications across countries highlights the concentration of research in regions with strong academic infrastructure, suggesting the need for broader geographical representation.

From a practical perspective, the analysis indicates that gamification in information security is most commonly implemented through serious games, simulation-based training, and reward systems such as badges and points. These approaches are primarily used to enhance security awareness and training effectiveness by increasing user engagement and motivation. However, less attention is given to adaptive gamification and personalised learning systems, which remain underexplored in the literature.

In terms of target groups, most studies focus on employees and students, particularly in organisational and educational contexts, while non-IT professionals and specialised sectors such as healthcare and critical infrastructure receive comparatively less attention. This suggests that current research is still concentrated on general user populations rather than highly specific or high-risk environments. These findings highlight the need for future research to explore more context-specific and adaptive gamification strategies tailored to different user groups.

Compared to previous systematic reviews in this field, which often rely on limited keyword sets, single database searches, or purely descriptive mapping, this study provides a more comprehensive analysis by integrating both Scopus and Web of Science databases and applying a broader keyword strategy. In addition, this study combines bibliometric mapping with systematic literature review principles, allowing for a more structured overview of thematic evolution, research gaps, and interdisciplinary connections in gamification within information security.

Finally, the evaluation of publication sources demonstrates that the field is supported by high-quality research, with the majority of studies published in Q1 and Q2 journals. The presence of both open-access and traditional publishers reflects a balance between accessibility and academic rigour. Overall, the findings suggest that while gamification in information security has reached a level of maturity, future research should focus on empirical validation, user-centred design, and the integration of advanced technologies to enhance the effectiveness and scalability of gamified security solutions.

5 Conclusions

This systematic literature review provides a comprehensive overview of research on gamification in information security from 2012 to March 2026, based on publications indexed in Scopus and Web of Science. The findings indicate that gamification is predominantly applied to enhance cybersecurity awareness, security training programs, and user behaviour change, with “cybersecurity” and “gamification” emerging as the most central and strongly interconnected keywords across the analysed literature.

The results further show that the research field is primarily situated within Computer Science and Engineering, with an additional contribution from Education and Social Sciences, reflecting its interdisciplinary nature. The publication landscape is dominated by high-impact journals (Q1 and Q2), indicating strong academic quality and relevance. In terms of geographical distribution, the United States and Germany represent the leading contributors, suggesting that research activity is concentrated in countries with well-established research infrastructures, strong digital governance frameworks, and advanced cybersecurity policies.

The keyword and temporal analyses reveal a clear evolution of the field, moving from foundational gamification concepts towards more advanced and applied approaches. Recent studies increasingly integrate technologies such as machine learning, advanced analytics, and federated learning, as well as domain-specific applications including healthcare, IoT environments, and organisational security contexts. At the same time, the presence of behavioural constructs such as trust, intrinsic motivation, and behaviour change highlights the continued importance of human-centred perspectives in security research.

Despite this progress, several research gaps remain evident. In particular, limited attention has been given to longitudinal evaluations, empirical validation of gamified interventions, user experience analysis, and standardised frameworks for measuring effectiveness. Additionally, uneven geographical distribution of studies suggests the need for broader international participation, particularly from underrepresented regions. These limitations indicate that much of the existing research remains conceptual or exploratory rather than fully validated in real-world environments.

Overall, the results show that research on gamification in information security is growing and becoming more advanced, but it is still not fully mature. Most studies focus on concepts and general ideas rather than real-world testing. This means that while the topic is widely studied, there is still a need for more practical and long-term research that tests how effective gamification really is in the field of information security.

6 Limitations and Future Research Directions

This study has several limitations that should be acknowledged. First, only English-language publications were included, which may introduce language bias. Second, the study primarily focuses on bibliometric and mapping analysis, and does not include a detailed methodological quality assessment of individual studies. In addition, journal-level indicators such as SJR quartiles were used instead of full study-level quality appraisal.

Future research could extend this work by including additional databases such as IEEE Xplore or SpringerLink to ensure broader coverage. More in-depth qualitative systematic reviews using formal quality assessment tools (e.g., CASP) could also complement the findings. Furthermore, future studies could explore the effectiveness of different gamification techniques in information security and investigate their impact across different industries and user groups.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Indre Grigaraviciute; methodology, Indre Grigaraviciute and Nikolaj Goranin; software, Indre Grigaraviciute; validation, Indre Grigaraviciute and Nikolaj Goranin; formal analysis, Indre Grigaraviciute; investigation, Indre Grigaraviciute; resources, Indre Grigaraviciute; data curation, Indre Grigaraviciute; writing—original draft preparation, Indre Grigaraviciute; writing—review and editing, Indre Grigaraviciute and Nikolaj Goranin; visualization, Indre Grigaraviciute; supervision, Nikolaj Goranin; project administration, Indre Grigaraviciute; funding acquisition, Indre Grigaraviciute. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Supplementary Materials: The supplementary material is available online at <https://www.techscience.com/doi/10.32604/cmc.2026.084893/s1>.

References

1. Sharif KH, Ameen SY. A review of security awareness approaches with special emphasis on gamification. In: Proceedings of the 2020 International Conference on Advanced Science and Engineering (ICOASE); 2020 Dec 23–24; Duhok, Iraq. p. 151–6. doi:10.1109/icoase51841.2020.9436595.
2. Aldemir T, Çelik B, Kaplan G. A qualitative investigation of student perceptions of game elements in a gamified course. *Comput Hum Behav*. 2018;78(2):235–54. doi:10.1016/j.chb.2017.10.001.
3. Gjertsen E, Gjære EA, Bartnes M, Flores W. Gamification of information security awareness and training. In: Proceedings of the 3rd International Conference on Information Systems Security and Privacy; 2017 Feb 19–21; Porto, Portugal.
4. Barata G, Gama S, Jorge J, Gonçalves D. Studying student differentiation in gamified education: a long-term study. *Comput Hum Behav*. 2017;71(1):550–85. doi:10.1016/j.chb.2016.08.049.
5. Chen CM, Li MC, Chen TC. A web-based collaborative reading annotation system with gamification mechanisms to improve reading performance. *Comput Educ*. 2020;144(11):103697. doi:10.1016/j.compedu.2019.103697.
6. Martí-Parreño J, Méndez-Ibáñez E, Alonso-Arroyo A. The use of gamification in education: a bibliometric and text mining analysis. *Comput Assist Learn*. 2016;32(6):663–76. doi:10.1111/jcal.12161.
7. Sharif KH, Ameen SY. A review on gamification for information security training. In: Proceedings of the 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI); 2021 Dec 4–6; Sana'a, Yemen. p. 1–8. doi:10.1109/mticti53925.2021.9664771.
8. Nguyen TA, Pham H. A design theory-based gamification approach for information security training. In: Proceedings of the 2020 RIVF International Conference on Computing and Communication Technologies (RIVF); 2020 Oct 14–15; Ho Chi Minh City, Vietnam. p. 1–4. doi:10.1109/rivf48685.2020.9140730.
9. Pahlavanpour O, Gao S. A systematic mapping study on gamification within information security awareness programs. *Heliyon*. 2024;10(19):e38474. doi:10.1016/j.heliyon.2024.e38474.
10. Gwenhure AK, Sapty Rahayu F. Gamification of cybersecurity awareness for non-IT professionals: a systematic literature review. *Int J Serious Games*. 2024;11(1):83–99. doi:10.17083/ijsg.v11i1.719.
11. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA, 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*. 2021;372:n71. doi:10.1136/bmj.n71.
12. Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering (EBSE Technical Report EBSE-2007-01). Keele, UK, Durham, UK: Keele University; 2007.
13. Prancutė R. Web of science (WoS) and Scopus: the titans of bibliographic information in today's academic world. *Publications*. 2021;9(1):12. doi:10.3390/publications9010012.

14. Deterding S, Dixon D, Khaled R, Nacke L. From game design elements to gamefulness: defining “gamification”. In: *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*; 2011 Sep 28–30; Tampere, Finland. p. 9–15. doi:10.1145/2181037.2181040.
15. Harwood T, Garry T. An investigation into gamification as a customer engagement experience environment. *J Serv Mark*. 2015;29(6/7):533–46. doi:10.1108/jsm-01-2015-0045.
16. Robson K, Plangger K, Kietzmann JH, McCarthy I, Pitt L. Is it all a game? Understanding the principles of gamification. *Bus Horiz*. 2015;58(4):411–20. doi:10.1016/j.bushor.2015.03.006.
17. Carrera-Rivera A, Ochoa W, Larrinaga F, Lasa G. How-to conduct a systematic literature review: a quick guide for computer science research. *MethodsX*. 2022;9(1):101895. doi:10.1016/j.mex.2022.101895.
18. Dybå T, Dingsøyr T. Empirical studies of agile software development: a systematic review. *Inf Softw Technol*. 2008;50(9–10):833–59. doi:10.1016/j.infsof.2008.01.006.
19. Kalibatiene D, Miliauskaitė J. A systematic mapping with bibliometric analysis on information systems using ontology and fuzzy logic. *Appl Sci*. 2021;11(7):3003. doi:10.3390/app11073003.
20. van Eck NJ, Waltman L. Visualizing bibliometric networks. In: Ding Y, Rousseau R, Wolfram D, editors. *Measuring scholarly impact: methods and practice*. Cham, Switzerland: Springer; 2014. p. 285–320. doi:10.1007/978-3-319-10377-8_13.
21. Ali Bukar U, Sayeed MS, Razak SFA, Yogarayan S, Amodu OA, Mahmood RAR. A method for analyzing text using VOSviewer. *MethodsX*. 2023;11(1):102339. doi:10.1016/j.mex.2023.102339.
22. Narong DK, Hallinger P. A keyword co-occurrence analysis of research on service learning: conceptual foci and emerging research trends. *Educ Sci*. 2023;13(4):339. doi:10.3390/educsci13040339.
23. Gunaseelan S, Chandrakasan R, Sumathi M. Research rabbit: an AI-powered scholarly discovery tool for comprehensive literature exploration. In: *Digital transformations for sustainable libraries methods and strategies*. New Delhi, India: Ess Ess Publications; 2025. p. 109–16. doi:10.5281/zenodo.16785247.
24. Borrego C, Fernández C, Blanes I, Robles S. Room escape at class: escape games activities to facilitate the motivation and learning in computer science. *J Technol Sci Educ*. 2017;7(2):162. doi:10.3926/jotse.247.
25. Khando K, Gao S, Islam SM, Salman A. Enhancing employees information security awareness in private and public organisations: a systematic literature review. *Comput Secur*. 2021;106(3):102267. doi:10.1016/j.cose.2021.102267.
26. Dincelli E, Chengalur-Smith IS. Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *Eur J Inf Syst*. 2020;29(6):669–87.
27. Alqahtani H, Kavakli-Thorne M. Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information*. 2020;11(2):121. doi:10.3390/info11020121.
28. Autsadee Y, Jeevan J, Bin Mohd Salleh NH, Bin Othman MR. Digital tools and challenges in human resource development and its potential within the maritime sector through bibliometric analysis. *J Int Marit Saf Environ Aff Shipp*. 2023;7(4):2286409. doi:10.1080/25725084.2023.2286409.
29. van Steen T, Deeelman JRA. Successful gamification of cybersecurity training. *Cyberpsychol Behav Soc Netw*. 2021;24(9):593–8. doi:10.1089/cyber.2020.0526.
30. Khadka K, Ullah AB. Human factors in cybersecurity: an interdisciplinary review and framework proposal. *Int J Inf Secur*. 2025;24(3):119. doi:10.1007/s10207-025-01032-0.
31. Wu T, Tien KY, Hsu WC, Wen FH. Assessing the effects of gamification on enhancing information security awareness knowledge. *Appl Sci Switz*. 2021;11(19):9266. doi:10.3390/app11199266.
32. Panagiotarou A, Stamatou YC, Pierrakeas C, Kameas A. Gamification acceptance for learners with different E-skills. *Int J Learn Teach Educ Res*. 2020;19(2):263–78. doi:10.26803/ijlter.19.2.16.
33. Fernández-Raga M, Aleksić D, İkiz AK, Markiewicz M, Streit H. Development of a comprehensive process for introducing game-based learning in higher education for lecturers. *Sustainability*. 2023;15(4):3706. doi:10.3390/su15043706.
34. Tran TM, Beuran R, Hasegawa S. Gamification-based cybersecurity awareness course for self-regulated learning. *Int J Inf Educ Technol*. 2023;13(4):724–30. doi:10.18178/ijiet.2023.13.4.1859.
35. Canham M, Posey C, Constantino M. Phish derby: shoring the human shield through gamified phishing attacks. *Front Educ*. 2022;6:807277. doi:10.3389/educ.2021.807277.

36. Ashley TD, Kwon R, Gourisetti SNG, Katsis C, Bonebrake CA, Boyd PA. Gamification of cybersecurity for workforce development in critical infrastructure. *IEEE Access*. 2022;10:112487–501. doi:10.1109/access.2022.3216711.
37. Tobarra L, Utrilla A, Robles-Gómez A, Pastor-Vargas R, Hernández R. A cloud game-based educative platform architecture: the CyberScratch project. *Appl Sci*. 2021;11(2):807. doi:10.3390/app11020807.
38. Hart S, Halak B, Sassone V. CIST: a serious game for hardware supply chain. *Comput Secur*. 2022;122(1):102912. doi:10.1016/j.cose.2022.102912.
39. Say B, Altunel H, Kosa M, Koca-Atabey M. Evaluation of an industrial case of gamification in software quality improvement. *Int J Serious Games*. 2023;10(3):23–42. doi:10.17083/ijsg.v10i3.594.
40. Thombre S, Velankar M. Gamification by Students: an effective approach to cyber security concept learning. *J Eng Educ Transform*. 2022;36(S1):73–81. doi:10.16920/jeet/2022/v36is1/22178.
41. Keller T, Guggemos J, Warwas J. Digital educational escape rooms as a novel approach to cybersecurity education: an empirical study on learner perceptions of usefulness and usability. *Comput Hum Behav Rep*. 2025;20(3):100785. doi:10.1016/j.chbr.2025.100785.
42. Taherdoost H. Towards an innovative model for cybersecurity awareness training. *Information*. 2024;15(9):512. doi:10.3390/info15090512.
43. Galbusera L, Cardarilli M, Gómez Lara M, Giannopoulos G. Game-based training in critical infrastructure protection and resilience. *Int J Disaster Risk Reduct*. 2022;78(3):103109. doi:10.1016/j.ijdrr.2022.103109.
44. Pirta-Dreimane R, Brilingaitė A, Roponen E, Parish K, Grabis J, Lugo RG, et al. Try to esCAPE from cybersecurity incidents! a technology-enhanced educational approach. *Technol Knowl Learn*. 2025;30(3):1577–606. doi:10.1007/s10758-024-09769-8.
45. Lai PC, Liew EJY. Towards a cashless society: the effects of perceived convenience and security on gamified mobile payment platform adoption. *Australas J Inf Syst*. 2021;25:1–25. doi:10.3127/ajis.v25i0.2809.
46. Karagiannis S, Ntantogian C, Magkos E, Ribeiro LL, Campos L. PocketCTF: a fully featured approach for hosting portable attack and defense cybersecurity exercises. *Information*. 2021;12(8):318. doi:10.3390/info12080318.
47. Rikkers V, Sarmah DK. A story-driven gamified education on USB-based attack. *J Comput High Educ*. 2025;37(1):248–72. doi:10.1007/s12528-023-09392-z.
48. Ahmed A, Watterson C, Alhashmi S, Gaber T. How universities teach cybersecurity courses online: a systematic literature review. *Front Comput Sci*. 2024;6:1499490. doi:10.3389/fcomp.2024.1499490.
49. Donekal Chandrashekar N, Lee A, Azab M, Gracanin D. Understanding user behavior for enhancing cybersecurity training with immersive gamified platforms. *Information*. 2024;15(12):814. doi:10.3390/info15120814.
50. Di Nocera F, Tempestini G. Getting rid of the usability/security trade-off: a behavioral approach. *J Cybersec Priv*. 2022;2(2):245–56. doi:10.3390/jcp2020013.
51. Zeijlemaker S, Rouwette EAJA, Cunico G, Armenia S, von Kutzschenbach M. Decision-makers' understanding of cyber-security's systemic and dynamic complexity: insights from a board game for bank managers. *Systems*. 2022;10(2):49. doi:10.3390/systems10020049.
52. Shahzadi A, Ishaq K, Nawaz NA, Rosdi F, Ali Khan F. Unveiling personalized and gamification-based cybersecurity risks within financial institutions. *PeerJ Comput Sci*. 2025;11(5):e2598. doi:10.7717/peerj-cs.2598.
53. Alghamdi MY, Younis YA. The use of computer games for teaching and learning cybersecurity in higher education institutions. *J Eng Res*. 2021;9(3):143–52. doi:10.36909/jer.v9i3a.10943.
54. Georgiou T, Baillie L, Chatzifoti O, Chan SC. Future forums: a methodology for exploring, gamifying, and raising security awareness of code-citizens. *Int J Hum Comput Stud*. 2023;169(4):102930. doi:10.1016/j.ijhcs.2022.102930.
55. Lazarov W, Schafeitel-Tähtinen T, Squillace J, Martinasek Z, Coufalikova A, Helenius M, et al. Lessons learned from using cyber range to teach cybersecurity at different levels of education. *Technol Knowl Learn*. 2025;16(5):2945. doi:10.1007/s10758-025-09840-y.
56. Mäses S, Maennel K, Brilingaitė A. Trends and challenges for balanced scoring in cybersecurity exercises: a case study on the example of Locked Shields. *Front Educ*. 2022;7:958405. doi:10.3389/educ.2022.958405.
57. Tempestini G, Merà S, Palange MP, Bucciarelli A, Di Nocera F. Improving the cybersecurity awareness of young adults through a game-based informal learning strategy. *Information*. 2024;15(10):607. doi:10.3390/info15100607.

58. Albaladejo-González M, Nespoli P, Gómez Mármol F, Ruipérez-Valiente JA. A multimodal and adaptive gamified system to improve cybersecurity competence training. *Cluster Comput.* 2025;28(9):567. doi:10.1007/s10586-025-05264-6.
59. Djotaroeno M, Beulen E. Information security awareness in the insurance sector: cognitive and internal factors and combined recommendations. *Information.* 2024;15(8):505. doi:10.3390/info15080505.
60. Vineetha Harish A, Tam K, Jones K. Generating training events for building cyber-physical security skills. *Comput J.* 2025;68(5):445–59. doi:10.1093/comjnl/bxae123.
61. Alissa KA, Aldeeb BA, Alshehri HA, Dahdouh SA, Alsubaie BM, Alghamdi AM, et al. Applying tracking game system to measure user behavior toward cybersecurity policies. *Int J Electr Comput Eng (IJECE).* 2022;12(5):5164. doi:10.11591/ijece.v12i5.pp5164-5175.
62. von der Linde M, Göcke M, Hirschfeld G, Thielsch MT. Check or reject? Trust and motivation development in app-based warning systems. *Saf Sci.* 2025;185(4):106724. doi:10.1016/j.ssci.2024.106724.
63. AlTuraif RK, AlSanad DS, AlSharifi NF, Almuaili AA. Exploring the catalysts and components of gamification in enterprise: a systematic literature review. *Ing Des Syst D'Inf.* 2023;28(4):975–92. doi:10.18280/isi.280418.
64. Moumouh C, García-Berná JA, Chkouri MY, Fernández-Alemán JL. Serious games to improve privacy and security knowledge for professionals: a systematic literature review. *Int J Serious Games.* 2025;12(1):3–24. doi:10.17083/ijsg.v12i1.825.
65. Yar MA, Goh HG, Adnan K, Gan ML, Ponnusamy V. Towards a tailored cybersecurity education framework for Malaysia: a systematic literature review. *Int J Adv Comput Sci Appl.* 2025;16(11):945. doi:10.14569/ijacsa.2025.0161191.
66. Torgersen LNS, Noble ER, Ask TF, Knox BJ. Strengths and knowledge gaps identified from cybersecurity education and training programs, and the implications for operational technology personnel in critical infrastructures: a scoping review. *IEEE Access.* 2025;13(4):138265–312. doi:10.1109/access.2025.3594045.
67. Parti K, Abdelhamid S, Ladancsik T. Designing for life: a socioeconomic view of digital learning preferences in cybersecurity, with emphasis on older adults. *Societies.* 2025;15(12):342. doi:10.3390/soc15120342.
68. Silko O, Kozubtsova L, Kozubtsov I, Beskrovnyi O. Professional training of lecturers of higher educational institutions based on the cyberontological approach and gamification. In: *Advances in artificial systems for logistics engineering III*. Cham, Switzerland: Springer Nature; 2023. p. 1068–79. doi:10.1007/978-3-031-36115-9_95.
69. Weijssenfeld FGJ, Sarmah DK. Gamifying cybersecurity: a narrative-driven approach to teaching steganography. *Comput Educ Open.* 2025;9(2):100288. doi:10.1016/j.caeo.2025.100288.
70. Andria A, Laksono RD, Sussolaikah K, Mat Din MB, Mansor S, Dawam SRM. Assessment of cyber security awareness using developed game from H5P on users aged at elementary and first secondary school in Madiun city. *J Appl Eng Technol Sci (JAETS).* 2025;7(1):539–49. doi:10.37385/jaets.v7i1.6705.
71. Al-Shammari ET. Integrating protection motivation theory with cultural context: a framework for cybersecurity education. *J Cases Inf Technol.* 2025;27(1):1–27. doi:10.4018/jcit.368146.
72. Schafeitel-Tähtinen T, Lazarov W. Teaching and learning cybersecurity using capture the flag: effectiveness comparison between university students in Finland and Czechia. *Comp Applic Eng.* 2025;33(5):e70082. doi:10.1002/cae.70082.
73. Arduin PE, Costé B. Learning to hack, playing to learn: gamification in cybersecurity courses. *J Cybersecur Priv.* 2026;6(1):16. doi:10.3390/jcp6010016.
74. Grech B. Creating a persistent competition to prepare undergraduate cybersecurity students for national cyber league competitions. *J Inf Syst Educ.* 2026;37(1):98–132. doi:10.62273/gkdz1277.
75. Criollo-C S, Guerrero-Arias A, Buenaño-Fernández D, Luján-Mora S. Usability and workload evaluation of a cybersecurity educational game application: a case study. *IEEE Access.* 2024;12:12771–84. doi:10.1109/access.2024.3352589.
76. Hsu WS. Analyzing student engagement and learning outcomes in a gamified blended cybersecurity course using LMS-based behavioral data. *Int J Eng Ped.* 2025;15(6):111–22. doi:10.3991/ijep.v15i6.57015.
77. Lugnet J, Ericson Å. Scenarios as a tool for professional training in information security dialogues. *Int J Technol Knowl Soc.* 2022;18(2):65–77. doi:10.18848/1832-3669/cgp/v18i02/65-77.

78. Balon T, Baggili I. Cybercompetitions: a survey of competitions, tools, and systems to support cybersecurity education. *Educ Inf Technol.* 2023;28(9):11759–91. doi:10.1007/s10639-022-11451-4.
79. Luh R, Eresheim S, Tavalato P, Petelin T, Gmeiner S, Holzinger A, et al. Gamifying information security: adversarial risk exploration for IT/OT infrastructures. *Comput Secur.* 2025;151(1):104287. doi:10.1016/j.cose.2024.104287.
80. Jawad HM, Tout S. Gamifying computer science education for Z generation. *Information.* 2021;12(11):453. doi:10.3390/info12110453.
81. Parvez MT, Alsuhibani AM, Alamri AH. Educational and cybersecurity applications of an Arabic CAPTCHA gamification system. *Ing Des Syst D'Inf.* 2023;28(5):1275–85. doi:10.18280/isi.280516.
82. Nurwardani S, Handayani PW. Health workers' perspectives on mobile health care learning stickiness: mixed methods study. *JMIR Med Educ.* 2025;11(2):e63827. doi:10.2196/63827.
83. Weichelt B, VanWormer J, Xu Y, Kadolph C, Lin S. Lessons learned from development of a mobile app for cardiovascular health awareness. *Sustainability.* 2021;13(11):5985. doi:10.3390/su13115985.
84. Salahdine F, Kaabouch N. Social engineering attacks: a survey. *Future Internet.* 2019;11(4):89. doi:10.3390/fi11040089.
85. Del-Valle-Soto C, Briseño RA, Valdivia LJ, Nolasco-Flores JA. Unveiling wearables: exploring the global landscape of biometric applications and vital signs and behavioral impact. *BioData Min.* 2024;17(1):15. doi:10.1186/s13040-024-00368-y.
86. Magano J, Quintela JA, Banerjee N. Driving consumer engagement through AI chatbot experience: the mediating role of satisfaction across generational cohorts and gender in travel tourism. *Sustainability.* 2025;17(17):7673. doi:10.3390/su17177673.
87. Giacalone M, Marciano C, Pipino C, Piscopo G, Marra S. Technological innovation and the role of smart surveys in the industrial context. *Appl Sci.* 2025;15(16):8832. doi:10.3390/app15168832.
88. Chu KF, Yuan H, Yuan J, Guo W, Balta-Ozkan N, Li S. A survey of artificial intelligence-related cybersecurity risks and countermeasures in mobility-as-a-service. *IEEE Intell Transport Syst Mag.* 2024;16(6):37–55. doi:10.1109/mits.2024.3427655.
89. Suhail S, Iqbal M, Hussain R, Jurdak R. ENIGMA: an explainable digital twin security solution for cyber-physical systems. *Comput Ind.* 2023;151(3):103961. doi:10.1016/j.compind.2023.103961.
90. Casey E, Jocz J, Peterson KA, Pfeif D, Soden C. Motivating youth to learn STEM through a gender inclusive digital forensic science program. *Smart Learn Environ.* 2023;10(1):2. doi:10.1186/s40561-022-00213-x.
91. Hendrix M, Al-Sherbaz A, Bloom V. Game based cyber security training: are serious games suitable for cyber security training? *Int J Serious Games.* 2016;3(1):53–61. doi:10.17083/ijsg.v3i1.107.
92. Scholefield S, Shepherd LA. Gamification techniques for raising cyber security awareness. *arXiv:1903.08454.* 2019. doi:10.48550/arXiv.1903.08454.
93. Hodhod R, Hardage H, Abbas S, Aldakheel EA. CyberHero: an adaptive serious game to promote cybersecurity awareness. *Electronics.* 2023;12(17):3544. doi:10.3390/electronics12173544.
94. Krath J, Schürmann L, von Korfflesch HFO. Revealing the theoretical basis of gamification: a systematic review and analysis of theory in research on gamification, serious games and game-based learning. *Comput Hum Behav.* 2021;125(21):106963. doi:10.1016/j.chb.2021.106963.
95. Boopathi K, Sreejith S, Bithin A. Learning cyber security through gamification. *Indian J Sci Technol.* 2015;8(7):642. doi:10.17485/ijst/2015/v8i7/67760.
96. Jin G, Tu M, Kim TH, Heffron J, White J. Game based cybersecurity training for high school students. In: *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*; 2018 Feb 21–24; Baltimore, MD, USA. p. 68–73. doi:10.1145/3159450.3159591.
97. Korkiakoski M, Antila A, Annamaa J, Sheikhi S, Alavesa P, Kostakos P. Hack the room: exploring the potential of an augmented reality game for teaching cyber security. In: *Proceedings of the Augmented Humans International Conference 2023*; 2023 Mar 12–14; Glasgow, UK. p. 349–53. doi:10.1145/3582700.3583955.
98. Yasin A, Lin L, Tong L, Fatima R, Wang J. Improving software security awareness using a serious game. *IET Softw.* 2019;13(2):159–69. doi:10.1049/iet-sen.2018.5095.

99. Yasin A, Liu L, Li T, Wang J, Zowghi D. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Inf Softw Technol.* 2018;95(5):179–200. doi:10.1016/j.infsof.2017.12.002.
100. Hart S, Margheri A, Paci F, Sassone V. Riskio: a serious game for cyber security awareness and education. *Comput Secur.* 2020;95(2):101827. doi:10.1016/j.cose.2020.101827.
101. Luh R, Temper M, Tjoa S, Schrittwieser S, Janicke H. PenQuest: a gamified attacker/defender meta model for cyber security assessment and education. *J Comput Virol Hacking Tech.* 2020;16(1):19–61. doi:10.1007/s11416-019-00342-x.
102. Löffler E, Schneider B, Zanwar T, Asprien PM. CySecEscape 2.0—a virtual escape room to raise cybersecurity awareness. *Int J Serious Games.* 2021;8(1):59–70. doi:10.17083/ijsg.v8i1.413.
103. Qusa H, Tarazi J. Cyber-hero: a gamification framework for cyber security awareness for high schools students. In: *Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*; 2021 Jan 27–30; Las Vegas, NV, USA. p. 677–82. doi:10.1109/ccwc51732.2021.9375847.
104. Abu-Amara F, Almansoori R, Alharbi S, Alharbi M, Alshehhi A. A novel SETA-based gamification framework to raise cybersecurity awareness. *Int J Inf Technol.* 2021;13(6):2371–80. doi:10.1007/s41870-021-00760-5.
105. Jaffray A, Finn C, Nurse JRC. SherLOCKED: a detective-themed serious game for cyber security education. *arXiv:2107.04506.* 2021. doi:10.48550/arXiv.2107.04506.