Journal of Information Technology Education: Research

An Official Publication of the Informing Science Institute
InformingScience.org

JITEResearch.org

Volume 24, 2025

# GAMIFIED CYBERSECURITY INITIATIVES: THE TREND, LIMITS, AND LESSONS

| | | |
|---|---|---|
| Anderson Kevin Gwenhure | Sirindhorn International Institute of Technology, Thammasat University, Pathum Thani, Thailand | d6722300115@g.siit.tu.ac.th |
| SangGyu Nam* | Sirindhorn International Institute of Technology, Thammasat University, Pathum Thani, Thailand | sanggyu@siit.tu.ac.th |

* Corresponding author

## ABSTRACT

| | |
|---|---|
| Aim/Purpose | To evaluate the sustainability of gamified cybersecurity education, training, and awareness (ETA) initiatives by addressing recurring limitations, conceptual misclassifications, and the overlooked influence of novelty and duration. |
| Background | Gamification has seen widespread application in cybersecurity ETA initiatives and is frequently credited with improving engagement, motivation, and learning outcomes. However, its true effectiveness remains uncertain. |
| Methodology | A systematic literature review (SLR) following the PRISMA framework was conducted, analyzing 12 peer-reviewed empirical studies focused on gamified cybersecurity ETA interventions. |
| Key Findings & Contribution | The review reveals that most gamified initiatives are short-term and assessed within the novelty effect window, which may inflate their perceived effectiveness. Only two studies applied established gamification frameworks, highlighting a widespread reliance on improvised designs. Common elements like leaderboards and time pressure often cause unintended negative effects, such as anxiety and disengagement. Additionally, poor reporting on intervention duration and negative outcomes hinders reproducibility. Long-term behavior change remains largely unexamined. By synthesizing these findings, this study offers design guidance and calls for more structured, evidence-based approaches to gamification in cybersecurity. |
| Recommendations for Practitioners | Design for long-term impact, not short-term stimulation. Align game elements with user motivations and context. Use theory-based frameworks to document |

Accepting Editor Kay Fielden | Received: April 19, 2025 | Revised: June 11, June 18, June 21, June 26, July 10, 2025 | Accepted: July 18, 2025.
Cite as: Gwenhure, A., K., & Nam, S. (2025). Gamified cybersecurity initiatives: The trend, limits and lessons. *Journal of Information Technology Education: Research, 24,* Article 24. https://doi.org/10.28945/5601

| | |
|---|---|
| | positive and negative outcomes to support continuous improvement and behaviour change. |
| Recommendations for Researchers | Researchers should adopt longitudinal study designs to assess the sustainability of gamified interventions beyond the novelty phase, focusing on behavioural change rather than short-term engagement. Future studies must explore optimal durations for meaningful outcomes and examine how game elements affect diverse user groups and contexts. Clarifying distinctions between gamification, serious games, and simulations is essential to reduce conceptual ambiguity. Developing context-sensitive frameworks that incorporate motivational and environmental factors is also critical. Finally, standardizing reporting on duration, design models, and both positive and negative outcomes will improve comparability and advance research in this field. |
| Impact on Society & Future Research | This research advances the design of evidence-based gamified interventions to help close the cybersecurity skills gap and promote a more security-conscious digital culture. Organizational adoption can enhance user awareness and reduce human-related risks. Future research should distinguish gamification from related methods like serious games and simulations, and shift focus from short-term engagement to long-term outcomes such as secure behavior and compliance. Studies must report both positive and negative effects, considering demographic and contextual factors. Developing integrated, context-aware frameworks and conducting longitudinal studies to determine optimal intervention durations are essential. Standardized reporting and exploration of gamified internal policies will further support effective and sustainable cybersecurity awareness. |
| Keywords | gamification, cybersecurity, education, training, awareness |


## INTRODUCTION

> "There should be no element of slavery in learning. Enforced exercise does no harm to the body, but enforced learning will not stay in the mind. So, avoid compulsion, and let lessons take the form of a play." - Aristocles (Plato).

This timeless insight captures the essence of gamification, a concept first introduced by Nick Pelling in 2002 to describe the use of game-inspired design elements in digital experiences to enhance enjoyment and effectiveness (Christians, 2018). Since its inception, gamification has gained wide popularity across multiple sectors, particularly appealing to younger generations through its playful, competitive, and goal-oriented characteristics (Grobbelaar & Alsemgeest, 2024). Despite this popularity, gamification lacks a single universally accepted definition (Meng et al., 2024). Interpretations range from motivational systems (Zichermann & Cunningham, 2011) to behavioral design frameworks (Tsou & Putra, 2023; Werbach & Hunter, 2020). However, there is a broad consensus that gamification refers to the application of game design elements in non-game contexts to increase motivation, engagement, and meaningful outcomes (Brehmer & Reinelt, 2023; Christensen et al., 2023; Deterding et al., 2011; Tran et al., 2023).

The core components of gamification are game elements and the non-gaming context (Muangsrinoon & Boonbrahm, 2019). Game elements such as points, badges, or leaderboards are structural components designed to evoke emotions, offer feedback, and maintain user interest (Valencia et al., 2019; Werbach & Hunter, 2020). Non-gaming contexts are environments where traditional game structures are absent (Fischer & Barabasch, 2020). With its application particularly prominent across initiatives aimed at education, training, and awareness (ETA), which although often used interchangeably, differ in objectives. Education focuses on the acquisition of broad knowledge and

critical thinking skills (Schmidt & Nøhr, 2023), training develops specific skills for practical tasks (Schmidt & Nøhr, 2023), and awareness fosters behavioral change and enhances risk perception (Benito et al., 2025). By fostering a playful or gameful attitude, gamification can enhance learning and engagement. However, it is crucial to distinguish it from play itself, as gamification aims to achieve specific outcomes rather than simply promote enjoyment (Kamalodeen et al., 2021).

Gamification supports these initiatives by promoting gameful attitudes and increasing user involvement. However, it should not be confused with mere play. Its goal is not entertainment, but rather the intentional use of game mechanics to enable progression, autonomy, and purpose (Werbach & Hunter, 2020) and to achieve specific outcomes rather than simply promote enjoyment (Kamalodeen et al., 2021). These effects are supported by Self-Determination Theory (Ryan & Deci, 2000), which emphasizes autonomy, competence, and social connection, and Flow Theory (Csikszentmihalyi, 1990), which highlights optimal engagement when challenges match individual skill levels. When these principles are integrated effectively, gamification can nurture both intrinsic and extrinsic motivation, leading to enhanced participation, meaningful behavioral change, and increased user satisfaction (Calles-Esteban et al., 2024; Chang et al., 2024; Mallick & Waheed, 2024). These potential benefits have led to the integration of gamification across sectors, not limited to education, healthcare, marketing, and finance, with promising results in motivation, satisfaction, performance, and behavioral change (Calles-Esteban et al., 2024; Chang et al., 2024; Mallick & Waheed, 2024; Yakubov et al., 2024).

In cybersecurity, gamification is being explored to support ETA efforts, referred to in this paper as gamified cybersecurity initiatives. These efforts arise in response to enduring challenges. Cybersecurity education and training are perceived as too technical, deterring enrollment and resulting in dropout or skill mismatches (M. E. Armstrong et al., 2018; Catota et al., 2019; Triplett, 2023). These systemic flaws have fueled a severe and widening shortage of cybersecurity professionals, as industry demand continues to far outpace the available skilled workforce (Burrell, 2018; Davies et al., 2022; Mogoane & Kabanda, 2019; Xu et al., 2023). Beyond the realms of education and training, individuals, organizations, and governments face an escalating cybersecurity threat landscape, placing data integrity, financial stability, and privacy at serious risk (Dave et al., 2023; Desolda et al., 2022).

Although technical advances such as hardware upgrades and improved security protocols offer some relief (Choi & Rubin, 2023; Zhuo et al., 2023), these measures are not adequate in addressing the rise of human-centric threats. Sophisticated tactics like social engineering and phishing bypass even the most advanced systems by targeting the human element, exploiting cognitive biases, inattentiveness, or lack of awareness (Choi & Rubin, 2023; Steves et al., 2020; Thomopoulos et al., 2024). Cybersecurity as a discipline now recognizes that humans are both its greatest defense and its greatest vulnerability (Petrykina et al., 2021). A growing body of empirical evidence points to human error as the primary cause of breaches, often stemming from users' lack of awareness or habitual risky behaviors (Petrykina et al., 2021; Qusa & Tarazi, 2021; Shah & Agarwal, 2023; Tran et al., 2023). This is evidenced by the ongoing prevalence of incidents linked to human error (Shah & Agarwal, 2023; Sharif & Ameen, 2020). Notably, 95% of cybersecurity breaches in 2024 were attributed to human factors (Coker, 2025; Mastercard Trust Center, n.d.), arising from either malicious insiders or negligent users who unknowingly compromise security (Harding et al., 2022).

To address human vulnerabilities in cybersecurity, organizations have implemented awareness initiatives that typically rely on conventional tools such as static videos, memos, PowerPoint slides, or email campaigns (Alqahtani & Kavakli-Thorne, 2020; Shah & Agarwal, 2023). However, these interventions are largely theoretical and often fail to result in meaningful behavioral change, improved compliance, or enhanced threat recognition (Qusa & Tarazi, 2021). Rather than fostering engagement, they frequently evoke disinterest, fatigue, or even resistance among employees, who may perceive such initiatives as irrelevant to their primary roles or as the sole responsibility of IT personnel

(Decusatis et al., 2022; Scherb et al., 2023). This disengagement is further compounded by the technical complexity and jargon often associated with cybersecurity, which can alienate non-technical users (Arora, 2019; Balakrishna & Charlton, 2022).

Yet newer generations, such as Millennials, Generation Z, and Generation Alpha, seek flexible, interactive, and meaningful learning experiences supporting personal fulfillment and professional development (Ribeiro e Silva & Carneiro, 2025). Although gamification has emerged as a strategic response, empirical evidence reveals a more nuanced and sometimes inconclusive picture of its effectiveness in this context (Dah et al., 2024). This underscores the need for a systematic literature review (SLR) to consolidate and evaluate the existing empirical research on gamified approaches within cybersecurity initiatives.

An SLR, also referred to as a systematic review (SR), is a structured method for identifying and synthesizing relevant literature to address a specific research question (Higgins et al., 2011; Lamé, 2019; Piper, 2013). The primary objective of an SLR is to reduce bias and enhance transparency through explicit, systematic procedures that govern study selection, quality assessment, and the objective synthesis of findings (Higgins et al., 2011; Liberati et al., 2009; Moher et al., 2009). The process involves defining research questions, searching for relevant literature, assessing the quality of included studies, and synthesizing the findings either qualitatively or quantitatively (R. Armstrong et al., 2011). When results are combined quantitatively, the process is referred to as meta-analysis (Egger et al., 2006; Lamé, 2019).

Notably, an SLR does not offer definitive answers but rather seeks to present, as accurately as possible, what is currently known and unknown about the research questions under investigation (Briner & Denyer, 2012). To ensure credible conclusions, an SLR must adhere to rigorous standards when assessing the quality of included studies (Higgins et al., 2011). Although the notion of quality can be complex, it generally refers to how well a study has been designed, conducted, analyzed, and reported in relation to its stated research aims (Higgins et al., 2011). High-quality studies are more likely to produce reliable findings, making their inclusion critical for drawing valid conclusions (Higgins et al., 2011).

# LITERATURE REVIEW

## *GAMIFICATION EFFECTIVENESS ACROSS LEARNING CONTEXTS*

Regarding ETA initiatives, gamification has demonstrated measurable effectiveness across a variety of digital learning environments, including Massive Open Online Courses (MOOCs), workplace and vocational training, healthcare education, university-level online courses, and global social learning platforms. In a MOOC on Lean Startup, the use of points, badges, and leaderboards significantly increased engagement, assignment submissions, and course completion and retention rates compared to a non-gamified version (M. R. Rodrigues & Mira da Silva, 2025). Employees exposed to low-intensity gamification in virtual workplace training achieved better retention test scores. They made fewer errors than those in high-intensity conditions, indicating that intense gamification does not always equate to better outcomes (Eger et al., 2024). Vocational college students engaged in gamified intercultural English learning showed marked improvements in intrinsic motivation and intercultural competence (Min et al., 2025). A gamified mobile app for teaching Operating Systems led to significantly higher post-test scores, particularly among visual learners, underscoring the importance of aligning game elements with learning preferences (Rey & Defensor, 2024).

In a professional healthcare context, ICU nurses trained through gamified clinical scenarios outperformed those in e-learning and control groups in knowledge acquisition and attitudinal change (Hossein et al., 2025). For adult learners in a national financial education program, gamification increased question response rates and overall completion, though its effectiveness declined in more complex decision-making tasks (Pitthan & De Witte, 2025). In a university-level computer programming

course, students using a gamified, socially interactive platform achieved the highest test scores and reported the greatest satisfaction (Gharbaoui et al., 2025). Lastly, university students using a gamified quiz app engaged more consistently when generic feedback and session pacing were applied, although tasks that were perceived as too easy discouraged continued participation (Welbers et al., 2019).

## *Psychological Dynamics in Gamified Learning*

While gamification is acknowledged for its ability to boost engagement, motivation, and behavior change, these outcomes are not guaranteed and may be influenced by overlooked psychological phenomena, most notably novelty (Hamari et al., 2014; L. Rodrigues et al., 2022) and habituation (Barrile et al., 1999; Gwenhure & Rahayu, 2024). The novelty effect refers to a temporary boost in interest and performance resulting from exposure to new or unfamiliar stimuli, such as game elements in a learning environment (Barrile et al., 1999). This effect has been well-documented in instructional design, where innovative teaching methods initially enhance learner engagement (Sweller et al., 2011). Conversely, the habituation effect describes a decline in responsiveness as individuals grow accustomed to a stimulus, leading to diminishing motivational returns over time (McSweeney & Murphy, 2009). Hamari et al. (2014) argued that engagement with gamified systems often decreases over time. This suggests that early positive effects may be linked to the initial novelty rather than sustained design impact and may fade as they become familiar with the gamified environment. Similarly, Meng et al. (2024) reported that while points and badges enhanced engagement in online learning, mandatory gamified tasks undermined users' autonomy, suggesting that while novelty may drive early engagement, its long-term effectiveness relies on sustained intrinsic motivation. In the context of gamification in cybersecurity, this typically manifests after approximately four weeks, when the initial excitement wanes and engagement levels begin to drop (L. Rodrigues et al., 2022).

## *Design Pitfalls and Contextual Limitations in Gamified Initiatives*

Effective gamification in non-game contexts requires deliberate design aligned with user psychology, learning goals, and contexts (Feng et al., 2023). Oversimplified or poorly contextualized gamification strategies risk undermining the very outcomes they aim to achieve. For instance, Eger et al. (2024) found that excessive or high-intensity gamification can have a negative effect on perceived autonomy and hinder training outcomes. Participants reported feeling overwhelmed or constrained by overly gamified content, indicating that too many game mechanics may reduce engagement rather than enhance it. Similarly, Bardach and Murayama (2025) argue that while extrinsic rewards such as points and badges can serve as effective entry points to spark initial engagement, their continued or overly salient use may disrupt the internal feedback loop of learning and undermine intrinsic motivation through the overjustification effect. Meng et al. (2024) also reported that while points enhanced multiple engagement dimensions, badges were effective only for participation, and both elements could undermine autonomy when used without thoughtful integration. Welbers et al. (2019) showed that high-performing students were less likely to continue using a gamified quiz app, possibly because overly easy tasks failed to challenge them, leading to disengagement. Similarly, gamification was found to enhance completion rates for simpler tasks but had no positive effect and sometimes a negative one for complex decision-making questions (Pitthan & De Witte, 2025), highlighting that gamification must be matched to task complexity and user needs. These examples illustrate the complexity of gamified design and reveal recurring challenges related to its effectiveness and contextual fit.

## *Research Motivation*

The preceding literature review highlights the complexity of designing effective gamified interventions in cybersecurity ETA initiatives. Across diverse studies, gamification has demonstrated both potential and limitations, with outcomes varying depending on psychological dynamics, task complexity, implementation intensity, and alignment with user needs. These inconsistencies raise important methodological and practical questions that remain unconsolidated across the field.

One pressing concern relates to how effectiveness is measured, particularly whether studies account for time-dependent effects such as the novelty effect. This psychological dynamic raises a critical question about the sustainability of gamification over time. Are the reported outcomes in gamified cybersecurity ETA initiatives measured after accounting for novelty, or do they capture data only within their limited timeframe? If the latter is true, there is a risk that the reported benefits overstate gamification's actual sustained impact. Such limitations are critical in cybersecurity awareness initiatives, where long-term engagement is essential, not just short-term participation. Without addressing these temporal dynamics, gamified solutions may fail to deliver lasting engagement and motivation, thereby undermining the primary objective of initiatives such as long-term awareness.

Beyond the novelty effect, the literature highlights recurring challenges stemming from mismatches between gamification design, user characteristics, and the contextual demands of the learning environment. While some game elements have demonstrated measurable benefits, others have produced mixed or even adverse outcomes depending on the context in which they were implemented. This variability highlights the need to examine gamification design choices. Accordingly, several key questions must be addressed. Key questions include: Which frameworks guide implementation? Which elements drive positive outcomes, and which pose challenges in specific contexts? Additionally, what negative emotional, cognitive, or behavioral consequences have been reported in past implementations? Given that gamification effectiveness depends heavily on thoughtful, user-centered design (Valencia et al., 2019), answering these questions is crucial for developing more effective and sustainable practices. Furthermore, identifying which cybersecurity domains have benefited from gamified approaches can help uncover under-explored areas and guide future efforts in deploying gamification more strategically.

To address these questions, it is essential to examine the current state of empirical research. This involves identifying recurring patterns, strengths, and limitations across existing implementations. Such an examination can provide valuable, evidence-informed guidance for both researchers and practitioners aiming to enhance the quality and long-term impact of gamified cybersecurity initiatives.

As a response to this need, the present study conducts a Systematic Literature Review (SLR) in accordance with Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. While meta-analysis is one approach to synthesis within SLRs, this review adopts a qualitative thematic synthesis approach. As noted by Higgins et al. (2011) and R. Armstrong et al. (2011), SLRs may synthesize findings either qualitatively or quantitatively depending on the nature and purpose of the research. In this case, the objective is to identify and organize conceptual patterns in how gamification is implemented within cybersecurity initiatives, rather than to perform statistical aggregation. Accordingly, quality assessment, transparent study selection, and structured thematic synthesis are prioritized over detailed study-level metadata extraction. The review is guided by the following overarching research question: What do existing implementations of gamified approaches in cybersecurity education, training, and awareness reveal? This main question is explored through the following sub-questions:

1. What primary categorizations among education, training, or awareness do gamified cybersecurity initiatives align with, and how are these emphases reflected across different implementations?
2. What are the target outcomes across reviewed gamified cybersecurity initiatives?
3. How effective are gamified cybersecurity initiatives compared to non-gamified approaches or pre-gamified initiatives?
4. How does the duration of gamified cybersecurity initiatives vary?
5. What specific gamification elements have been identified as potentially effective for maintaining user motivation and engagement in cybersecurity initiatives?
6. Which specific game elements have a negative/unwanted impact, and what are their effects?
7. What gamification-based frameworks have been used to guide the design of gamified cybersecurity initiatives?
8. Which topics within cybersecurity have been explored through gamification?

The structure of this paper continues with a detailed explanation of the methodology, including the review planning process, selection criteria, and data extraction approach. This is followed by a presentation of the results based on a qualitative synthesis of relevant studies. The discussion then interprets the key findings and examines their implications within the context of gamified cybersecurity education, training, and awareness. The paper concludes with a summary of core insights, consideration of the review limitations, and recommendations for future research aimed at advancing the design and effectiveness of gamified cybersecurity initiatives.

# METHODOLOGY

The review protocol in this study follows the guidelines proposed in earlier work (Kitchenham, 2004, 2007) and further developed in subsequent literature (Kitchenham et al., 2015), encompassing the planning, execution, and documentation stages. These stages align with the systematic review steps described in earlier literature (Egger et al., 2006).

## *PLANNING THE REVIEW*

Planning involves two major steps: Step 1, justifying the need for a systematic review, and Step 2, formulating the review questions. Step 1 entails defining why the review is necessary (Egger et al., 2006), while Step 2 involves identifying the specific questions the review seeks to answer (Egger et al., 2006). These questions must be formulated to be specific, focused, and valid, as they guide the entire review process, including the selection of primary studies, data extraction, and synthesis (Rahayu et al., 2020). As outlined in the introduction, the justification and research questions guiding this review were developed based on identified gaps in the literature. These questions form the framework for the subsequent systematic literature review process.

## *CONDUCTING THE REVIEW*

Guideline 2, conducting the review, consists of five steps: locating relevant studies, selecting studies, assessing quality, and extracting data, which align with the PRISMA guidelines (Moher et al., 2009). Locating studies involves developing a search strategy to identify relevant literature (Egger et al., 2006; Rahayu et al., 2020). In this study, an automated search strategy was designed by first identifying key terms related to the research focus, including cybersecurity, gamification, education, training, and awareness. Alternative terms were also incorporated to capture conceptual variations. The search covered literature published from 2017 to 2024 and was conducted using the Scopus database. Search strings were applied to article titles, abstracts, and keywords. Following recommendations for clarity and rigor, it is advised to use a few comprehensive databases rather than multiple sources (Paré et al., 2015). Scopus was selected as the sole database due to its global coverage and broad disciplinary scope, indexing over 43,465 academic journals, including 9,270 rated as Quartile 1 and 3,978 ranked among the top 10% of the most influential journals worldwide, while ensuring that all indexed articles undergo rigorous peer review and meet high research quality standards (Azman et al., 2024). As a result, it is widely recognized for its breadth, relevance, accessibility, and up-to-date content (Pranckutė, 2021), making it a comprehensive and reliable source of peer-reviewed literature across a wide range of research domains (Azman et al., 2024; Mercuri et al., 2016). The Scopus search identified 114 relevant publications. The search string used is as follows:

> ( TITLE-ABS-KEY ( “gamification” OR “gamify” OR “gamified” OR “game dynamics” OR “game mechanics” OR “game elements” OR “game design elements” OR “game components” OR “game aesthetics” ) ) AND ( TITLE-ABS-KEY ( “cybersecurity education” OR “cybersecurity training” OR “cybersecurity awareness” OR “information security education” OR “information security training” OR “information security awareness” OR “IT security education” OR “IT security training” OR “IT security awareness” OR “cyber threat education” OR “cyber threat training” OR “cyber threat awareness” OR “phishing education” OR “phishing training” OR “phishing awareness” OR “data privacy education” OR “data privacy training” OR “data privacy awareness” ) ) AND ( PUBYEAR > 2017 AND PUBYEAR < 2024 ) AND ( LIMIT-TO ( LANGUAGE , “English” ) )

The next step, selecting studies, involves identifying primary studies based on the inclusion and exclusion criteria (Egger et al., 2006), which should be defined in alignment with the research questions and applied consistently (Siddaway et al., 2019). In this study, papers were included or excluded based on their relevance to addressing the research objectives, thus answering the research questions. In line with best practices recommended by Moher et al. (2009), Page et al. (2021), and Siddaway et al. (2019), independent and duplicate screening and data extraction were conducted to ensure consistency and reliability. After the initial database search, two reviewers independently screened titles and abstracts. Although the resulting sets of included papers differed slightly in number, the results remained within the same range. Discrepancies arose primarily from differing interpretations of the term gamification, particularly for studies that fell within the boundaries of game-based learning or serious games. To resolve these differences, the reviewers engaged in discussion and reached consensus on the definitional boundaries between gamification, game-based learning, and serious games. Based on this shared understanding, dichotomous classification was adopted to determine whether each paper aligned with the review's scope. As illustrated in Figure 1, the final inclusion and exclusion process proceeded as follows:

- Exc1: Excluded studies unrelated to gamification in cybersecurity initiatives based on keyword screening and abstract review, reducing the initial pool to 99 papers.
- Exc2: Removed studies focused on serious games, game-based learning, or simulations, resulting in 68 papers.
- Exc3: Excluded conceptual, theoretical, and review papers, leaving 54 empirical studies.
- Exc4: Removed studies that did not explicitly address cybersecurity contexts, reducing the total to 50.

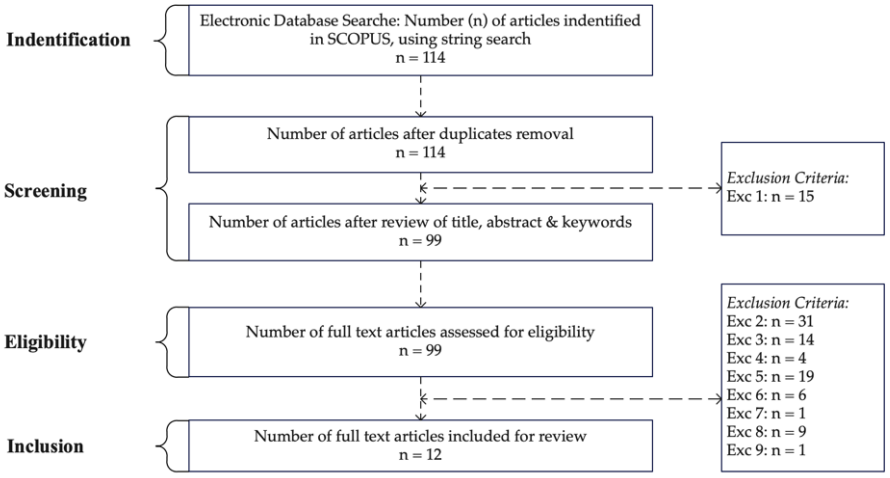


**Figure 1. Article selection and screening process based on PRISMA**

Studies that had cybersecurity ETA initiatives as their central focus were included, while those that only mentioned cybersecurity incidentally or had unrelated learning goals were excluded.

- Exc5: Excluded studies where gamification was not the primary focus, leaving 31 papers.
- Exc6: Excluded papers without full-text access.
- Exc7: Removed one non-English language paper, yielding 22 eligible articles.
- Exc8: A peer-review validation was conducted in which the 22 studies were reassessed using the binary criteria proposed by Uzun and Tekinerdogan (2018).

This served as a second, more stringent round of review to ensure agreement on the final pool of relevant studies. This additional phase was necessary to mitigate the effects of cognitive overload, where reviewers overwhelmed by volume may make quicker and less accurate decisions during initial screening, and inattentional blindness, in which relevant weaknesses or misalignments are unintentionally overlooked initially. Re-evaluation under reduced cognitive load allowed for a more deliberate assessment of study relevance to the review's focus. Following this deeper evaluation, nine studies were excluded, leaving 13.

- Exc9: One additional paper was excluded after it was discovered to have been retracted during the preparation of this review.

Ultimately, 12 high-quality empirical studies were retained in this review. This outcome is not unusual since systematic reviews commonly exclude a large portion of initially identified records due to strict methodological screening, especially when empirical rigor and risk of bias assessments are prioritized (Liberati et al., 2009; Page et al., 2021). Thus, systematic reviews with a narrow empirical focus, such as those excluding theoretical or conceptual papers, will yield smaller sets of studies, as inclusion criteria tailored to empirical rigor limit the review's scope (Siddaway et al., 2019). This is due to the fact that inclusion and exclusion criteria must be defined based on the research question and applied consistently (Siddaway et al., 2019). This is true in this case, where papers were excluded due to their relevance to the predefined questions. Such inclusion or exclusion is not only expected but essential for transparency and replicability (Liberati et al., 2009; Page et al., 2021). Besides, the quality of a review lies not in the number of studies included, but in the transparency, theoretical grounding, and methodological coherence of the review process (Boell & Cecez-Kecmanovic, 2015; Moher et al., 2009). As an implication, in a review, the number of studies should not be used as an indicator of quality; rather, the relevance and treatment of selected literature are key (Boell & Cecez-Kecmanovic, 2015).

In line with this reasoning, the limited number of included studies in this review did not hinder its analytical goals. Thematic saturation, defined as the point where no new insights emerge from additional data and is accepted as an indicator of adequacy in qualitative synthesis and evidence reviews (Hennink & Kaiser, 2022), was observed in this research. The 12 studies addressed all predefined research questions, and no new conceptual themes emerged in the final stages of analysis. This was confirmed after the extension of the timeline from the preferred five-year window (2019 to 2024), intended to capture recent trends while ensuring relevance and depth, to seven years (2017 to 2024), which also did not introduce additional themes relevant to the scope of the review as defined by its research questions, nor did it alter the direction of findings, supporting the conclusion that saturation had been reached. Therefore, the final pool of studies, though small, was sufficient to fulfil the objectives of the review. Nonetheless, despite the methodological justifications presented, certain limitations are inherent to the study design and scope. These will be acknowledged and discussed in the conclusion section.

## *Data Extraction*

Once the final studies were identified, data were extracted from each of the 12 papers. A standardized data extraction Excel form was designed to collect information necessary for answering the research questions. This included results on the effectiveness of gamified approaches, such as metrics on user performance, retention rates, and behavior change. Details on the objectives and outcomes targeted by gamification initiatives were recorded, along with descriptions of applied gamification elements and their observed impacts, both positive and negative. Challenges, limitations, and the specific platforms used in implementing gamified initiatives were noted. Lastly, the specific themes of cybersecurity topics addressed in the gamified initiatives were documented. This structured process ensured comprehensive data collection to support thorough analysis and synthesis. Table 1 displays the data summaries from the 12 papers, including the reference, study focus, target participants, platform used, and duration (the length of time the gamified initiative is implemented or the length of time over which its effectiveness is assessed).

**Table 1. Overview of reviewed gamified cybersecurity studies**

| Focus | Participants | Country | Platform | Duration | Reference |
|---|---|---|---|---|---|
| Cybersecurity training | Employees | Norway | Web-based | Five-minute session | (Gjertsen et al., 2017) |
| Cybersecurity foundational concepts | Beginners in cybersecurity | Iran | Web-based | Not mentioned | (Raisi et al., 2021) |
| Evaluating gamification effects on security awareness | Students | Taiwan | Web-based | Four weeks | (Wu et al., 2021) |
| Cybersecurity awareness | Employees | United Arab Emirates | Web-based | One week | (Abu-Amara et al., 2021) |
| Cybersecurity knowledge | Students | United States | Web-based | One class session | (Matovu et al., 2022) |
| Secure coding practices | Students | United Kingdom | Mobile-based | Fifteen minute session | (Berisford et al., 2022) |
| Phishing detection | Employees | United States | Web-based | One month | (Canham et al., 2022) |
| Phishing awareness | Students | Indonesia | Web-based | Not mentioned | (Natalia et al., 2023) |
| Personal data protection | General users | Indonesia | Web-based | Not mentioned | (Rendreana et al., 2023) |
| Information security awareness | General users | China | Mobile-based | Three minute session | (Chen et al., 2023) |
| USB attack prevention | Students | The Nether-lands | Computer-based | Not mentioned | (Rikkers & Sarmah, 2025) |
| Cybersecurity education | Students | Germany | Web-based | Not mentioned | (Brehmer & Reinelt, 2023) |

# QUALITATIVE ANALYSIS AND RESULTS

This section presents a qualitative analysis of the collected data, structured in alignment with the research questions outlined in the methodology section of this paper. The findings are examined to highlight key themes, patterns, and insights that emerged from the review. Each research question is addressed individually, with a detailed discussion of relevant findings derived from the reviewed papers.

## *RQ1. DOMAINS OF APPLICATION*

Gamified cybersecurity programs are designed to support learning and behavioral outcomes in dynamic, interactive ways. However, their alignment within the traditional cybersecurity education, training, and awareness framework varies by context and design. Table 2 provides a classification of selected studies based on their stated or inferred focus, categorizing each initiative according to whether it primarily serves educational, training, or awareness purposes. While awareness emerges as the most frequently addressed objective, especially in areas like phishing recognition and personal data protection, many initiatives incorporate elements of training through scenarios, hands-on challenges, or behavioral tasks. A subset supports education by structuring content through curricula,

theoretical frameworks, or standards-aligned modules. This classification reveals that while some gamified interventions are purpose-built for specific domains, many exhibit hybrid characteristics that blur categorical lines.

**Table 2. Classification of gamified cybersecurity initiatives by domain: education, training, and awareness**

| Reference | Education | Training | Awareness |
|---|---|---|---|
| (Gjertsen et al., 2017) | | ✔Through task-based and role-relevant exercises | ✔Raises attentiveness to security issues |
| (Natalia et al., 2023) | | ✔Students interact with missions, quizzes | ✔Phishing awareness |
| (Rendreana et al., 2023) | | | ✔Data protection threat awareness |
| (Matovu et al., 2022) | | ✔Scenario-based gamified sessions | ✔Social engineering awareness |
| (Berisford et al., 2022) | ✔Teaches secure coding concepts using OWASP Top 10 | ✔In-game code reviews and decision-making | ✔Insecure coding pattern awareness |
| (Raisi et al., 2021) | ✔Structured learning with adaptive content and ISO standards | ✔Hands-on tasks, duels, problem-solving | ✔General cybersecurity awareness |
| (Wu et al., 2021) | | | ✔ISA in password, internet use, info handling |
| (Chen et al., 2023) | | | ✔Users' information security awareness |
| (Canham et al., 2022) | | ✔Real-time phishing reporting exercises, and analysis of phishing cues, aligning with behavioral training. | ✔Phishing awareness |
| (Rikkers & Sarmah, 2025) | | | ✔USB attack awareness |
| (Abu-Amara et al., 2021) | | ✔Interactive decision-making scenarios | ✔Awareness of threats like phishing, misuse |
| (Brehmer & Reinelt, 2023) | | | ✔ISA in password, email, social media, and info handling |

## *RQ2. Core Target Outcomes Across Gamified Interventions*

Across diverse gamified cybersecurity initiatives, objectives are rarely singular; instead, they target multiple overlapping outcomes reflective of the field's multifaceted learning demands. A thematic synthesis of the reviewed literature identifies six recurrent outcomes: engagement, motivation, awareness, behavior change, skill development, and knowledge retention. These were either embedded in design goals or evaluated through post-intervention assessments. Engagement was defined as active, sustained participation, enhanced through narrative, interactivity, and social elements. Motivation encompassed intrinsic drivers (e.g., curiosity, autonomy) and extrinsic reinforcements (e.g., points, re-

wards, competition). Awareness refers to increased understanding of threats like phishing, social engineering, and data breaches. Behavior change was understood as a shift toward more secure digital practices, though often measured via self-reported intent rather than long-term behavioral data. Skill development related to the acquisition of applied competencies, particularly in technical domains such as secure coding or phishing identification. Knowledge retention was measured through learners' ability to recall and apply content over time, assessed via pre-/post-tests or performance indicators. The recurrence of these themes across varied contexts underscores the inherently multidimensional nature of gamified initiatives, where the goal is not merely to inform but to instill enduring behavioral and cognitive change. Table 3 presents a comparative overview of how these six core outcomes were addressed across the reviewed initiatives.

**Table 3. Target outcomes across reviewed gamified cybersecurity initiatives**

| Reference | Engagement | Motivation | Awareness | Behavior change | Skill development | Knowledge retention |
|---|---|---|---|---|---|---|
| (Gjertsen et al., 2017) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| (Natalia et al., 2023) | ✔ | ✔ | ✔ | ✖ | ✖ | ✔ |
| (Rendreana et al., 2023) | ✔ | ✔ | ✔ | ✔ | ✖ | ✔ |
| (Matovu et al., 2022) | ✔ | ✔ | ✔ | ✖ | ✖ | ✔ |
| (Berisford et al., 2022) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| (Raisi et al., 2021) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| (Wu et al., 2021) | ✔ | ✔ | ✔ | ✔ | ✖ | ✔ |
| (Chen et al., 2023) | ✔ | ✔ | ✔ | ✔ | ✖ | ✔ |
| (Canham et al., 2022) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| (Rikkers & Sarmah, 2025) | ✔ | ✔ | ✔ | ✔ | ✖ | ✔ |
| (Abu-Amara et al., 2021) | ✔ | ✔ | ✔ | ✔ | ✖ | ✔ |
| (Brehmer & Reinelt, 2023) | ✔ | ✔ | ✔ | ✔ | ✖ | ✔ |

## *RQ3. Comparative Effectiveness of Gamified vs. Non-Gamified Approaches*

Across the twelve reviewed studies, gamified cybersecurity initiatives outperformed non-gamified or pre-gamified formats in promoting engagement, motivation, awareness, skill acquisition, behavioral adaptation, and knowledge retention. Engagement levels were elevated through the use of immersive narratives, point systems, team-based leaderboards, and personalized challenges. For example, one study reported an 83% user willingness to reuse the system due to its interactive design (Raisi et al., 2021), while another sustained engagement over four weeks (Canham et al., 2022). Similarly, research revealed a strong learner preference for game-like formats compared to conventional delivery methods (Abu-Amara et al., 2021; Brehmer & Reinelt, 2023). Motivation levels increased substantially when game mechanics were tailored to user preferences and contexts. For instance, one study reported an 88.64% motivation score (Rendreana et al., 2023), and another found that 97% of participants felt more motivated in gamified environments (Matovu et al., 2022). Improvements in cybersecurity awareness were universally observed (Brehmer & Reinelt, 2023; Rikkers & Sarmah, 2025; Wu et al., 2021). Skill development was most evident in applied contexts such as secure coding, with effective learning outcomes achieved through targeted gamified coding exercises (Berisford et al.,

2022). While longitudinal behavior change remains challenging to track, preliminary evidence suggests that gamification influenced users' password habits and phishing responses (Abu-Amara et al., 2021; Canham et al., 2022). Moreover, story-driven scenarios enhanced pattern recognition and fostered behavior framing (Rikkers & Sarmah, 2025). Knowledge retention was bolstered through microlearning strategies, narrative repetition, and adaptive reinforcement, with post-intervention improvements recorded in several studies (Brehmer & Reinelt, 2023; Raisi et al., 2021; Rendreana et al., 2023). Collectively, these findings underscore the superiority of gamified initiatives in fostering sustained engagement, effective learning, and proactive security behavior, outcomes that traditional approaches consistently struggle to achieve. Table 4 summarizes the outcomes of gamified cybersecurity initiatives, showing positive effects on engagement, motivation, awareness, retention, and skills, but also highlighting inconsistent use of pre-tests, post-tests, and control groups.

**Table 4. Summary of gamification outcomes in cybersecurity ETA initiatives**

| Study | Gamification results | Comparison methods | | |
|---|---|---|---|---|
| | | Pre-test | Post test | Control group |
| (Gjertsen et al., 2017) | Enhanced participant engagement and retention. | ✗ | ✗ | ✗ |
| (Natalia et al., 2023) | +1.74 score increase in phishing awareness. | ✓ | ✓ | ✓ |
| (Rendreana et al., 2023) | +36.4 points improvement in understanding and retention. | ✓ | ✓ | ✓ |
| (Matovu et al., 2022) | 94% participant preference for gamified method and better post-session retention. | ✓ | ✓ | ✗ |
| (Berisford et al., 2022) | Increased motivation and performance in secure coding tasks. | ✓ | ✓ | ✗ |
| (Raisi et al., 2021) | 83% showed measurable skill improvement. | ✓ | ✓ | ✗ |
| (Wu et al., 2021) | Cybersecurity knowledge improvement. | ✓ | ✓ | ✓ |
| (Chen et al., 2023) | Improved retention and cybersecurity awareness. | ✗ | ✓ | ✗ |
| (Canham et al., 2022) | Increased phishing attack reporting. | ✗ | ✗ | ✗ |
| (Rikkers & Sarmah, 2025) | Higher post-training understanding of USB attack risks. | ✓ | ✓ | ✗ |
| (Abu-Amara et al., 2021) | 51.4% increase in awareness after gamified training. | ✓ | ✓ | ✗ |
| (Brehmer & Reinelt, 2023) | Improved awareness. | ✗ | ✓ | ✗ |

## *RQ4. Duration of Interventions*

To address Research Question 4, the reviewed studies were examined based on the duration of their gamified cybersecurity initiatives, categorized into short-term, extended, and unspecified timeframes.

### Short-term initiatives

Most gamified cybersecurity initiatives are designed for short durations, ranging from a single session to engagements spanning a few days or weeks. For instance, gamified tasks were implemented in sessions lasting only fifteen minutes per participant, emphasizing immediate interaction (Berisford et al., 2022). Similarly, other initiatives were short, one-time efforts, consisting of a 5-minute session, a single class session, and a 3-minute session, respectively, focusing on delivering quick, targeted training (Chen et al., 2023; Gjertsen et al., 2017; Matovu et al., 2022). Other initiatives, while still considered

short-term, extended engagement over multiple sessions within limited timeframes. One such initiative included a pre-game survey conducted one day prior and a post-game survey a week later, spanning a total of seven days (Abu-Amara et al., 2021). These models maintain a short duration but aim to enhance learning by distributing sessions over a slightly extended period.

### Extended initiatives

Some studies employed longer durations to allow for deeper engagement and sustained learning. For example, one study implemented a month-long gamified initiative, enabling participants to interact repeatedly with the content over an extended period (Canham et al., 2022). Another required participant to engage with a gamified platform for four weeks, three times a week, in fifty-minute sessions (Wu et al., 2021). While less common, such initiatives demonstrate the potential for more substantial impacts on participant behavior and retention.

### Unspecified durations

Several studies did not specify the duration of their gamified initiatives, reflecting a reporting gap in the field. Some described gamification methods but provided no clear indication of the timeframes involved (Natalia et al., 2023; Rendreana et al., 2023; Rikkers & Sarmah, 2025). Another study discussed iterative gamification cycles, suggesting an extended timeline, but omitted exact details (Brehmer & Reinelt, 2023).

Figure 2 illustrates the distribution of gamified cybersecurity initiatives based on duration, showing that most studies focus on short-term interventions, particularly within the 0–15-minute range, with some extending to 60 minutes (one class session) and others up to 7 days. Some initiatives extend up to 30 days, but they are significantly fewer, indicating that long-term gamified approaches remain underexplored. Additionally, a notable number of studies do not specify their duration, making it difficult to assess the sustainability and long-term impact of gamification in cybersecurity initiatives, especially awareness initiatives.

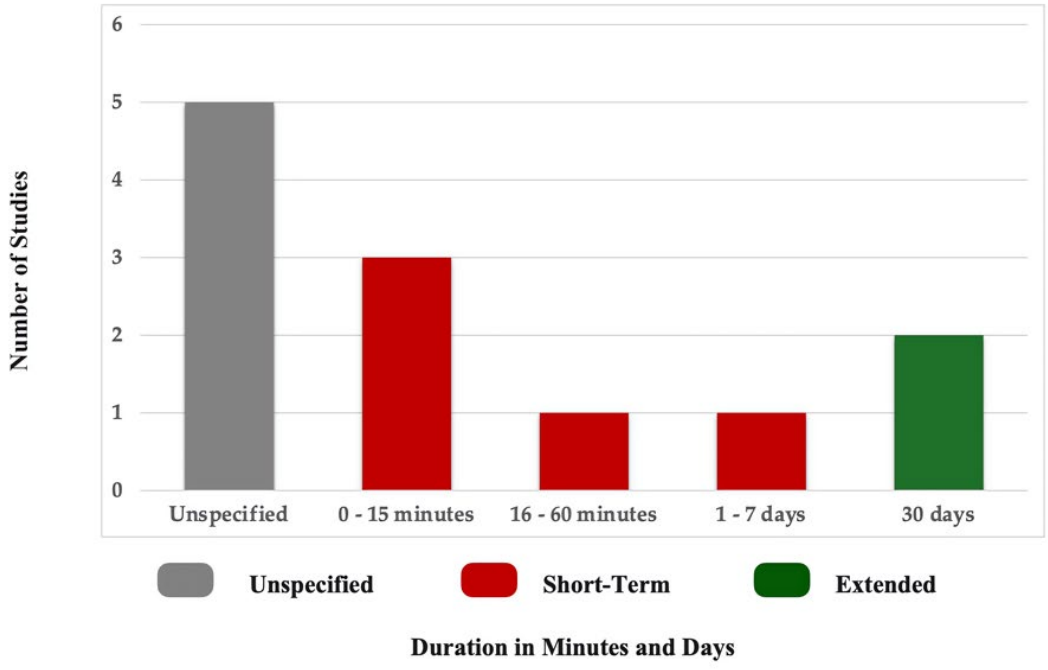


**Figure 2. Reported durations of gamified cybersecurity initiatives**

## *RQ5. Positive Impact Of Game Elements*

As illustrated in Figure 3, a broad range of game elements has been employed in gamified cybersecurity initiatives across the reviewed literature. These elements include points, leaderboards, narratives/storytelling, rewards, feedback, progression, achievements, levels, badges, challenges, avatars, tools, promotion/firing systems, agency, timers, competition, and prompts. While the frequency of use varies, with points and leaderboards being the most prevalent, these elements are not effective in every context. Among these, several game mechanics have been highlighted across studies for their particularly positive effects on learner engagement, motivation, and knowledge retention. Collectively, these include:

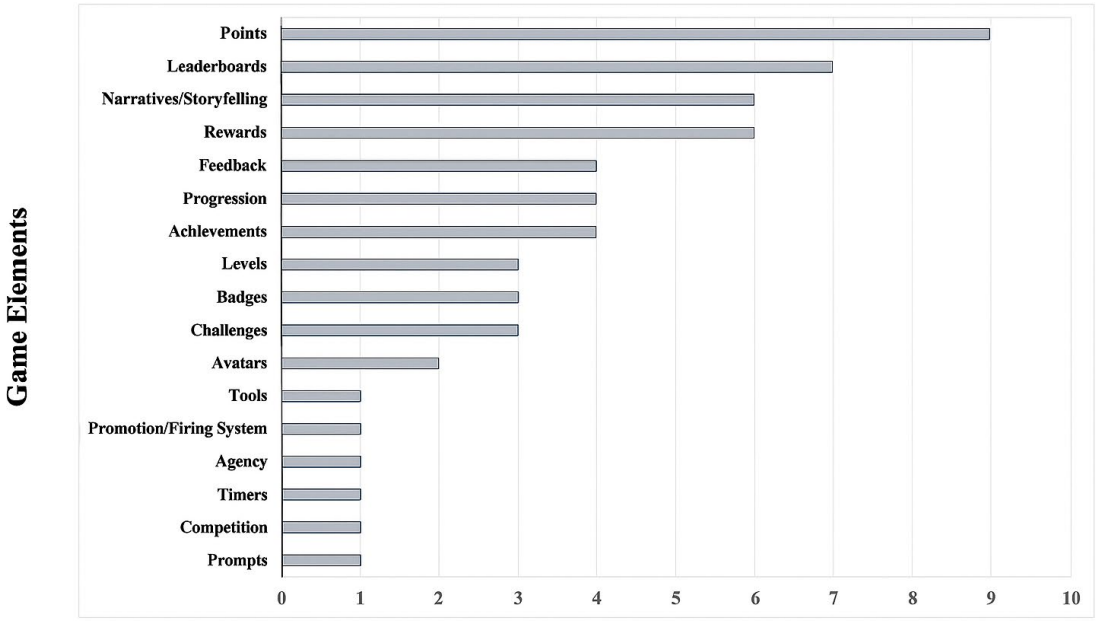


**Figure 3. Game elements in reviewed literature**

### Progress tracking and feedback mechanisms

Progress tracking, through features like progress bars and milestones, has been highlighted as an effective tool for sustaining motivation. For instance, one study emphasized that progress bars allow users to track completed and remaining tasks, maintaining their motivation to proceed (Gjertsen et al., 2017). Similarly, visual progress indicators were shown to encourage participants to persist in completing challenges (Wu et al., 2021). The same study also highlighted the importance of immediate feedback, noting that providing real-time corrective guidance helps learners feel a sense of achievement and promotes iterative learning (Wu et al., 2021).

### Competition and social interaction

Gamification mechanics like leaderboards, team-based competitions, and challenges have been found to enhance engagement through social interaction and competition. Leaderboards, in particular, have been shown to foster a competitive spirit and encourage participants to improve their performance (Matovu et al., 2022; Raisi et al., 2021). For some users, competition provides external validation and recognition, which motivates sustained participation (Gjertsen et al., 2017; Wu et al., 2021). However, it is important to keep in mind that some researchers caution that competitive elements should be applied judiciously, as overly intense competition may alienate participants, particularly those less confident in their abilities (Gjertsen et al., 2017; Natalia et al., 2023).

### Reward systems

The use of points, badges, and tangible or virtual rewards has been acknowledged for its role in motivating continued engagement. Rewards serve as positive reinforcement, encouraging participants to persist in cybersecurity programs (Wu et al., 2021). Another study echoed these findings, noting that reward systems like points, badges, and coins create both immediate and long-term goals, providing learners with a sense of accomplishment (Raisi et al., 2021).

## *RQ6. Negative Impacts of Game Elements*

Table 5 summarizes the negative impacts of specific gamification elements in cybersecurity initiatives as reported in various studies. While gamification has proven effective in enhancing engagement and learning, certain elements may hinder participation or motivation. For example, leaderboards, while motivating for some, can demoralize individuals who consistently rank low, leading to disengagement (Gjertsen et al., 2017; Raisi et al., 2021; Wu et al., 2021). Similarly, competitive elements can create stress for less confident participants or those focused on learning rather than comparison (Canham et al., 2022; Gjertsen et al., 2017; Matovu et al., 2022). Time constraints, often incorporated into gamified tasks, may frustrate slower learners or those struggling with decision-making under pressure (Matovu et al., 2022). When poorly designed or overly abstract, narratives can detract from the educational content, reducing their effectiveness (Berisford et al., 2022; Brehmer & Reinelt, 2023). Other elements, such as challenges, avatars, points, and extrinsic rewards, have been criticized for causing anxiety, perceived superficiality, or undermining intrinsic motivation (Raisi et al., 2021; Wu et al., 2021). These findings highlight the need for careful design and contextual adaptation of gamification elements to ensure they support diverse learner needs effectively. The negative impacts of each gamification element have been summarized into shorter phrases, preserving the original meaning to facilitate easier comprehension.

**Table 5. Reported negative impacts of specific gamification elements in cybersecurity initiatives**

| Gamification element | Negative impacts | References |
|---|---|---|
| Leaderboards | Demotivate low-ranking participants, leading to frustration and disengagement; induce stress in non-competitive environments; cause anxiety due to performance pressure. | (Canham et al., 2022; Gjertsen et al., 2017; Raisi et al., 2021; Wu et al., 2021) |
| Competition | Creates stress and discouragement for less confident users; not universally motivating, may shift focus to outperforming others rather than meaningful learning. | (Canham et al., 2022; Gjertsen et al., 2017; Matovu et al., 2022) |
| Time Pressure | Frustrates slower learners and those who struggle with quick decision-making, affecting their performance. | (Matovu et al., 2022) |
| Narratives | Repetitive or disconnected storylines can reduce relevance and effectiveness; poor narrative design may distract from learning objectives. | (Berisford et al., 2022; Brehmer & Reinelt, 2023; Raisi et al., 2021) |
| Challenges | Excessive difficulty can intimidate learners, lowering confidence and willingness to continue. | (Raisi et al., 2021) |
| Avatars | Perceived as superficial or lacking educational value, reducing learner engagement. | (Raisi et al., 2021) |
| Points | Overemphasis on earning points promotes superficial engagement, distracting from deep learning. | (Wu et al., 2021) |
| Rewards | Heavy reliance on external rewards weakens intrinsic motivation, diminishing long-term engagement. | (Wu et al., 2021) |

These impacts were then categorized into three key domains: Emotional Issues, Cognitive Issues, and Engagement Issues. Table 6 presents a structured overview of how specific gamified elements may influence learners by affecting their emotional well-being, cognitive processing, and sustained engagement with the content. To enhance clarity and streamline interpretation, based on the findings of Research Questions 5 and 6, the reported positive and/or negative effects of each gamification element were mapped into a unified visual representation. As shown in Table 7, this mapping enables a more intuitive understanding of which elements may produce both beneficial and negative outcomes.

**Table 6. Categorization of negative impacts of gamification elements by emotional, cognitive, and engagement domains**

| Gamification element | Emotional issues | Cognitive issues | Engagement issues |
|---|---|---|---|
| Leaderboards | Demotivation, frustration, anxiety | | Disengagement |
| Competition | Stress, discouragement | Surface learning | |
| Time Pressure | Frustration for slower learners | Impaired decision-making | |
| Narratives | | Disconnected, repetitive storylines | Reduced engagement |
| Challenges | Intimidation, reduced confidence | | Reluctance to continue |
| Avatars | | Trivial, lacks learning value | |
| Points | | Surface learning | |
| Rewards | Undermined intrinsic motivation | | Reduced long-term engagement |

**Table 7. Mapping of game elements and their reported positive and/or negative effects**

| Gamification element | Positive effect | Negative effect |
|---|---|---|
| Progress | Sustaining Motivation | |
| Feedback | Corrective Guidance | Surface Learning |
| Leaderboards | Fosters Competition | Demotivate |
| | | Stress |
| | | Anxiety |
| Competition | Enhance Engagement | Stress |
| | | Discouraging |
| Challenges | Enhance Engagement | Intimidating |
| Avatars | | Perceived as Superficial |
| Points | Reinforce Participation | Superficial Engagement |
| Rewards | Positive Reinforcement | Weaken Intrinsic Motivation |
| Narratives | | Distracting |
| Avatars | | Frustrating |

## *RQ 7. Gamification Design Frameworks In Use*

As illustrated in Figure 4, the majority of the reviewed studies adopted an ad hoc approach to gamification design. These initiatives were developed in a customized or improvised manner, often grounded in researchers' assumptions, prior empirical findings, intuition, or experiential insights, rather than being guided by an established theoretical framework (Abu-Amara et al., 2021; Berisford et

al., 2022; Brehmer & Reinelt, 2023; Canham et al., 2022; Chen et al., 2023; Gjertsen et al., 2017; Matovu et al., 2022; Raisi et al., 2021; Rikkers & Sarmah, 2025; Wu et al., 2021). This reliance on informal design strategies reflects a broader trend in the gamification literature, where the absence of structured methodological guidance may limit replicability, scalability, and theoretical consistency. In contrast, only two studies employed predefined gamification design frameworks to inform their development process: one utilized the Mechanics-Dynamics-Aesthetics (MDA) Framework (Natalia et al., 2023), while the other applied the Octalysis Framework (Rendreana et al., 2023). These instances demonstrate the potential of structured frameworks to enhance the conceptual clarity and strategic alignment of gamification interventions.

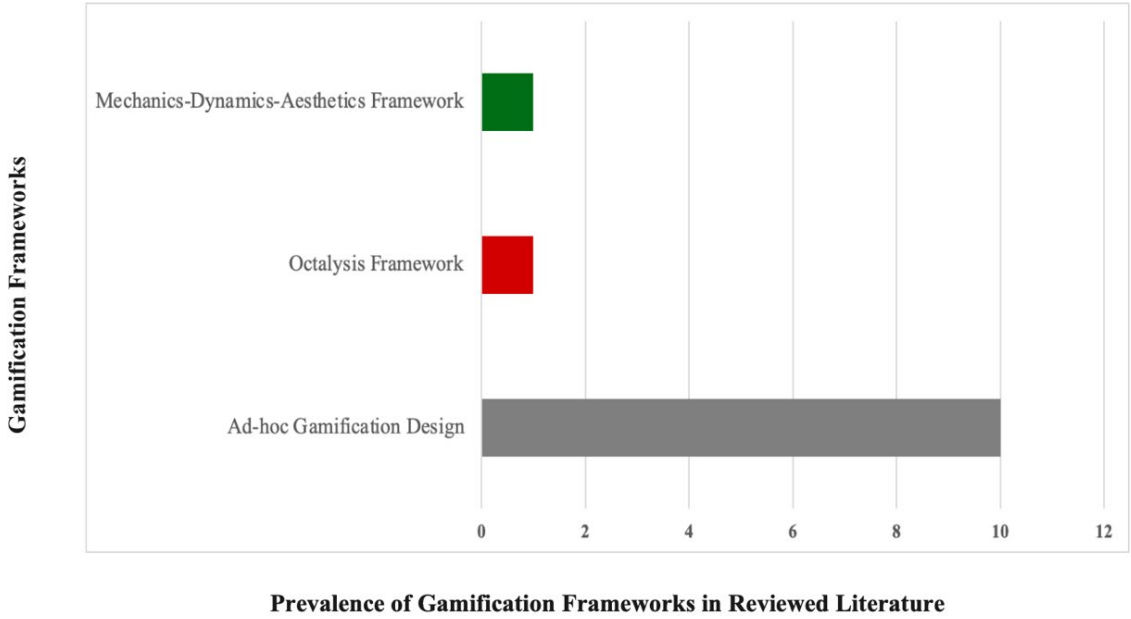


**Figure 4. Distribution of gamification design frameworks in reviewed studies**

## *RQ 8. Cybersecurity Topics Covered*

Table 8 presents a thematic categorization of the core cybersecurity topics addressed across gamified cybersecurity initiatives. The analysis reveals that phishing and social engineering constitute the most frequently targeted themes, reflecting the persistent threat posed by human-centered attacks and the necessity of cultivating vigilance in digital interactions. In parallel, password security and data protection are emphasized, highlighting their foundational role in safeguarding both individual and organizational assets. Web and Email Security emerges as another domain that is addressed, reflecting the widespread reliance on these platforms and their susceptibility to exploitation.

Beyond user-centric vulnerabilities, several gamified interventions incorporate more technically advanced themes, including cryptography, code security, and network security. Collectively, including human factors, technical competencies, and general cybersecurity principles indicates a holistic pedagogical approach that increases knowledge and encourages proactive and sustained security behavior among users.

**Table 8. Thematic classification of cybersecurity topics addressed in gamified initiatives**

| Common theme | Specific topics addressed | References |
|---|---|---|
| Phishing and Social Engineering | Phishing, deceptive phishing, link manipulation, in-session phishing, vishing, smishing, social engineering, baiting, tailgating, incident reporting | (Abu-Amara et al., 2021; Canham et al., 2022; Gjertsen et al., 2017; Matovu et al., 2022; Natalia et al., 2023; Wu et al., 2021) |
| Data Protection and Handling | Personal data protection, secure data storage, handling sensitive information, confidential data management | (Abu-Amara et al., 2021; Chen et al., 2023; Gjertsen et al., 2017; Rendreana et al., 2023; Rikkers & Sarmah, 2025) |
| Password Security | Creating strong passwords, secure password management | (Abu-Amara et al., 2021; Brehmer & Reinelt, 2023; Gjertsen et al., 2017; Natalia et al., 2023; Wu et al., 2021) |
| Web and Email Security | Web security, secure email practices, avoiding unsafe websites, internet usage | (Gjertsen et al., 2017; Raisi et al., 2021; Wu et al., 2021) |
| Code Security | Secure coding, SQL injection, broken access controls | (Berisford et al., 2022; Raisi et al., 2021) |
| Device and Media Security | Wireless security, mobile security, USB threats, removable media safety | (Gjertsen et al., 2017; Rikkers & Sarmah, 2025; Wu et al., 2021) |
| Network Security and Attacks | Network vulnerabilities, ethical hacking, reverse engineering | (Chen et al., 2023; Raisi et al., 2021) |
| Physical Security | Physical access control, tailgating prevention | (Abu-Amara et al., 2021; Gjertsen et al., 2017) |
| General Cybersecurity Awareness | Core principles, best practices, proactive security behavior | (Gjertsen et al., 2017; Raisi et al., 2021; Wu et al., 2021) |

# DISCUSSION

The findings of this systematic literature review provide valuable insights into the application, benefits, limitations, and future research opportunities regarding gamification in cybersecurity initiatives. Cumulative evidence from the reviewed studies suggests that gamification is a valuable strategy for enhancing cybersecurity education, training, and awareness by improving motivation, engagement, skill development, comprehension of cybersecurity concepts, and potentially promoting behavior change. Gamification can be argued to operate through a systematic process grounded in Self-Determination Theory (Ryan & Deci, 2000). Thus, by intentionally incorporating game elements that fulfill the needs for autonomy, competence, and relatedness (Ryan & Deci, 2000), gamification influences users' motivation, whether intrinsic or extrinsic. The type of motivation then drives specific behaviors and fosters engagement, leading to desired outcomes such as improved learning, productivity, participation, and potential behavior change. Therefore, gamification is not merely a tool for entertainment but a structured design approach that empowers users through psychologically meaningful experiences. However, several limitations and avenues for future research have also been identified, which are essential for advancing the effective application of gamification in cybersecurity initiatives.

## *Conceptual Misclassification of Gamification*

A persistent issue within the gamification literature is the frequent conflation of gamification with adjacent concepts such as game-based learning, serious games, simulations, and video games. This conceptual ambiguity has resulted in misclassification and inconsistency across studies. During the process of identifying relevant literature, several papers were excluded due to misuses of the term "gamification," wherein the interventions aligned with game-based learning or full-scale educational games rather than with the application of gamification principles. For example, studies such as Salman et al. (2023) deploy fully developed educational games with layered levels, narrative progression, and interactive simulations, which are features characteristic of serious games, yet label these interventions as gamified. This misclassification reduced the number of eligible studies, leaving only 12 eligible for inclusion.

A plausible underlying cause of conceptual misclassification may be poor definitional interpretation. Gamification, game-based learning, and serious games are grouped under the broader umbrella of gameful design approaches or game-based interventions. While these approaches share the common use of game-derived principles to enhance engagement and learning, they differ substantially in their structure, purpose, and design philosophy. To reiterate, gamification involves the integration of discrete game elements such as points, badges, or leaderboards into non-game contexts (Brehmer & Reinelt, 2023; Christensen et al., 2023; Tran et al., 2023). Serious games, in contrast, are purpose-built to teach specific skills or address real-world challenges, often incorporating immersive storytelling, role-playing, or simulation-based scenarios. Game-based learning refers to the use of complete games, whether originally designed for entertainment or educational purposes, as instructional tools (Al Fatta et al., 2018). Whether this conflation or misclassification occurs intentionally for simplicity or due to disciplinary conventions, or unintentionally through a lack of definitional awareness, it reinforces conceptual inconsistencies and risks misrepresenting the actual mechanisms influencing observed outcomes. In such cases, the impact of gamification may be overstated by attributing outcomes that were in fact achieved through other gameful methods.

To advance the field, it is critical to promote greater conceptual clarity and definitional rigor. This includes establishing clear distinctions regarding whether simulations fall within the scope of gamification or should be considered distinct pedagogical tools. Such clarity will improve methodological consistency across studies and enable more accurate assessment, comparison, and meta-analysis of gamification-specific interventions in cybersecurity initiatives and related domains.

## *Methodological Limitations and the Novelty Effect*

Although several studies have reported positive outcomes following the implementation of gamified cybersecurity initiatives, the absence of rigorous comparative designs in many cases complicates the interpretation of these results. A substantial number of studies (such as Abu-Amara et al., 2021; Brehmer & Reinelt, 2023; Canham et al., 2022; Chen et al., 2023; Gjertsen et al., 2017) did not employ a control group or pre-test structure. This omission makes it difficult to isolate the specific impact of gamification from other instructional approaches and confounding variables. Without these comparative benchmarks, claims regarding the efficacy of gamification remain speculative.

Moreover, although some studies incorporated both control groups and pre-test/post-test assessments, the duration of their interventions was either not reported or limited to only a few weeks (Natalia et al., 2023; Rendreana et al., 2023; Wu et al., 2021). This presents a methodological limitation in evaluating the true impact of gamification, particularly in light of the novelty effect. The novelty effect refers to a temporary increase in engagement or performance that occurs when individuals are exposed to a new or unfamiliar stimulus, such as gamified features, rather than the intrinsic efficacy of the intervention itself (Barrile et al., 1999). Research suggests that this effect generally lasts between two and four weeks (L. Rodrigues et al., 2022), after which user engagement and motivation tend to normalize or decline. Therefore, initiatives assessed within this novelty window may yield inflated results that do not reflect gamification's actual or sustainable impact.

Although such initiatives may show initial promise, especially in structured and time-bound settings such as educational courses or training sessions where learning objectives can be achieved through short-term engagement, they raise important concerns when applied to cybersecurity awareness programs. The goals of these programs extend beyond short-term knowledge acquisition and instead aim to foster long-term engagement, vigilance, and behavior change. Consequently, questions arise about whether short-term gamified interventions are adequate to support continuous engagement and sustained behavioral transformation. This is relevant in professional or utilitarian contexts, where users tend to be task-focused and may perceive gamified elements as trivial or irrelevant, thereby diminishing their effectiveness (Hamari et al., 2014).

As noted, such initiatives are often susceptible to the novelty effect. Initial engagement often fades as users become accustomed to the experience (Hamari et al., 2014; L. Rodrigues et al., 2022). Thus, the observed short-term effectiveness of many gamified interventions may not stem from the gamification design itself but rather from the transient appeal of novelty. This implies that although short-term gamification shows promise, its applicability to long-term cybersecurity awareness initiatives must be approached with caution. Programs of an enduring nature require strategies designed to sustain engagement over extended periods and to mitigate the diminishing influence of novelty and habituation. To that end, future research should adopt standardized reporting on the duration and outcomes of gamified interventions. This will be essential for understanding the relationship between gamification effectiveness and time. Additional studies are needed to identify and recommend optimal durations for gamified interventions across various contexts in order to credibly evaluate their potential to achieve long-term objectives. Without such clarity, the impact of gamified programs may remain ambiguous or overstated, as the effectiveness of gamification cannot be assessed in isolation from the duration and context of its implementation.

### *Overemphasis on Short-Term Performance Metrics*

The majority of studies on gamified interventions emphasize key performance indicators (KPIs) such as engagement, satisfaction, motivation, and knowledge retention or pass rates. While these metrics offer immediate and accessible insights into usability and short-term efficacy, they often neglect behavioral change as a critical indicator of success. This oversight is consequential in cybersecurity awareness, where the objective extends beyond knowledge acquisition to the sustained adoption of secure behaviors and compliance with security practices.

Focusing only on cognitive or affective outcomes may obscure gamification's long-term impact. As Wu et al. (2021) argue, knowledge-based assessments alone are insufficient to determine whether users translate what they learn into actionable, real-world behavior. This is a serious concern given that cybersecurity breaches often result not from ignorance, but from a failure to apply known best practices. To strengthen the rigor and relevance of gamification research in this domain, future studies should incorporate behavioral outcome measures. These may include adherence to security protocols, reduction in risky behavior, and sustained use of secure practices. Integrating such measures would provide a more holistic evaluation of gamified cybersecurity programs, ensuring they address both learning and behavioral transformation.

Although only a handful of studies assessed the impact of gamification on behavior change, the findings generally indicate a positive influence, though they must be interpreted with caution. For instance, one study concluded that gamification had a direct and positive impact on employee cybersecurity behavior (Canham et al., 2022). Similarly, gamification that combined narrative elements with team-based leaderboards led to measurable behavioral improvements (Brehmer & Reinelt, 2023). Another study demonstrated that story-driven gamification enhanced behavioral responses, especially in mitigating USB-based cyber threats, outperforming both non-narrative gamified approaches and traditional instructional methods (Rikkers & Sarmah, 2025). Significant improvements in observable cybersecurity behavior following gamified interventions were reported (Abu-Amara et al., 2021). One study noted the potential of gamification to improve security behavior by increasing the frequency

and motivational appeal of training, but emphasized that poorly designed elements, such as forced competition or irrelevant content, may lead to adverse behavioral effects (Gjertsen et al., 2017). Likewise, another study cautioned that gamification alone may not be sufficient to induce lasting behavioral change, highlighting the need for integration with complementary strategies (Chen et al., 2023). Therefore, while the behavioral impact of gamification is increasingly supported, it is not inherently guaranteed. The effectiveness of gamification depends heavily on the quality, relevance, and contextual alignment of its design.

## *Ambivalent Game Elements*

Several gamification elements demonstrated context-dependent and sometimes contradictory effects across the reviewed studies. Competitive elements such as leaderboards, team-based competitions, challenges, and time pressure were associated with increased engagement, motivation, and short-term participation (Raisi et al., 2021; Wu et al., 2021). However, when applied without careful consideration of user groups or situational context, these same elements were linked to negative outcomes. For example, leaderboards, team competitions, challenges, and time constraints were found to induce stress, disengagement, or demotivation among lower-performing or less confident users (Canham et al., 2022; Gjertsen et al., 2017; Matovu et al., 2022). Similarly, although points and rewards can support extrinsic motivation, several studies noted that excessive reliance on them encouraged superficial engagement and undermined intrinsic motivation (Raisi et al., 2021; Wu et al., 2021).

These findings highlight that some game elements operate as double-edged swords, offering benefits or causing harm depending on the learning environment and participant characteristics. Their effectiveness is not inherent but rather depends on thoughtful alignment with pedagogical goals, learner motivation, and emotional readiness. This insight also reveals a broader concern: many studies failed to assess the negative effects of gamification elements within their interventions. Merely reporting positive outcomes is insufficient and potentially harmful, as it may mislead future researchers or practitioners into repeating flawed designs without being aware of their limitations.

Based on these findings, it is recommended that researchers and practitioners apply the following game elements with caution: leaderboards, competition, time pressure, narratives, challenges, points, and extrinsic rewards. These can be termed context-sensitive gamification elements or ambivalent game elements, as they have the potential to serve as both a benefit and a drawback depending on the context. Their use should therefore be adaptive, inclusive, and evidence-informed, particularly in ETA initiatives, where participant diversity and learning needs vary significantly.

To support the thoughtful use of these ambivalent elements, several flexible and learner-centered design strategies can be considered. Personalized gamification can be used to tailor elements such as competition, rewards, or time constraints to individual learner profiles, aligning better with varying confidence levels, motivation types, and learning preferences. A gamification preference toggle can allow users to control how they interact with the system, for example, by opting out of leaderboards or selecting a relaxed pacing mode. A multi-pathway design can offer different routes, such as competitive, narrative-driven, or mastery-focused tracks, giving learners the opportunity to engage in ways that suit them best. Sentiment-aware feedback loops can be employed to monitor user experience through simple check-ins and make adjustments in response to signs of frustration or disengagement. During the design phase, an ethical gamification checklist can support the identification of potential trade-offs, such as between motivation and pressure or cooperation and competition. For users who prefer less public visibility, shadow progress systems can provide private feedback and internal tracking without reliance on comparison-based mechanisms. Finally, hybrid gamification combined with behavioral nudges can offer subtle motivators, such as peer examples ("80% of your peers have completed this") or reminder prompts, that encourage participation without adding competitive pressure.

Lastly, rather than focusing solely on the benefits of gamification, future research should also make it standard practice to report both the potential benefits and negative effects of game elements, particularly in relation to context and participant demographics. Collectively, such reporting, along with thoughtful design strategies, can contribute to more inclusive, adaptive, and context-aware gamified initiatives.

## *Limited Use Of Gamification Frameworks*

While it is commendable that a few studies have explored user variability, it remains evident that, in many cases, limited effort was made to understand user profiles in depth prior to implementation. Such understanding is critical for selecting game elements that align with the target audience and for avoiding negative reactions. Although frameworks like the Octalysis Framework (Chou, 2014) and the Gamification User Types Hexad (Marczewski & Uk, 2016) are available to help identify user motivations and guide element selection, they are not systematically applied in practice. Instead, many initiatives continue to rely on ad hoc design decisions. This raises an important question: why are these well-established frameworks, which offer valuable guidance, often neglected in real-world applications? Future research should investigate the factors influencing their limited adoption, which may include practical constraints, lack of awareness, or institutional inertia. Understanding these barriers will be essential for encouraging more strategic and evidence-based use of gamification frameworks in both research and practice.

## *Lack of Context-Specific Frameworks*

Although several gamification frameworks exist, they often lack explicit guidance on how to select game elements based on the specific context of implementation, focusing instead primarily on user motivations. Frameworks such as the Octalysis Framework and the Gamification User Types Hexad are effective in identifying user motivations and aligning game elements with individual preferences. However, they fall short in addressing scenarios where user motivations may conflict with the overarching objectives of a gamified initiative. One study argued that gamification strategies must be contextually grounded, as certain motivational drivers may lead to unintended or even counterproductive outcomes (Werbach & Hunter, 2020). For example, competitive elements like rankings and leaderboards may engage users with an achiever-oriented profile, yet these same elements may undermine collaboration and group cohesion in team-based environments. While gamification often taps into universal human desires (such as achievement, recognition, and competition), these motivations must be balanced to avoid negative consequences, particularly in collaborative, sensitive, or goal-specific contexts (Zichermann & Cunningham, 2011).

To address these limitations, future frameworks should move beyond motivation-centric models and incorporate context-sensitive design principles. This means ensuring that game elements are selected not only based on user profiles but also in alignment with the specific goals, environmental factors, and intended outcomes of the initiative. By integrating context-based recommendations, gamification frameworks can bridge the gap between motivational alignment and practical implementation, reducing the risk of undermining the initiative's core objectives. Ultimately, next-generation gamification frameworks should guide practitioners in designing systems that are not only engaging and motivating but also tailored to the contextual and strategic needs of the target environment.

## *Influence Of Confounding Factors*

While gamification has been associated with increased motivation, engagement, and various other positive outcomes, it is essential to examine the underlying factors that contribute to these effects in order to understand its actual impact. The success of gamification is not inherent or guaranteed; rather, it may be influenced by confounding variables that are not consistently accounted for, controlled, or measured in many studies (Hamari et al., 2014). Thus, although gamified interventions often enhance engagement, motivation, and knowledge acquisition, factors external to the gamification

itself, such as pre-existing intrinsic motivation or contextual influences, may contribute to these outcomes (Wu et al., 2021).

For instance, in educational contexts, fear of failure may act as a more powerful motivator than the presence of game elements. However, in professional training settings, the desire to develop skills for career advancement may drive participation independently of gamification. In such cases, the presence of game mechanics might coincide with increased engagement, yet not be the primary causal factor. Accordingly, these additional motivational drivers may operate independently of gamification, thereby diluting its isolated effect.

Consequently, the explanatory power of gamification as reflected in the R-squared value in empirical models may be relatively low, suggesting that gamification alone accounts for only a limited proportion of the observed variance in outcomes. This highlights the need for future research to assess the relative contribution of gamification, especially in contexts where multiple motivational factors are at play. To achieve this, researchers must employ rigorous experimental designs, including the use of appropriate control groups, to isolate the specific impact of gamified interventions from other influencing variables.

## *Gamification in Policy Engagement: An Untapped Potential*

Despite a handful of attempts in gamified cybersecurity initiatives, organizational internal cybersecurity policies remain an underexplored area. In many organizations, these policies are still disseminated as static documents that employees seldom read or actively engage with. This limited interaction significantly hinders policy awareness and reduces the likelihood of compliance. Integrating gamification into the communication and dissemination of internal cybersecurity policies presents a promising opportunity to transform these documents into interactive and engaging tools. Given the critical role that internal cybersecurity policy awareness plays in organizational cybersecurity posture, this area represents a high-potential avenue for future research and innovation, particularly in efforts aimed at enhancing cybersecurity compliance across institutions.

## *Persistent Gaps And Lack Of Progress*

There is a consistent recurrence of unresolved issues within the gamification research field, many of which were already identified more than a decade ago. For example, positive outcomes observed in gamification studies may be influenced more by the novelty effect, where user interest is elevated due to the newness of the intervention, rather than by the actual effectiveness of the gamification design (Hamari et al., 2014). The importance of conducting longitudinal studies to assess the long-term sustainability of gamification's impact has likewise been emphasized (van Roy & Zaman, 2017). Despite these early and well-documented recommendations, and although the current review includes studies published from 2017 onward, which is at least three years after those recommendations were made, most studies in this area continue to rely on short-term interventions. For instance, almost all papers reviewed in this context, including but not limited to Canham et al. (2022), Natalia et al. (2023), and Rendreana et al. (2023), relied on short-term interventions without any follow-up. These studies fall within the novelty period described in earlier research, making it difficult to determine whether the reported effects reflect genuine lasting impact or are merely temporary responses to initial exposure (L. Rodrigues et al., 2022).

Thus, despite the passage of time, little meaningful progress has been made in addressing these methodological gaps. Researchers often continue to use approaches that have been critiqued and recommended for revision, raising a critical question: Why are these recommendations not being implemented or expanded upon? Future research must move beyond repeating known limitations and instead explore the underlying reasons for this lack of progress. Possible explanations may include practical challenges such as limited access to long-term study participants, time constraints, publication pressures that favor shorter studies, or insufficient institutional support for extended research timelines. Unless these structural and methodological barriers are identified and addressed, the field

risks remaining stagnant. Advancing gamification research in a meaningful way requires not only recognizing persistent limitations but also investigating the reasons for their continued presence and finding ways to overcome them.

## CONCLUSIONS

This study set out to investigate the effectiveness, limitations, and design considerations of gamification ETA initiatives. The motivation stemmed from two persistent challenges: the human factor in cybersecurity breaches and declining engagement associated with traditional ETA methods. Although gamification has attracted increasing enthusiasm, evidence of its sustained effectiveness in cybersecurity contexts remains fragmented and methodologically inconsistent. This gap underscored the need for a rigorous synthesis of empirical research to guide both academic inquiry and practical application.

To address this objective, a systematic literature review was conducted following PRISMA guidelines and established review protocols. An automated search strategy was applied using Scopus, which was selected for its comprehensive and high-quality peer-reviewed coverage. The search targeted English-language literature published between 2017 and 2024, focusing specifically on studies that implemented gamified interventions in cybersecurity ETA contexts. From an initial pool of 114 records, a multi-stage screening process encompassing definitional clarity, empirical focus, cybersecurity relevance, and full-text availability was implemented. This was followed by peer validation using binary inclusion criteria, resulting in a final set of 12 high-quality empirical studies. While limited in number, these studies reached thematic saturation, offering robust insights into current practices and challenges in the field.

The findings of this review, structured around eight guiding research questions, reveal several key insights. First, gamified interventions most frequently targeted awareness, followed by training and education, although many displayed hybrid characteristics. Second, these initiatives pursued multidimensional outcomes, most commonly engagement, motivation, and awareness, along with behavior change, skill development, and knowledge retention. Third, across all studies, gamified interventions consistently outperformed non-gamified or pre-gamified approaches in enhancing user engagement and motivation. However, evidence for long-term behavioral change remained mixed or insufficient.

Fourth, most initiatives were short-term, often lasting under 15 minutes or comprising a single session, with few extending beyond one month. This raised concerns about sustainability in light of the novelty effect, where early engagement may reflect temporary excitement rather than genuine or lasting impact. Fifth, commonly used and positively evaluated game elements included points, leaderboards, and narratives, though their effectiveness was highly dependent on context. Sixth, several elements, including competition, time pressure, and leaderboards, also exhibited negative effects such as stress, disengagement, and reduced intrinsic motivation, especially when poorly aligned with user profiles. Seventh, most studies lacked the use of structured gamification frameworks, with only two explicitly employing models such as Octalysis or MDA. Finally, while reviewed initiatives addressed a variety of cybersecurity topics, there was a dominant focus on phishing, data protection, and password security, with fewer studies exploring less-addressed domains such as policy engagement or network security.

These findings have several implications. Conceptually, the ongoing misclassification of gamification, often conflated with serious games or simulations, highlights the need for clearer definitions to avoid inflated claims of effectiveness. Methodologically, many studies failed to incorporate control groups, longitudinal tracking, or behavioral outcome measures, which limit causal inferences and underrepresent long-term impact.

One key limitation is the short duration of most initiatives. Many interventions were evaluated immediately after brief exposure, often less than one hour or within a four-week period, without examining retention or behavior beyond the initial novelty phase. In cybersecurity awareness contexts, where lasting vigilance and behavioral transformation are critical, this is especially problematic. The novelty effect, characterized by a temporary surge in engagement due to new or unfamiliar stimuli, may artificially elevate perceived effectiveness. Without longitudinal designs, short-term success can be easily mistaken for sustainable impact.

Additionally, some game elements exhibited ambivalent, context-dependent effects, functioning as double-edged tools that could either enhance or hinder learning. For instance, while leaderboards and competition boosted motivation in certain contexts, they also caused stress or disengagement among less confident users. Despite this, many studies reported only positive outcomes, overlooking potential drawbacks. This type of reporting risks reinforcing ineffective or even harmful design practices.

Practically, the lack of user-centered design approaches and the underutilization of established motivational frameworks such as Hexad and Octalysis indicate the need for more deliberate, evidence-based development. Furthermore, despite growing interest in gamified cybersecurity interventions, internal policy awareness remains a critically underexplored area. Given the centrality of internal policies to organizational cybersecurity posture, this represents a significant missed opportunity for research and innovation.

In summation, while gamification holds considerable promise for enhancing cybersecurity ETA initiatives, its effectiveness is not guaranteed. Success depends on factors such as duration, contextual alignment, theoretical grounding, and user-centered design. To realize the transformative potential of gamification, future research must prioritize longitudinal evaluation, behavioral outcome measurement in cases of awareness, and the development of comprehensive, context-sensitive frameworks that integrate both motivation and environmental constraints. Only through such rigor can gamification mature from an experimental novelty into a credible and sustainable educational methodology.

Beyond academic and organizational settings, the need to adapt is amplified by evolving societal expectations and the challenge of meeting them. The urgency to reform cybersecurity learning is intensified by the rise of digitally native generations, learners accustomed to games, mobile interfaces, and interactive media. For these audiences, traditional methods such as static documents or slide-based instruction may fail to capture interest or promote retention. Gamification presents a compelling opportunity to align cybersecurity education, training, and awareness with these digital expectations.

Theoretically, this review reinforces the need to move beyond isolated game elements or motivation triggers and toward strategically grounded, long-term, and context-sensitive designs. When applied with theoretical depth, empirical rigor, and adaptive sensitivity to user and organizational contexts, gamification can serve not just as a tool for engagement but as a transformative mechanism for cultivating cybersecurity mindsets and behaviors that endure.

## *LIMITATIONS*

This review is subject to several important limitations. First, the final pool included only 12 empirical studies. While this number may appear small, it reflects the widespread conceptual conflation of gamification with adjacent approaches such as serious games, game-based learning, and simulations. Many studies were excluded not due to quality concerns, but because they mislabeled non-gamified interventions as gamification, thereby failing to meet the definitional and methodological criteria of this review. Second, a substantial portion of the literature in this field remains conceptual or theoretical. While such works offer valuable frameworks and perspectives, they often lack empirical data on implementation or outcomes. Since this review focused on empirical studies to assess effectiveness, these conceptual contributions were excluded. This decision sharpened the analytical focus but limited the diversity of insights and approaches included.

Although the selected studies achieved thematic saturation and addressed the predefined research objectives, the inherent limitation of a small sample size warrants cautious interpretation of the findings. The results offer meaningful insights into the selected period gamification practices in cybersecurity but may not be fully generalizable across other periods and contexts. Future reviews that consider broader inclusion criteria, and or complementary conceptual studies could help extend and enrich these findings.

### *FUTURE RESEARCH DIRECTIONS*

Based on the gaps observed and recommendations proposed throughout the course of this review, Table 9 reiterates these directions along with their underlying rationale in a more structured and consolidated format to guide future research and practice in the design, implementation, and evaluation of gamified cybersecurity initiatives.

**Table 9. Future research recommendations for gamified cybersecurity initiatives**

| Recommendation | Justification |
|---|---|
| Define clear boundaries between gamification and related methods | Misuse and conceptual overlap with serious games, simulations, and game-based learning led to exclusions during study selection. Clear definitions are needed to improve methodological consistency and facilitate accurate analysis. |
| Systematically report context-specific negative effects | Most studies emphasized only positive outcomes. Transparent documentation of unintended emotional or cognitive impacts (e.g., stress from leaderboards, disengagement) will support inclusive, user-sensitive design. |
| Create contextually aware gamification frameworks | Existing frameworks focus mainly on user motivation. Future models should integrate situational factors such as learning goals, context, and user demographics to improve practical relevance and scalability. |
| Investigate sustainability beyond the novelty phase | Short intervention durations dominated current studies. Longitudinal research is needed to assess whether engagement and behavioral impacts persist after the initial novelty wears off. |
| Determine effective duration thresholds for outcomes | Many gamified interventions failed to report the length of the intervention or used overly short sessions that fall within the novelty period. Identifying optimal exposure durations will help ensure both efficiency and effectiveness of outcomes. |
| Clarify the conceptual overlap between gamification and simulations | Unclear treatment of simulations creates definitional confusion. Clarifying whether and how simulations fit within gamification will improve theoretical precision and intervention design. |
| Standardize reporting across studies | Inconsistent documentation of intervention features, context, duration, and outcomes impedes synthesis and replication. Implementing standardized reporting guidelines will support the development of cumulative knowledge. |
| Apply gamification to internal cybersecurity policy awareness | Internal policy compliance remains underexplored despite its importance. Gamifying policy content can improve employee engagement, understanding, and adherence to organizational security practices. |

## ACKNOWLEDGMENT

The first author gratefully acknowledges the support of the Sirindhorn International Institute of Technology (SIIT) and Thammasat University (TU) through the Excellent Foreign Students (EFS-A)

Scholarship and the TU PhD Scholarship. This research was supported by the SIIT Young Research Grant under Contract No. SIIT 2022-YRG-SN02.

## REFERENCES

Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology*, *13*(6), 2371–2380. https://doi.org/10.1007/s41870-021-00760-5

Al Fatta, H., Maksom, Z., & Zakaria, M. H. (2018). Game-based learning and gamification: Searching for definitions. *International Journal of Simulation: Systems, Science and Technology*, *19*(6), 41.1–41.5. https://doi.org/10.5013/IJSSST.a.19.06.41

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information*, *11*(2), 121. https://doi.org/10.3390/info11020121

Armstrong, M. E., Jones, K. S., Namin, A. S., & Newton, D. C. (2018). The knowledge, skills, and abilities used by penetration testers: Results of interviews with cybersecurity professionals in vulnerability assessment and management. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62*(1), 709–713. https://doi.org/10.1177/1541931218621161

Armstrong, R., Hall, B. J., Doyle, J., & Waters, E. (2011). 'Scoping the scope' of a Cochrane review. *Journal of Public Health*, *33*(1), 147–150. https://doi.org/10.1093/pubmed/fdr015

Arora, B. (2019). Teaching cyber security to non-tech students. *Politics*, *39*(2), 252–265. https://doi.org/10.1177/0263395718760960

Azman, A. A., Leow, A. T. C., Noor, N. D. M., Noor, S. A. M., Latip, W., & Ali, M. S. M. (2024). Worldwide trend discovery of structural and functional relationship of metallo-β-lactamase for structure-based drug design: A bibliometric evaluation and patent analysis. *International Journal of Biological Macromolecules*, *256*, 128230. https://doi.org/10.1016/j.ijbiomac.2023.128230

Balakrishna, C., & Charlton, P. (2022). Using game-based learning methods to demystify cyber security concepts for adult learners. *Proceedings of the 16th European Conference on Games Based Learning*, *16*(1), 73–80. https://doi.org/10.34190/ecgbl.16.1.804

Bardach, L., & Murayama, K. (2025). The role of rewards in motivation – Beyond dichotomies. *Learning and Instruction*, *96*, 102056. https://doi.org/10.1016/j.learninstruc.2024.102056

Barrile, M., Armstrong, E. S., & Bower, T. G. R. (1999). Novelty and frequency as determinants of newborn preference. *Developmental Science*, *2*(1), 47–52). https://doi.org/10.1111/1467-7687.00053

Benito, O. P., Ahmed, N. I., Prasetyo, Y. T., Cahigas, M. M. L., & Nadlifatin, R. (2025). Factors affecting the drought preparedness in Somaliland. *Sustainability*, *17*(2), 668. https://doi.org/10.3390/su17020668

Berisford, C. J., Blackburn, L., Ollett, J. M., Tonner, T. B., Yuen, C. S. H., Walton, R., & Olayinka, O. (2022). Can gamification help to teach Cybersecurity? *Proceedings of the 20th International Conference on Information Technology Based Higher Education and Training, Antalya, Turkey,* 1–9. https://doi.org/10.1109/ITHET56107.2022.10031716

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being "systematic" in literature reviews in IS. *Journal of Information Technology*, *30*(2), 161–173. https://doi.org/10.1057/jit.2014.26

Brehmer, M., & Reinelt, R. (2023). Gamifying a learning management system: Narrative and team leaderboard in the context of effective information security education. *Proceedings of the 56th Hawaii International Conference on System Sciences*, 24–33. https://doi.org/10.24251/HICSS.2023.005

Briner, R. B., & Denyer, D. (2012). Systematic review and evidence synthesis as a practice and scholarship tool. In D. M. Rousseau (Ed.), *The Oxford handbook of evidence-based management* (pp. 112–129). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199763986.013.0007

Burrell, D. N. (2018). An exploration of the cybersecurity workforce shortage. *International Journal of Hyperconnectivity and the Internet of Things*, *2*(1), 1072–1081. https://doi.org/10.4018/IJHIoT.2018010103

Calles-Esteban, F., Hellín, C. J., Tayebi, A., Liu, H., López-Benítez, M., & Gómez, J. (2024). Influence of gamification on the commitment of the students of a programming course: A case study. *Applied Sciences*, *14*(8), 3475. https://doi.org/10.3390/app14083475

Canham, M., Posey, C., & Constantino, M. (2022). Phish Derby: Shoring the human shield through gamified phishing attacks. *Frontiers in Education*, *6*, Article 807277. https://doi.org/10.3389/feduc.2021.807277

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz001

Chang, S. J., Kim, G. M., & Kim, J. A. (2024). The effects of flipped learning and gamification on nursing students' patient safety education: A mixed method study. *Heliyon*, *10*(8), e29538. https://doi.org/10.1016/j.heliyon.2024.e29538

Chen, H., Zhang, Y., Zhang, S., & Lyu, T. (2023). Exploring the role of gamified information security education systems on information security awareness and protection behavioral intention. *Education and Information Technologies*, *28*(12), 15915–15948. https://doi.org/10.1007/s10639-023-11771-z

Choi, Y. B., & Rubin, J. (2023). Social engineering cyber threats. *Journal of Global Awareness*, *4*(2), Article 8. https://doi.org/10.24073/jga/4/02/08

Chou, Y.-K. (2014). *Actionable gamification: Beyond points, badges, and leaderboards.*

Christensen, M., Britze, D., Vejlin, J., Sorensen, L. T., & Pedersen, J. M. (2023, May). The privacy universe – A game-based learning platform for data protection, privacy and ethics. *Proceedings of the IEEE Global Engineering Education Conference, Kuwait, Kuwait,* 1–8. https://doi.org/10.1109/EDUCON54358.2023.10125160

Christians, G. (2018). *The origins and future of gamification* [Senior Thesis, University of South Carolina]. https://scholarcommons.sc.edu/senior_theses

Coker, J. (2025, March 11). *95% of data breaches tied to human error in 2024*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/data-breaches-human-error/

Csikszentmihalyi, M. (1990). *The psychology of optimal experience* (1st ed.). Harper & Row. https://doi.org/https://www.researchgate.net/publication/224927532_Flow_The_Psychology_of_Optimal_Experience

Dah, J., Hussin, N., Zaini, M. K., Isaac Helda, L., Senanu Ametefe, D., & Adozuka Aliu, A. (2024). Gamification is not working: Why? *Games and Culture*. https://doi.org/10.1177/15554120241228125

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The new frontier of cybersecurity: Emerging threats and innovations. *Proceedings of the 29th International Conference on Telecommunications*, *Toba, Indonesia,* 1–6. https://doi.org/10.1109/ICT60153.2023.10374044

Davies, G., Mison, A., & Eden, P. (2022). Addressing the skills shortage. *International Conference on Cyber Warfare and Security*, *17*(1), 544–551. https://doi.org/10.34190/iccws.17.1.69

Decusatis, C., Alvarico, E., & Dirahoui, O. (2022). Gamification of cybersecurity training. *Proceedings of the 1st International Workshop on Gamification of Software Development, Verification, and Validation* (pp. 10–13). Association for Computing Machinery. https://doi.org/10.1145/3548771.3561409

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, *54*(8), Article 173. https://doi.org/10.1145/3469886

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011, September 28). From game design elements to gamefulness: Defining "gamification". *Proceedings of the 15th International Academic MindTrek Conference Envisioning Future Media Environments* (pp. 9-15). Association for Computing Machinery. https://doi.org/10.1145/2181037.2181040

Eger, V. M., Georganta, E., Zuercher, P. D. J., Mueller, F., Bohné, T., & Diefenbach, S. (2024). The power of play: Gamification in virtual workplace training. *European Journal of Work and Organizational Psychology*, *34*(2), 218–236. https://doi.org/10.1080/1359432X.2024.2412360

Egger, M., Altman, D. G., & Smith, D. G. (2006). *Systematic reviews in health care: Meta-analysis in context*. BMJ Books. https://www.amazon.com/Systematic-Reviews-Health-Care-Meta-Analysis/dp/072791488X

Feng, Z., Lau, N., Zhu, M., Liu, M., Refati, R., Huang, X., & Lee, K. (2023). Behavioural design of gamification elements and exploration of player types in youth basketball training. *Smart Learning Environments*, *10*, Article 56. https://doi.org/10.1186/s40561-023-00278-2

Fischer, S., & Barabasch, A. (2020). Gamification: A novel didactical approach for 21st century learning. In E. Wuttke, J. Seifried, & H. Niegemann (Eds.), Vocational education and training in the age of digitization: Challenges and opportunities (pp. 89-106). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctv18dvv1c.8

Gharbaoui, H., Mansouri, K., & Poirier, F. (2025). Social learning and gamification strategies for optimizing online learning in a computer science course. *International Journal of Engineering Pedagogy*, *15*(3), 60–74. https://doi.org/10.3991/ijep.v15i3.54101

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., & Flores, W. R. (2017). Gamification of information security awareness and training. *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, *Porto, Portugal,* 59–70. https://doi.org/10.5220/0006128500590070

Grobbelaar, C., & Alsemgeest, L. (2024). Gamification as an educational tool for retirement planning. *Adult Learning*. https://doi.org/10.1177/10451595241286913

Gwenhure, A. K., & Rahayu, F. S. (2024). Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review. *International Journal of Serious Games*, *11*(1), 83–99. https://doi.org/10.17083/ijsg.v11i1.719

Hamari, J., Koivisto, J., & Sarsa, H. (2014, January). Does gamification work? A literature review of empirical studies on gamification. *Proceedings of the 47th Hawaii International Conference on System Sciences*, *Waikoloa, HI, USA*, 3025–3034. https://doi.org/10.1109/HICSS.2014.377

Harding, J., Snyman, D., & Drevin, G. R. (2022). Establishing cybersecurity awareness of technical security measures through a serious game. *International Conferences on Applied Computing and WWW/Internet*. https://www.computing-conf.org/wp-content/uploads/2022/11/2_AC2022_S_082.pdf

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science and Medicine*, *292,* 114523. https://doi.org/10.1016/j.socscimed.2021.114523

Higgins, J. P. T., Altman, D. G., Gøtzsche, P. C., Jüni, P., Moher, D., Oxman, A. D., Savović, J., Schulz, K. F., Weeks, L., & Sterne, J. A. C. (2011). The Cochrane Collaboration's tool for assessing risk of bias in randomised trials. *BMJ*, *343*. https://doi.org/10.1136/bmj.d5928

Hossein, M. P., Ansari, M., Fekri, N., & Yazdimoghaddam, H. (2025). The effects of e-learning vs. gamification-based training on ICU nurses' knowledge and attitudes toward organ donation candidates: A study based on the psychological security and empowerment model. *BMC Medical Education*, *25*, Article 760. https://doi.org/10.1186/s12909-025-07299-0

Kamalodeen, V. J., Ramsawak-Jodha, N., Figaro-Henry, S., Jaggernauth, S. J., & Dedovets, Z. (2021). Designing gamification for geometry in elementary schools: Insights from the designers. *Smart Learning Environments*, *8*, Article 36. https://doi.org/10.1186/s40561-021-00181-8

Kitchenham, B. A. (2004). *Procedures for performing systematic reviews*. NICTA Technical Report 0400011T.1. https://www.researchgate.net/publication/228756057_Procedures_for_Performing_Systematic_Reviews

Kitchenham, B. A. (2007). *Guidelines for performing systematic literature reviews in software engineering*. EBSE Technical Report. https://www.researchgate.net/publication/302924724

Kitchenham, B. A., Budgen, D., & Brereton, P. (2015). *Evidence-based software engineering and systematic reviews*. Chapman & Hall/CRC. https://doi.org/10.1201/b19467

Lamé, G. (2019). Systematic literature reviews: An introduction. *Proceedings of the International Conference on Engineering Design Delft, The Netherlands*, 1633–1642. https://doi.org/10.1017/dsi.2019.169

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *PLoS Medicine*, *6*(7), e1000100. https://doi.org/10.1371/journal.pmed.1000100

Mallick, A., & Waheed, S. (2024). Learning urogenital diseases in oddity (LUDO) – A gamification-based innovation for learning urogenital diseases in emergency medicine. *International Journal of Emergency Medicine*, *17*, Article 8. https://doi.org/10.1186/s12245-023-00567-0

Marczewski, A., & Uk, G. (2016). User types HEXAD. In Dutch Driver (Ed.), *User types hexad* (1st ed.). Dutch Driver. https://www.researchgate.net/publication/303920474

Mastercard Trust Center. (n.d.). *Cybersecurity solutions for every business*. https://caribbean.mastercard.com/en-region-car/business/overview/safety-and-security/cybersecurity.html

Matovu, R., Nwokeji, J. C., Holmes, T., & Rahman, T. (2022, October). Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges. *Proceedings of the IEEE Frontiers in Education Conference, Uppsala, Sweden,* 1–9. https://doi.org/10.1109/FIE56618.2022.9962519

McSweeney, F. K., & Murphy, E. S. (2009). Sensitization and habituation regulate reinforcer effectiveness. *Neurobiology of Learning and Memory*, *92*(2), 189–198. https://doi.org/10.1016/j.nlm.2008.07.002

Meng, C., Zhao, M., Pan, Z., Pan, Q., & Bonk, C. J. (2024). Investigating the impact of gamification components on online learners' engagement. *Smart Learning Environments*, *11*, Article 47. https://doi.org/10.1186/s40561-024-00336-3

Mercuri, E. G. F., Kumata, A. Y. J., Amaral, E. B., & Vitule, J. R. S. (2016). Energy by microbial fuel cells: Scientometric global synthesis and challenges. *Renewable and Sustainable Energy Reviews*, *65*, 832–840. https://doi.org/10.1016/j.rser.2016.06.050

Min, S., Atan, N. A., & Habibi, A. (2025). Gamification with self-determination theory to foster intercultural communicative competence and intrinsic motivation. *International Journal of Evaluation and Research in Education*, *14*(3), 1985–1994. https://doi.org/10.11591/ijere.v14i3.29858

Mogoane, S. N., & Kabanda, S. (2019). Challenges in information and cybersecurity program offering at higher education institutions. *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems*, *12*, 202–212. https://doi.org/10.29007/nptx

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., Antes, G., Atkins, D., Barbour, V., Barrowman, N., Berlin, J. A., Clark, J., Clarke, M., Cook, D., D'Amico, R., Deeks, J. J., Devereaux, P. J., Dickersin, K., Egger, M., Ernst, E., Gøtzsche, P. C., … Tugwell, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine*, *6*(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Muangsrinoon, S., & Boonbrahm, P. (2019). Game elements from literature review of gamification in healthcare context. *Journal of Technology and Science Education*, *9*(1), 20–31. https://doi.org/10.3926/jotse.556

Natalia, M. C., Cayhono, S., Purwoko, R., & Maha Putra, I. G. (2023, November). Gamification design as learning media to motivate students to increase cyber security awareness towards phishing. *Proceedings of the International Conference on Informatics, Multimedia, Cyber and Information Systems*, *Jakarta Selatan, Indonesia,* 252–256. https://doi.org/10.1109/ICIMCIS60089.2023.10349069

Page, M. J., Moher, D., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., Mcdonald, S., … Mckenzie, J. E. (2021). PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *The BMJ*, *372*(160). https://doi.org/10.1136/bmj.n160

Paré, G., Trudel, M. C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information and Management*, *52*(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

Petrykina, Y., Schwartz-Chassidim, H., & Toch, E. (2021). Nudging users towards online safety using gamified environments. *Computers and Security*, *108,* 102270. https://doi.org/10.1016/j.cose.2021.102270

Piper, R. J. (2013). *How to write a systematic literature review: A guide for medical students*. Studypool. https://www.studypool.com/documents/39279887/how-to-write-a-systematic-literature-review-a-guide-for-medical-students

Pitthan, F., & De Witte, K. (2025). Game over or continue? How gamification can improve completion rate in adaptive learning. *Education and Information Technologies*, *30*, 2757–2786. https://doi.org/10.1007/s10639-024-12928-0

Pranckutė, R. (2021). Web of Science (WoS) and Scopus: The titans of bibliographic information in today's academic world. *Publications*, *9*(1), 12. https://doi.org/10.3390/publications9010012

Qusa, H., & Tarazi, J. (2021, January). Cyber-Hero: A gamification framework for cyber security awareness for high school students. *Proceedings of the IEEE 11th Annual Computing and Communication Workshop and Conference*, *NV, USA,* 677–682. https://doi.org/10.1109/CCWC51732.2021.9375847

Rahayu, F. S., Nugroho, L. E., Ferdiana, R., & Setyohadi, D. B. (2020). Research trend on the use of it in digital addiction: An investigation using a systematic literature review. *Future Internet*, *12*(10), 1–23. https://doi.org/10.3390/fi12100174

Raisi, S., Ghasemshirazi, S., & Shirvani, G. (2021, December). UltraLearn: Next-generation cybersecurity learning platform. *Proceedings of the 12th International Conference on Information and Knowledge Technology*, *Babol, Iran,* 83–88. https://doi.org/10.1109/IKT54664.2021.9685940

Rendreana, N. A., Cahyono, S., & Wijayanti, R. A. (2023, November). Implementation of gamification to enhance understanding of personal data protection based on Republic of Indonesia Law Number 27 of 2022. *Proceedings of the International Conference on Informatics, Multimedia, Cyber and Information Systems, Jakarta Selatan, Indonesia*, 246–251. https://doi.org/10.1109/ICIMCIS60089.2023.10349080

Rey, W., & Defensor, K. E. (2024). OS Odyssey: Developing and assessing gamified learning in operating systems instruction. *Proceedings of the 8th International Conference on Digital Technology in Education* (pp. 78–83). Association for Computing Machinery. https://doi.org/10.1145/3696230.3696259

Ribeiro e Silva, M., & Carneiro, P. J. (2025). Game on! Antecedents and consequents of gamification in the workplace. *Journal of Workplace Learning, 37*(2), 153-170. https://doi.org/10.1108/JWL-09-2024-0193

Rikkers, V., & Sarmah, D. K. (2025). A story-driven gamified education on USB-based attack. *Journal of Computing in Higher Education, 37,* 248–272. https://doi.org/10.1007/s12528-023-09392-z

Rodrigues, L., Pereira, F. D., Toda, A. M., Palomino, P. T., Pessoa, M., Carvalho, L. S. G., Fernandes, D., Oliveira, E. H. T., Cristea, A. I., & Isotani, S. (2022). Gamification suffers from the novelty effect but benefits from the familiarization effect: Findings from a longitudinal study. *International Journal of Educational Technology in Higher Education*, *19*, Article 13. https://doi.org/10.1186/s41239-021-00314-6

Rodrigues, M. R., & Mira da Silva, M. (2025). Evaluating a gamified MOOC. *Cogent Education*, *12*(1), Article 2479400. https://doi.org/10.1080/2331186X.2025.2479400

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist, 55*(1), 68–78. https://doi.org/10.1037//0003-066X.55.1.68

Salman, O. H., Alawida, M., Abu Hazeem, R. M., Zeyadeh, M. S., & Alameri, M. R. (2023, December). CyberSafe: A gamified cyber security training method. *Proceedings of the 4th International Conference on Electrical, Communication and Computer Engineering, Dubai, United Arab Emirates,* 1-6. https://doi.org/10.1109/ICECCE61019.2023.10442243

Scherb, C., Bryan Heitz, L., Grimberg, F., Grieder, H., & Maurer, M. (2023). A cyberattack simulation for teaching cybersecurity. *EPiC Series in Computing, 93,* 129–140. https://doi.org/10.29007/dkdw

Schmidt, T., & Nøhr, C. (2023). Perceptions of learning activities in electronic health record transition. In M. Hägglund, M. Blusi, S. Bonacina, L. Nilsson, I. C. Madsen, S. Pelayo, A. Moen, A. Benis, L. Lindsköld, P. Gallos (Eds.), *Caring is sharing - Exploiting the value in data for health and innovation* (pp. 448–452). IOS Press. https://doi.org/10.3233/SHTI230170

Shah, P., & Agarwal, A. (2023). Cyber Suraksha: a card game for smartphone security awareness. *Information and Computer Security*, *31*(5), 576–600 https://doi.org/10.1108/ICS-05-2022-0087

Sharif, K. H., & Ameen, S. Y. (2020, December). A review of security awareness approaches with special emphasis on gamification. *Proceedings of the International Conference on Advanced Science and Engineering, Duhok, Iraq*, 151–156. https://doi.org/10.1109/ICOASE51841.2020.9436595

Siddaway, A. P., Wood, A. M., & Hedges, L. V. (2019). How to do a systematic review: A best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. *Annual Review of Psychology, 70*, 747–770. https://doi.org/10.1146/annurev-psych-010418-102803

Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing human phishing difficulty: A Phish Scale. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa009

Sweller, J., Ayres, P., & Kalyuga, S. (2011). *Cognitive load theory*. Springer. https://doi.org/10.1007/978-1-4419-8126-4

Thomopoulos, G. A., Lyras, D. P., & Fidas, C. A. (2024). A systematic review and research challenges on phishing cyberattacks from an electroencephalography and gaze-based perspective. *Personal and Ubiquitous Computing*, *28*, 449–470 https://doi.org/10.1007/s00779-024-01794-9

Tran, T. M., Beuran, R., & Hasegawa, S. (2023). Gamification-based cybersecurity awareness course for self-regulated learning. *International Journal of Information and Education Technology*, *13*(4), 724–730. https://doi.org/10.18178/ijiet.2023.13.4.1859

Triplett, W. J. (2023). Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability*, *3*(1), 47–67.

Tsou, H. T., & Putra, M. T. (2023). How gamification elements benefit brand love: The moderating effect of immersion. *Marketing Intelligence and Planning*, *41*(7), 1015–1036. https://doi.org/10.1108/MIP-04-2023-0143

Uzun, B., & Tekinerdogan, B. (2018). Model-driven architecture based testing: A systematic literature review. *Information and Software Technology*, *102*, 30–48. https://doi.org/10.1016/j.infsof.2018.05.004

Valencia, K., Rusu, C., Quiñones, D., & Jamet, E. (2019). The impact of technology on people with autism spectrum disorder: A systematic literature review. *Sensors*, *19*(20), 4485. https://doi.org/10.3390/s19204485

van Roy, R., & Zaman, B. (2017). Why gamification fails in education and how to make it successful: Introducing nine gamification heuristics based on self-determination theory. In M. Ma & A. Oikonomou (Eds.), *Serious games and edutainment applications* (pp. 485–509). Springer. https://doi.org/10.1007/978-3-319-51645-5_22

Welbers, K., Konijn, E. A., Burgers, C., de Vaate, A. B., Eden, A., & Brugman, B. C. (2019). Gamification as a tool for engaging student learning: A field experiment with a gamified app. *E-Learning and Digital Media*, *16*(2), 92–109. https://doi.org/10.1177/2042753018818342

Werbach, K., & Hunter, D. (2020). *For the win: The power of gamification and game thinking in business, education, government, and social impact*. Wharton School Press. https://doi.org/10.9783/9781613631041

Wu, T., Tien, K.-Y., Hsu, W.-C., & Wen, F.-H. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. *Applied Sciences*, *11*(19), 9266. https://doi.org/10.3390/app11199266

Xu, X. Y., Tayyab, S. M. U., Jia, Q. D., & Wu, K. (2023). Exploring the gamification affordances in online shopping with the heterogeneity examination through REBUS-PLS. *Journal of Theoretical and Applied Electronic Commerce Research*, *18*(1), 289–310. https://doi.org/10.3390/jtaer18010016

Yakubov, A., Nazarov, Y., & Rodionov, A. A. (2024, June). Advancing e-learning and m-learning environments incorporating AI and gamification to boost learner motivation. *Proceedings of the 4th International Conference on Technology Enhanced Learning in Higher Education, Lipetsk, Russian Federation*, 29–31. https://doi.org/10.1109/TELE62556.2024.10605689

Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., & Russello, G. (2023). SoK: Human-centered phishing susceptibility. *ACM Transactions on Privacy and Security*, *26*(3), Article 24. https://doi.org/10.1145/3575797

Zichermann, G., & Cunningham, C. (2011). *Gamification by design: Implementing game mechanics in web and mobile apps*. O'Reilly Media.

## AUTHORS

**Kevin Gwenhure** is a PhD candidate in Computer Engineering at the Sirindhorn International Institute of Technology (SIIT), Thammasat University (TU), Thailand. He has a Master's degree from the Universitas Atma Jaya Yogyakarta (UAJY), Indonesia. His research interests include gameful design approaches, information security, and cybersecurity, with a bias toward human-centric and behavioral cybersecurity. His current research focuses on addressing the weakest link in the cyber chain – the user – through the use of gamification.

**Dr SangGyu Nam** is a lecturer in the School of Information, Computer, and Communication Technology (ICT) at the Sirindhorn International Institute of Technology (SIIT), Thammasat University (TU), Thailand. He received his PhD from the Japan Advanced Institute of Science and Technology (JAIST), Japan. His research interests include procedural content generation, entertaining games, gamification, human-like artificial intelligence, and reinforcement learning. He is particularly interested in enhancing player experience by designing games that are more entertaining, interactive, and emotionally engaging.