International Journal of Serious Games

ISSN: 2384-8766
https://journal.seriousgamessociety.org/

Article

Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review

Anderson Kevin Gwenhure[1], and Flourensia Sapty Rahayu[2]

[1]Departmen of Informatics, Universitas Atma Jaya Yogyakarta, Yogyakarta, Indonesia; [2]Department of Informatics, Universitas Atma Jaya Yogyakarta, Yogyakarta, Indonesia
{kevingwenhuree} @gmail.com; {sapty.rahayu} @uajy.ac.id.

Keywords:

Cybersecurity
Cybersecurity awareness
Gamification
Game elements
non-IT Professionals

Received: December 2023
Accepted: March 2024
Published: March 2024
DOI: 10.17083/ijsg.v11i1.719

Abstract

This literature review delves into research on the gamification of cybersecurity awareness for non-IT professionals, aiming to provide an accurate report on known and unknown information regarding three key questions: the impact of gamification on cybersecurity awareness interest and engagement, measurable results related to game elements and their connection to specific learning goals, and the long-term effectiveness of gamified cybersecurity. Examining five relevant papers, the findings confirm short-term effectiveness and indicate that the incorporation of various game elements, such as storytelling, team leaderboards, and interactive scenarios, results in increased knowledge, improved engagement, and positive behavior changes aligned with specific cybersecurity awareness learning goals. However, the review also identifies recurring gaps in evaluating individual game elements and customizing gamification strategies for non-IT professionals. Highlighting a critical gap in understanding long-term effectiveness, we argue for further empirical studies to consider habituation effects, emphasizing the need for a nuanced understanding of gamification's impact on cybersecurity awareness over an extended period. Thus, the review contributes to the existing body of knowledge by emphasizing the necessity for empirical studies focusing on sustained, long-term effectiveness and habituation effects in gamified cybersecurity initiatives.

1. Introduction

In the rapidly evolving digital age characterized by swift technological advancements [1], the internet has fundamentally transformed how businesses and individuals connect with one another, compelling both to adapt [2]. About 4.9 billion people utilize the internet globally as of 2023, accounting for 62.5 percent of the world's population [3]. This interconnected world offers enhanced communication and productivity, but also significantly heightened the risk of attacks [4], [5], [6], posing threats to the confidentiality, integrity, and availability of an organization’s digital assets [7]. These cybersecurity threats manifest in various forms, from sophisticated cyberattacks and covert data breaches, and can range from minor disruptions to

major incidents like ransomware, impacting entire organizations [8]. This is substantiated by the growing number of daily reports on cyberespionage, cybercrimes, and data breaches which underscore the rising vulnerability of organizations and government agencies, leading to compromised sensitive information [9]. As an imperative, cybersecurity emerges as a crucial safeguard [5], [10], [11], necessitating a combination of diverse knowledge, skills, and tailored strategies to counter threats like unauthorized access, disruptions, and data breaches [9], [12], [13]. Consequently, the demand for competent cybersecurity professionals is on the rise [8]. However, there is a persistent shortage of cybersecurity across sectors [14], which make it essential to broaden the reach of cybersecurity awareness and educate a wider audience to effectively address the evolving landscape of cyber threats [8].

Threats within organizations can be traced to malicious insiders and naive or negligent insiders [9]. The user's capacity to identify, refrain from compromising actions, evaluate, and lessen risks [15], thereby promoting responsible actions in the cyber realm [16], is the essence of what cybersecurity awareness entails. [17] emphasizes that cybersecurity awareness entails recognizing users' vulnerabilities and instructing them on identifying and preventing cyberattacks. At its core, cybersecurity awareness recognizes the human element as both a valuable defense and a significant vulnerability [18], as studies reveal that users often constitute the weakest link and root cause of cyber threats [6], [16], [18], [19], [20], mainly due to their lack of cyber awareness and underestimation of risks in routine online activities, exposing themselves and organizations to cyber threats [12]. Navigating cyberspace, these users unwittingly face a constant risk of unintentional actions exploited in targeted attacks. For instance, while navigating cyberspace, a user can unwittingly face a constant risk of unintentional actions exploited in targeted attacks, such as phishing attacks, which can circumvent even the most sophisticated cybersecurity defenses, potentially resulting in devastating organization breaches, emphasizing the need for robust cybersecurity awareness [1], [21]. Cybersecurity awareness serves as countermeasures to minimize user-related cybersecurity incidents [19]. Informed and vigilant users are better equipped to make informed security decisions, effectively preventing, or mitigating cyber risks [1], [9], [19], [22], making it is crucial to instill this awareness early on to alter users' behavior and responses when faced with cyberattacks [16].

However, in practice, organizations either neglect to implement cybersecurity awareness programs or employ unsustainable methods [23]. Those who do implement awareness initiatives often rely on conventional approaches like paper-based, computer-based, and web-based training, as well as presentations, videos, notes, and emails [6], [17], [19]. Unfortunately, these methods are predominantly theoretical, lacking effectiveness in enabling users to identify and respond to cyber threats, ultimately failing to alter employee behavior [16], instead leading users to feel bored, overwhelmed, and uninterested [13], [22]. In some cases, some users resist cybersecurity awareness, seeing it as an extra burden beyond their tasks and viewing security as solely the Information Technology (IT) department's responsibility rather than a shared concern within the organization [24]. The perception of cybersecurity as overly complex and purely technical further hinders user engagement [2]. All this point to the fact that traditional cybersecurity awareness methods have limited success in engaging and motivating end users to adopt recommended cybersecurity measures, leading to low success rates [19], [20], [25], evident in the frequency of cyberattacks linked to user behavior [24]. According to [15], successful cybersecurity awareness programs require users to reach three essential states: perception (understanding cybersecurity's importance), comprehension (deep understanding of its significance and personal relevance), and projection (influencing behavior and ensuring adherence to security rules post-awareness). [15] argues that users need motivation to learn and act, meaning reducing cyber-attacks requires motivating users to be aware of best practices [16], yet lack of motivation is arguably one of the primary limitations of traditional cybersecurity awareness programs. In addition, traditional awareness programs face criticism

for their inflexible, repetitive content and their lack of adaptation to the dynamic cybersecurity landscape. The process of raising awareness about cybersecurity necessitates constant assessment and modification to handle new risks and difficulties [23].

Recognizing the limitations of traditional cybersecurity methods and their disconnect with the dynamic nature of cybersecurity awareness has prompted the exploration of more innovative and engaging training strategies, such as gamification, which influences early-stage behavior change, placing a strong emphasis on motivation [15], [16]. Gamification integrates game elements and mechanics into real-world settings [8], [12], [26]. It is a versatile strategy applicable across diverse non-game contexts and learning environments, whether digital or non-digital, aiming to gamify content partially or fully and enhance the learning experience [27]. In this context, "non-game" refers to using game design elements beyond their original entertainment purpose [27]. These game elements, fundamental features in most games, play a pivotal role in shaping the overall gaming experience. Borrowed from games used in various educational processes [27], [28], these game elements effectively address limitations often associated with traditional training, education, and awareness programs, mitigating challenges related to low engagement and lack of intrinsic motivation. It's crucial to understand that gamification goes beyond introducing game elements; it represents user-centered approach prioritizing human motivation to enhance engagement, motivation, and information retention [24].

Ongoing research supports the advantages of using gamification as an educational method [5], [29]. Gamification provides learners with motivation, mental relaxation, and habit reinforcement through the integration of game-like elements and interactive activities [12], [16]. Game elements offer visible indicators of learners' efforts, motivating progress in their learning journey [12]. This motivation aligns with the Self-Determination Theory (SDT) theory, which examines how people's well-being and motivation are influenced by their environment and individual differences. SDT identifies two main types of motivation: autonomous (from within) and controlled (external or pressured). This theory predicts how motivation impacts learning, performance, experiences, and mental health. It emphasizes autonomy, competence, and relatedness as fundamental needs for optimal learning performance [28], [30]. Learners' motivation can be intrinsic, driven by a desire for knowledge growth or intellectual expansion, or extrinsic, fueled by recognition from peers, rewards for overcoming challenges, or points earned for progress [12]. The strategic use of game elements enables learners to witness a genuine increase of their knowledge and intellect, nurturing intrinsic motivation. Suggesting learners are motivated when they have a clear understanding of their position, acquired abilities, feedback on development, achievements, and a sense of community [12]. Gamification fosters a positive learning perspective, providing an enjoyable experience, intrinsic motivation, and the potential for achieving a state of flow, promoting the development of deeper knowledge structures [27], [28]. It offers a dynamic, feedback-driven approach, enabling real-time assessment of learner performance and encouraging continuous engagement and improvement [28], while meeting the need for continuous cybersecurity awareness.

Gamification, effectively employed in cyber awareness training [28], [29], in contrast to traditional cybersecurity methods perceived as dull and lacking engagement, introduces an element of fun and interactivity to the learning process, rendering it more captivating and enjoyable for participants [31]. Thus, when executed correctly, it creates a playful environment and promotes active participation and healthy competition [20], ultimately fostering a cybersecurity awareness culture and improving the overall training experience [28]. It also serves as a sandbox for individuals to experiment and explore in a risk-free setting, empowering learners to confront challenges, make security decisions [16], and engage in trial and error, learning from mistakes before facing assessments or real-world situations [6]. This iterative process accelerates the acquisition of knowledge, experience, and skills [16]. However, it's crucial to note that although gamification has garnered significant popularity in both academia

and industry over the past decade [16], [26], it is complex [5] and its improper application and design can lead to a lack of intrinsic motivation, causing frustration, dissatisfaction, stress, resistance, and decreased motivation [26].

Although gamification has gained significant popularity in academia and industry over the past decade [16], [26], its application in cybersecurity awareness reveals notable gaps. One gap is the absence of a well-established theoretical framework tailored to incorporating game design elements into cybersecurity awareness programs [26]. This underscores the critical need for a comprehensive theoretical foundation to effectively leverage game design elements for promoting cybersecurity awareness. Creating an engaging activity goes beyond adding game elements [28]; there is a need for evidence-based recommendations on which game design elements should be implemented for effective cybersecurity awareness programs, which is currently lacking [26]. While various gamification elements with a high level of interactivity have been used to motivate participants [32], their connection to achieving specific learning goals in cybersecurity awareness programs remains unclear. Evidence-based recommendations are lacking, and the evaluation of each game elements is often vague or treated holistically, highlighting the need for further research to establish a robust link between applied game elements and learning outcomes in cybersecurity awareness [26], [33]. Evaluation is crucial, as inappropriate gamification elements can lead to adverse consequences, such as anxiety or inappropriate behavior [26].

Although existing literature suggests that gamification boosts engagement, these findings are largely confined to the short term, highlighting a significant absence of evidence supporting medium and long-term effectiveness [33]. While initial engagement may be satisfactory in the short term, habituation, a psychological phenomenon characterized by decreased responsiveness to a repeated stimulus over time, suggests that users may become less responsive to stimulation with repeated exposure [34]. This process involves individuals becoming accustomed to a particular stimulus, leading to a reduced reaction. This, in turn, allows the brain to conserve mental resources and attention for novel or significant stimuli. The diminishing reaction typically follows a pattern where the decrease is more pronounced initially but lessens as one is exposed to the stimulus more frequently [35]. As gamification aims to stimulate participation and learning through game elements [36], it's crucial to recognize the potential for habituation. Therefore, to gauge the sustained effectiveness of gamification in ensuring continuous engagement in cybersecurity awareness initiatives, an essential question arises: Does gamification maintain prolonged engagement in learning about cybersecurity, or does it succumb to habituation, similar to the traditional cybersecurity awareness approaches it aims to improve upon? Sustaining participant engagement in the long term through gamification is critical, especially in the context of continuous cybersecurity awareness, as it is an ongoing concern.

Prior literature has examined gamification in cybersecurity awareness interventions across various participant groups, but without specifically targeting individuals based on educational and professional backgrounds. However, this approach becomes a limitation when trying to understand whether gamification enhances learning about cybersecurity awareness, particularly for those who typically find it dull. Bias may arise from participants already interested in IT-related fields, such as IT professionals and students, skewing results. To address this, our survey focuses exclusively on non-IT professionals and students—individuals not primarily involved in IT-related work or studies.

Our proposed separation is justified by two psychological theories: the Self-Determination Theory [30] and the Expectancy-Value Theory. The Expectancy-Value Theory posits that individuals' decisions regarding achievement are influenced by their expectations for success and the subjective value they attach to specific tasks or activities within particular domains. Essentially, people are more likely to engage in an activity or pursue a goal if they believe in their potential for success and find the activity valuable or important [37]. According to SDT,

people are driven by three basic psychological needs: relatedness, competence, and autonomy [30]. IT professionals and students may feel more motivated to study cybersecurity awareness because it aligns with their sense of competence and autonomy, being relevant to their skill set and essential for their professional growth. The Expectancy-Value Theory emphasizes the significance of perceived competence and the value attached to knowledge [37]. IT professionals may possess higher intrinsic motivation for cybersecurity awareness tasks due to their expertise, while non-IT professionals may start with lower expectancy of success, impacting their motivation. The perceived value of cybersecurity awareness may already be high among IT professionals, but not necessarily for non-IT professionals. To evaluate gamification's effectiveness in engaging non-IT professionals in cybersecurity awareness, it's crucial to separate these groups. This enables tailored strategies to address distinct motivational factors, ensuring interventions meet the specific needs of each group. By doing so, awareness campaigns can be precisely calibrated to increase motivation and participation in cybersecurity awareness within each demographic.

This systematic literature review (SLR) aims to address knowledge gaps in gamification in cybersecurity awareness. The article structure includes the research methodology, data analysis, and results. A discussion of findings and acknowledgment of study limitations follow. The conclusion summarizes key insights and suggests directions for future research in gamification for cybersecurity awareness.

2. Methodology

In order to determine how the gamification strategy has been applied in cybersecurity awareness initiatives, particularly for non-IT professionals, we adopted a systematic review methodology by [38], [39] in this article. A SLR is an independent academic method that aims to identify and evaluate all relevant literature on a topic to derive conclusions about the question under consideration. A SLR is a rigorous academic methodology employed to systematically identify, collect, evaluate, and interpret all relevant literature on a specific topic, with the goal of deriving comprehensive conclusions about the question or questions under consideration [40], [41], [42]. It uses a clear, methodical approach to formulate the question, identify applicable research, evaluate its quality, and synthesize results, either qualitatively or quantitatively [43]. A SLR, however, never offers "solutions." SLR only provide an accurate report of the information that is known and unknown regarding the review's questions [44]. A SLR adheres to a set of core principles; thus, it follows a systematic and organized method designed to address specific questions, it transparently states the method used in the review, it allows for replication, modification, or updating by other researchers, and lastly it organizes and summarizes results in a structured manner [40], [44]. A SLR is divided into three main phases, according to [40]: Planning the Review, which entails formulating research questions, creating search queries and selecting studies based on inclusion and exclusion criteria (Figure 1), and Conducting the Review, which involves selecting studies; and Reporting the Review, which deals with data extraction and answering research questions. A thorough rundown of the major procedures in each phase is given in the sections that follow.

2.1 Planning the Review

We began by clearly defining the primary objective of this systematic literature review and defining the following research questions (RQ) in light of the gaps in the literature that we discovered:

1. Does gamification make learning about cybersecurity awareness more interesting?
2. What measurable results do gamified elements in cybersecurity awareness initiatives achieve, and how do these relate to specific learning goals in cybersecurity awareness?

3. Do gamified cybersecurity awareness initiatives keep people engaged continuously in learning about cybersecurity in the long run?

Next, we created a list of keywords, which include non-IT professionals, cybersecurity awareness, and gamification. These keywords served as specific terms or phrases during the literature search process [45], playing a crucial role in identifying and collecting relevant studies that contribute to a comprehensive understanding of the review topic [42]. Then, as authors may use different terminology to refer to the same concept, we ascertained the other terms for each of the keywords. Next, in order to locate the relevant studies, we identified the fundamental strings to employ in an automated search across electronic data sources. The database source that we used is the Scopus database. The literature released between 2020 and 2023 was included in the search results. The literature included in the Scopus database was searched using the strings in the article title, abstract, and keywords sections. Ninety-one papers were found as an outcome of this first search phase. The search string is used as follows:

(TITLE-ABS-KEY ("gamification") OR TITLE-ABS-KEY ("gamif*") OR TITLE-ABS-KEY ("gamified") OR TI-TLE-ABS-KEY ("game elements") OR TITLE-ABS-KEY ("game mechanics ") OR TITLE-ABS-KEY ("game com-ponents") OR TITLE-ABS-KEY ("game dynamics") OR TITLE-ABS-KEY ("game aesthetics") AND TITLE-ABS-KEY ("Cybersecurity Awareness") OR TITLE-ABS-KEY ("Security Awareness Training") OR TITLE-ABS-KEY ("Security Awareness Programs") OR TITLE-ABS-KEY ("Security Awareness") OR TITLE-ABS-KEY ("Information Security Awareness") OR TITLE-ABS-KEY ("Phishing Awareness") OR TITLE-ABS-KEY ("Data Privacy Education") OR TITLE-ABS-KEY ("Security Literacy") OR TITLE-ABS-KEY ("Cyber Threat Awareness") OR TITLE-ABS-KEY ("In-ternet Security Education") OR TITLE-ABS-KEY ("Cybersecurity Education") OR TITLE-ABS-KEY ("Safe Online Practices")) AND PUBYEAR > 2019 AND PUBYEAR < 2024

2.2 Conducting the Review

To ensure precision and relevance, stringent criteria were applied when selecting studies for research on gamification in cybersecurity awareness. Studies published between 2020 and 2023 were included to capture recent advancements, while those before 2020 were excluded. Only studies with abstracts were considered, facilitating quick evaluation of alignment with study objectives. Full-text access was required for comprehensive review, excluding studies lacking this availability. Criteria for inclusion were strictly defined, focusing solely on gamification in cybersecurity awareness. Papers referring to gamification as game-based learning, serious games, games, or video games were excluded to maintain a focused exploration of cybersecurity awareness through gamification. Only studies directly addressing gamification interventions in cybersecurity awareness were included, while those aimed at technical skill enhancement were excluded. Participant criteria targeted non-IT professionals, excluding IT professionals and students in IT-related fields. Empirical research types were prioritized, omitting non-empirical studies for a more evidence-based approach. Only English-language papers were included to streamline the review process. These criteria ensured a targeted and thorough evaluation of relevant literature in gamification for cybersecurity awareness.

2.2.1 Results of the Search

The most comprehensive summary of empirical research on the gamification of cybersecurity awareness for non-IT workers is presented in this literature review. Figure 1 illustrates the process of selecting relevant studies, where 'n' represents the number of research papers. The applied exclusion criteria are as follows:

- Exclusion 1: Papers lacking a full abstract and full accessibility were excluded, reducing the number to 88.
- Exclusion 2: Papers with similar limitations were further excluded, resulting in a count of 82.
- Exclusion 3: Papers unrelated to the study's focus, specifically those using gamification to refer to game-based learning, serious games, games, and video games, were eliminated, reducing the count to 69.
- Exclusion 4: Non-empirical studies, including opinions, reviews, and theoretical/conceptual articles, were removed, further reducing the count to 52.
- Exclusion 5: Articles whose research participants included IT-related professionals and students were excluded since the review focused on cybersecurity awareness for non-IT personnel, resulting in a reduction to 29.
- Exclusion 6: Articles not solely focused on gamification in cybersecurity awareness, emphasizing training professionals within the cybersecurity domain to enhance skills, were eliminated, reducing the number to 14.
- Additional Exclusion: Nine papers were further eliminated based on relevance to the study, resulting in a final set of 5 papers.

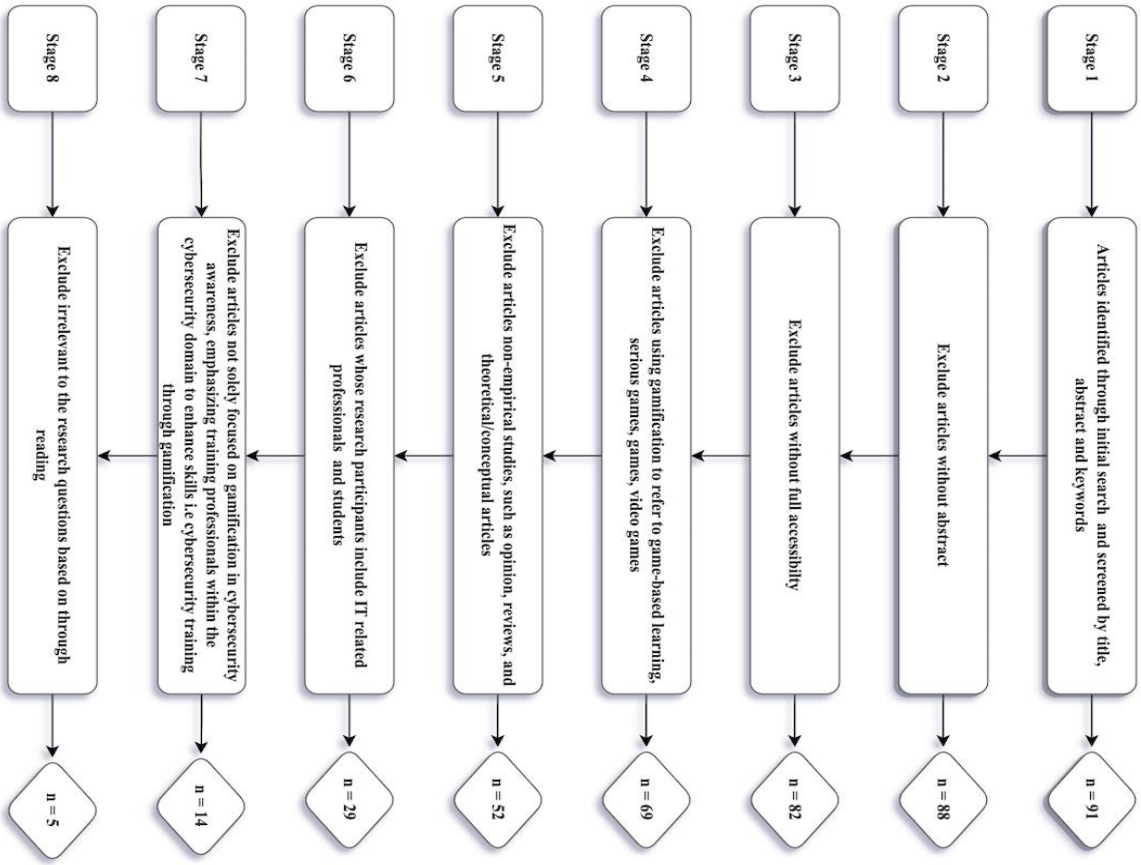

Figure 1. Process flow diagram for selecting articles.

2.3 Data Extraction

We created a data extraction form and employed it to retrieve data from every research that was included. To systematically investigate our research questions, we specifically considered empirical papers, such as case studies or experiments, aiming to document the game elements employed and their collective impact on enhancing engagement, paying attention only to papers that targeted non-IT related individuals. Furthermore, we looked for identifiable results

achieved through gamified elements to explore their connection with specific learning goals in cybersecurity awareness. Additionally, we collected data on the reported duration of engagement in gamified cybersecurity awareness initiatives to understand sustained involvement over an extended period. This comprehensive approach allowed us to extract relevant insights from prior literature and address our research questions systematically. Table 1 displays the data summaries from the five papers.

Table 1. Selected studies on the use of Gamification in Cybersecurity Awareness for Non-IT Professionals

Year	Citation	Aim	Target	Game Elements
2021	[6]	Improve employees' cybersecurity awareness.	Employees that are non-IT professionals	Feedback, Scenarios, Levels, Points, Avatars
2021	[16]	Verify the effectiveness of gamification in cybersecurity awareness and training.	High School Students	Points, Timers, Narration, Avatars
2022	[44]	To gamify the phishing security awareness training process.	Employees	Points, Competition, Alerts, Feedback
2023	[45]	To evaluate how well story-driven gamification works to shield students against USB-based threats.	University Students	Story, Narrative, Avatar
2023	[26]	To enhance information security awareness by increasing user motivation and reducing learning barriers.	University Students	Narrative, Team leaderboards (TL)

3. Results

The organization of the data analysis and results section is in line with the research questions presented at the outset of this paper.

RQ1 Does gamification make learning about cybersecurity awareness more interesting?

To answer the above question, this review explored the impact of gamification on cybersecurity awareness, specifically targeting non-IT professionals and students to avoid bias as highlighted in the introduction. The findings from multiple studies consistently indicate that gamification makes learning about cybersecurity awareness more interesting, especially for individuals who might find traditional training methods boring. In the study by [26], [46], which specifically targeted non-IT professionals and students, the integration of game-design elements like narration and leaderboards in learning management systems significantly correlated with increased information security awareness. Thus, the use of these elements was found to effectively enhance cybersecurity awareness. Similarly, [46] demonstrated that story-driven gamified education on Universal Serial Bus (USB) based attack prevention, with engaging story elements, was perceived as effective in increasing participants' awareness of cybersecurity. The incorporation of narrative elements and effective story design contributed to the success of conveying cybersecurity awareness concepts and making the learning experience more interesting. It's worth noting that this study focused on master's and bachelor's students aged 18 to 25 from European and North American countries with diverse academic backgrounds.

Furthermore, [6] conducted a study involving general employees from different institutions in Abu Dhabi City, using a gamified approach Cyber Shield Game. The results showed an average improvement of 51.4% in security awareness, suggesting that gamification actively engaged employees and contributed to increased security awareness. Study [47] emphasized the positive impact of gamification in phishing awareness exercises, particularly with the Phish Derby. Participants enjoyed the gamified experience, highlighting that the focus on positive

reporting behaviors, competition, and rewards enhanced engagement and interest in cybersecurity awareness training. Lastly, the study by [16], targeting students ranging from 9 to 22 years old, observed positive outcomes in enhancing cybersecurity awareness, specifically in password selection, through gamification. Despite not presenting detailed pre-test and post-test results, the study indicated a 5% improvement in selecting stronger passwords over a two-month period.

In conclusion, the cumulative evidence from these studies strongly suggests that gamification is a valuable strategy for enhancing cybersecurity awareness, making the learning experience more engaging and interesting, especially for individuals who may find traditional methods less appealing.

RQ 2 What measurable results do game elements in cybersecurity awareness initiatives achieve, and how do these relate to specific learning goals in cybersecurity awareness?

To address the question, we synthesized measurable outcomes associated with the incorporation of gamification elements in cybersecurity awareness initiatives, drawing from the reviewed papers. Measurable outcomes are tangible and quantifiable results or changes that can be observed, assessed, or recorded, providing a clear indication of the impact or effectiveness of a particular intervention, program, or strategy. These outcomes were organized based on common themes identified in the findings from the reviewed papers.

According to [26], the utilization of gamified elements such as storytelling and team leaderboards in cybersecurity awareness Security programs, demonstrated positive effects. Students participating in these programs exhibited enhanced cybersecurity understanding and awareness when exposed to the combination of storytelling and team leader boards within a Learning Management System. The incorporation of these gamification elements effectively addressed personal motivation and educational success factors, leading to increased engagement and enjoyment among students. Despite limitations, such as a relatively small survey size, the study suggests that employing storytelling and team leaderboards in a Learning Management System can positively impact cybersecurity awareness.

Similarly, [46] focused on gamification elements, including a story-driven framework based on Thorndyke's structure, and found that they successfully increased participants' knowledge of USB-based attacks. High engagement was noted, attributed to the narrative structure, trial format, and realistic elements. Participants expressed a preference for gamification over traditional methods, emphasizing its effectiveness in surpassing traditional approaches. The study concluded that participants had a positive experience, with engaging story elements, successful knowledge transfer, and challenges contributing to overall enjoyment. Comparisons with other gamified training underscored the effectiveness of the story-driven approach in engaging users and enhancing cybersecurity awareness.

A study conducted by [6] investigated the effectiveness of the Cyber Shield Game (CSG), an interactive video game designed to boost cybersecurity awareness among organizational employees. The game, featuring four levels, addresses various cybersecurity threats such as password complexity, social engineering, phishing attacks, and physical security. Employing gamified elements like feedback, scenarios, levels, and points, the authors reported a substantial 51.4% improvement in employees' cybersecurity knowledge. This improvement was calculated based on pre-game and post-game surveys, indicating increased awareness post-engagement. Player feedback highlighted the superior interactivity of CSG compared to traditional methods, emphasizing active participation in diverse game scenarios. The game effectively targeted specific learning goals across its levels, achieving notable progress in areas like password complexity, phishing attacks, and social engineering. Quantifiable improvements in survey scores validated the effectiveness of game elements in enhancing cybersecurity

knowledge and promoting positive changes in employee behavior. Noteworthy improvements were observed in several areas. Regarding password complexity, employees transitioned from using passwords containing personal information to more secure practices. Additionally, a positive shift towards adopting multi-factor authentication was noted. In the handling of confidential documents, a decrease in using email for sensitive information and an increase in the preference for in-person document delivery were observed. Overall, the Cyber Shield Game significantly enhanced employees' security awareness across the four threat categories, with password complexity and phishing attacks standing out as key areas of improvement.

Positive behavior changes, as a measurable outcome associated with game elements, are supported by the studies of [16] and [47]. In their study, [47] explored the impact of gamification elements, including Points, Competition, Alerts, and Feedback, in the Phish Derby experiment. The Phish Derby experiment involved gamifying phishing security awareness training to understand employees' reporting behaviors regarding phishing emails. Participants competed in a month-long competition where they were instructed to report suspicious emails as potential phishing attacks. They earned points and money based on the number of attacks they successfully reported and the speed at which they issued alerts. Difficult simulated phishing attacks were used to increase variance in user responses. The findings revealed measurable results significantly influencing participants' behavior, with the competition format leading to a marked increase in phishing alert rates and fostering a heightened sense of awareness and engagement. The study emphasized the importance of prompt responses to potential threats, and the success of the Phish Derby highlighted the potential of gamification elements as an effective strategy in increasing awareness of phishing threats.

Similarly, [16] demonstrated measurable results in their gamification of cybersecurity awareness training, utilizing Cyber-Hero. The Cyber-Hero framework was employed for information security awareness and training targeted towards high school students. It aimed to improve cybersecurity skills and capabilities by utilizing gamification as a methodology to change behavior concerning the selection of passwords, thereby addressing human error in cybersecurity. The framework incorporated game elements such as points, timers, and narration. The meticulous process of progress monitoring and evaluation within the gamification framework allowed continuous measurement of users' information security skills and capabilities. The pre-test and post-test results indicated an improvement in participant's password selection, achieving a 5% enhancement over a two-month period, suggesting that gamified approaches, specifically utilizing narrative instructions, could effectively influence and enhance behavior.

In summary, gamified elements consistently yield measurable results, such as increased knowledge, improved engagement, and behavior changes, effectively aligning with specific learning goals in cybersecurity. These include enhanced cybersecurity understanding and awareness [6], [26], demonstrated by improved phishing threat recognition [47] and positive changes in employee behavior related to cybersecurity practices [6], as evidenced by improved password selection [16].

RQ 3 Do gamified cybersecurity awareness initiatives keep people engaged continuously in learning about cybersecurity in the long run?

The empirical findings from the studies offer insights into short-term engagement in gamified cybersecurity awareness initiatives, suggesting positive outcomes within relatively brief periods. For instance, in the study by [26], the focus on a semester duration of three months indicates positive outcomes and sustained engagement during that timeframe. Similarly, the study by [6] reports interactive engagement and increased awareness levels among participants, but the results are within a short period, indicating short-term effectiveness. However, the studies do not provide direct empirical evidence or insights into the long-term sustainability of

engagement beyond the immediate learning experience. The study by [46] emphasizes the positive impact on knowledge acquisition and the overall positive experience with story-driven gamification but does not explicitly address long-term engagement. The same is true for the studies by [16], [47] where positive outcomes and improvements are observed, but the duration of the experiments is relatively short (one month and two months, respectively).

4. Discussions

Few studies on the gamification of cybersecurity awareness for non-IT professionals were found through this systematic review. Research on gamifying cybersecurity awareness has gained momentum in recent years, as seen by the rise in research articles and systematic reviews of research articles. The following subsections highlight the current state of gamification techniques for raising cybersecurity awareness among non-IT professionals.

4.1 Gamification in Cybersecurity Awareness:

The findings from the reviewed studies collectively support the idea that incorporating gamification into cybersecurity awareness is a valuable strategy. This suggests that a gamified approach can enhance participants' learning experiences, especially for those who may not be as engaged with traditional methods. The use of gamification elements like storytelling, team leaderboards, and interactive game scenarios serves as motivators or feedback to encourage participation and acknowledge individuals' efforts [48], [49]. This positive impact of gamification is evidenced by demonstrated outcomes related to specific cybersecurity learning goals, including increased knowledge, improved engagement, and positive behavioral changes. However, the positive influence of gamification in cybersecurity awareness, as observed across all the studies, tends to be more prominent in the short term, such as within a few months.

4.2 Empirical Gaps and Trends in Gamified Cybersecurity Awareness

In general, the cumulative evidence from these studies strongly suggests that gamification is a valuable strategy for enhancing cybersecurity awareness, making the learning experience more engaging and interesting, especially for individuals who may find traditional methods less appealing. Several shortcomings can be identified with five major limitations:

First, we noted from RQ1 in our systematic literature analysis that most of these studies primarily used qualitative assessments instead of quantitative pre- and post-surveys.. Qualitative assessment is a constructivist and interpretivist approach that involves exploring phenomena through non-numeric, verbalistic methods without measuring their extent in numerical terms [50]. While qualitative insights are valuable, the interpretation of non-numeric data, such as text, interviews, or observations, can be influenced by the researcher's personal perspectives and biases, leading to variations in the interpretation of data among different researchers, affecting the reliability and consistency of the findings compared to quantitative approaches [50]. Quantitative assessment is an objective, scientific approach grounded in positivism, relying on numerical data to establish causal relationships, emphasizing measurement, and often resulting in clearer and more easily evaluated outcomes [50]. The advantage of quantitative assessment is its objective and standardized nature, minimizing variations in data interpretation among researchers, enhancing reliability, enabling measurement of actual improvement magnitude, and providing a robust foundation for informed conclusions and recommendations. As a result, the use of quantitative approaches for evaluation has become more prevailing [51]. Hence, utilizing quantitative assessment ensures a comprehensive and objective evaluation of gamification’s impact on cybersecurity awareness, allowing researchers to measure actual improvement magnitude and draw informed conclusions and recommendations.

Secondly, the limitation of lack of proper assessment from RQ1 also extends to results of RQ2 regarding the lack of assessment outcomes tied to individual game elements. All the studies reviewed consistently present outcomes associated with combinations of two or more gaming elements, creating a challenge in discerning the unique influence of each element. This deficiency in granularity obstructs a precise understanding of the effectiveness of individual game elements, a crucial factor for guiding future design and implementation strategies in refining gamification approaches for enhanced cybersecurity awareness initiatives. The significance of this lies in the recognition that appropriate game elements can significantly boost user motivation, while inappropriate ones have the potential to demotivate users [52], [53]. Hence, for gamification designers to achieve effectiveness, it is crucial that they possess an understanding of the potential outcomes of specific game elements within a given scenario and for a particular audience [33]. As such, it becomes essential to carefully choose a set of game elements that precisely match the intended results. In order to do this, a methodical investigation of the effects of each game element independently is required [54]. Therefore, extensive research is necessary to improve our comprehension of the precise relationships between particular game elements and motivational and behavioral results. This understanding is vital for identifying the distinct contributions of each element in cases that incorporate multiple game elements, as observed in the reviewed literature [54].

Thirdly, findings related to RQ3, reveal that the field remains concentrated on short-term insights ranging for a few months, lacking a comprehensive understanding of the enduring effects of gamification, as underscored by [33]. While these studies contribute valuable insights into short-term engagement dynamics, they do not sufficiently address the critical question of whether gamified cybersecurity awareness initiatives can sustain continuous engagement over the medium to long term.

Moreover, despite an initial pool of 91 papers, only 5 were both empirical and specifically targeted toward non-IT professionals in the realm of gamified cybersecurity awareness. This highlights a notable scarcity of empirical studies, and more specifically, a lack of research focusing on the niche non-IT professional and students' audience. The fourth limitation, the dearth of empirical studies, hampers the ability to draw robust conclusions based on concrete data and real-world scenarios. Conceptual studies provide valuable insights, but their arguments are not based on primary data; instead, they involve combining and assimilating evidence from previously developed concepts, assumptions, and theories [55]. This means that while conceptual papers do contain factual observations, they also rely upon created hypotheses and notions that have not yet been tested and can only be tested through empirical study [56]. Empirical research involves gathering data from experience, observations, or experiments, relying on factual experience rather than theoretical assumptions [57]. Its distinctiveness lies in the rigorous collection and observation of data and experiences, providing tangible evidence that enhances the credibility of findings. This emphasis on concrete evidence makes it essential for testing and establishing the effectiveness and practical implications of gamification in cybersecurity awareness initiatives.

The scarcity of empirical studies exclusively targeting non-IT professionals and students highlights a crucial gap in understanding the dynamics of gamified cybersecurity awareness in this specific context. Considering non-IT professionals alongside technical IT professionals might introduce biased outcomes due to their distinct characteristics, needs, and motivations. The self-determination theory posits that individuals have different psychological needs, including autonomy, competence, and relatedness [30]. Non-IT professionals may have distinct motivations and expectations compared to their IT counterparts, as highlighted by the expectancy theory, which emphasizes the importance of individual expectations in shaping behavior [37]. Recognizing that non-IT professionals constitute a significant portion of the user base exposed to cybersecurity threats, the scarcity of tailored empirical research for this demographic hampers the development of targeted and effective gamification strategies. [58]

argued against assuming homogeneous characteristics among learners and highlighted the importance of considering individual needs. Thus, personalized training is advantageous, considering the diverse preferences, styles, and abilities of learners [59]. In this regard, tailored empirical studies for non-IT professionals and students not only enrich gamification outcomes but also align with the idea of personalizing training to meet individual needs [60].

5. Conclusions

With a focus on non-IT professionals and students, we conducted a SLR to explore the use of gamification in cybersecurity awareness initiatives. A systematic review aims to provide an accurate report of both known and unknown information regarding the review's questions. In our case the review questions were, what's the impact of gamification on cybersecurity awareness interest and engagement; what measurable results are related to game elements in relation to particular learning goals; and the long-term impact of gamified cybersecurity. To answer these questions, we examined a total of five relevant papers.

Regarding the impact of gamification on cybersecurity awareness interest, engagement, and measurable results related to game elements in relation to particular learning goals, reviewed studies consistently affirm that gamification effectively enhances cybersecurity awareness. This is achieved by making the learning experience engaging, particularly for those who may find traditional methods less appealing. The incorporation of various game elements, such as storytelling, team leaderboards, and interactive scenarios, results in increased knowledge, improved engagement, and positive behavior changes aligned with specific cybersecurity awareness learning goals. However, a notable gap in cybersecurity awareness gamification initiatives persists as none of the reviewed papers provided insights into the efficacy of each game element independently, despite prior recommendations emphasizing this crucial aspect.

Another significant observation is that, despite prior recommendations urging tailoring of gamification initiatives to individual needs and recognizing differences among learners, most cybersecurity gamification initiatives persist in adopting a one-size-fits-all approach. Out of 91 papers reviewed, only 5 demonstrated efforts to customize their strategies for non-IT professionals. This neglect of customization for a demographic identified as the weakest link in cybersecurity is concerning, emphasizing the need for more focused and personalized approaches. This observation underscores a critical disparity between established recommendations and actual implementation in the field.

Regarding the long-term impact of gamified cybersecurity awareness, while short-term effectiveness is affirmed by reviewed papers, sustained long-term effectiveness remains unknown. Short-term effectiveness does not reliably indicate long-term effectiveness due to habituation, where individuals become accustomed to a stimulus over time, resulting in diminished responsiveness. Initial positive responses and engagement may occur during short-term assessments, but as users become habituated to gamified elements, the impact may wane. Therefore, relying solely on short-term results can be misleading. Practitioners should conduct long-term empirical studies to understand sustained effectiveness, considering potential habituation effects and providing a comprehensive assessment of their impact on cybersecurity awareness over time.

Lastly, while established recommendations emphasize the significance of empirical studies to assess gamification effectiveness, most literature on gamifying cybersecurity awareness remains theoretical or conceptual. This suggests a misalignment with best practices among practitioners. Factors such as ignorance, time constraints, resource limitations, or lack of awareness about evaluation necessity contribute to this dearth of empirical studies. The gap between recognized best practices and practical implementation indicates a disconnect between theoretical knowledge and real-world application. To bridge this gap, practitioners should

prioritize staying informed, allocate resources for empirical studies, and acknowledge evidence's value in refining initiatives.

Acknowledgments

We thank the Department of Informatics, Universitas Atma Jaya Yogyakarta for their support in this research.

Conflicts of interest

The authors declare no conflict of interest.

References

[1] C. Croucamp, G. R. Drevin, and D. Snyman, "Promoting Cybersecurity Awareness Utilizing a 'Build Your Own Adventure' Serious game.," in International Conference on Applied Computing 2022 and WWW/Internet 2022, Lisbon, Portugal, Nov. 2022.

[2] C. Balakrishna and P. Charlton, "Using Game-based Learning Methods to Demystify Cyber Security Concepts for Adult Learners," in Proceedings of the 16th European Conference on Games Based Learning, 2022. doi: https://doi.org/10.34190/ecgbl.16.1.804.

[3] K. Wang et al., "Effects of Digital Game-Based Learning on Students' Cyber Wellness Literacy, Learning Motivations, and Engagement," Sustainability (Switzerland), vol. 15, no. 7, Apr. 2023, doi: https://doi.org/10.3390/su15075716.

[4] K. Hussein Sharif and S. Yousif Ameen, "A Intelligent Security Power Lab (SPL): The Ultimate Serious Game Training in Cybersecurity," Original Research Paper International Journal of Intelligent Systems and Applications in Engineering IJISAE, vol. ISSN:2147-6799, no. 11s, pp. 245–259, 2023, [Online]. Available: www.ijisae.org

[5] Thombre Sneha and Makarand Velankar Makarand, "Gamification by Students: An effective approach to cyber security concept learning," Journal of Engineering Education Transformations, vol. Volume No 36, no. 2394–1707, pp. 1–9, 2022, doi: https://doi.org/10.16920/jeet/2022/v36is1/22178.

[6] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, "A novel SETA-based gamification framework to raise cybersecurity awareness," International Journal of Information Technology (Singapore), vol. 13, no. 6, pp. 2371–2380, Dec. 2021, doi: https://doi.org/10.1007/s41870-021-00760-5.

[7] I. Ortiz-Garces, R. Gutierrez, D. Guerra, S. Sanchez-Viteri, and W. Villegas-Ch, "Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions," Electronics (Switzerland), vol. 12, no. 7, Apr. 2023, doi: https://doi.org/10.3390/electronics12071753.

[8] M. Christensen, D. Britze, J. Vejlin, L. T. Sorensen, and J. M. Pedersen, "The Privacy Universe - A game-based learning platform for data protection, privacy and ethics," in IEEE Global Engineering Education Conference, EDUCON, IEEE Computer Society, 2023. doi: https://doi.org/10.1109/EDUCON54358.2023.10125160.

[9] J. Harding, D. Snyman, and G. R. Drevin, "Establishing Cybersecurity Awareness of Technical Security Measures Through a Serious Game.," in International Conferences on Applied Computing 2022 and WWW/Internet 2022, 2022.

[10] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, and S. Furnell, "Evaluation of Contextual and Game-Based Training for Phishing Detection," Future Internet, vol. 14, no. 4, Apr. 2022, doi: https://doi.org/10.3390/fi14040104.

[11] J. C. Paiva, R. Queirós, and T. Gasiba, "Sifu Reloaded: An Open-Source Gamified Web-Based CyberSecurity Awareness Platform," in OpenAccess Series in Informatics, Schloss Dagstuhl-Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing, Aug. 2023. doi: 10.4230/OASIcs.ICPEC.2023.5.

[12] T. M. Tran, R. Beuran, and S. Hasegawa, "Gamification-Based Cybersecurity Awareness Course for Self-regulated Learning," International Journal of Information and Education Technology, vol. 13, no. 4, pp. 724–730, Apr. 2023, doi: https://doi.org/10.18178/ijiet.2023.13.4.1859.

[13] R. Hodhod, H. Hardage, S. Abbas, and E. A. Aldakheel, "CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness," Electronics (Switzerland), vol. 12, no. 17, Sep. 2023, doi: https://doi.org/10.3390/electronics12173544.

[14] M. Jelo and P. Helebrandt, "Gamification of cyber ranges in cybersecurity education," in 20th Anniversary of IEEE International Conference on Emerging eLearning Technologies and Applications, ICETA 2022 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 280–285. doi: https://doi.org/10.1109/ICETA57911.2022.9974714.

[15] E. G. B. Gjertsen, E. A. Gjære, M. Bartnes, and W. R. Flores, "Gamification of information security awareness and training," in ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy, SciTePress, 2017, pp. 59–70. doi: https://doi.org/10.5220/0006128500590070.

[16] H. Qusa and J. Tarazi, "Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students," in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 677–682. doi: https://doi.org/10.1109/CCWC51732.2021.9375847.

[17] H. Alqahtani and M. Kavakli-Thorne, "Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)," Information (Switzerland), vol. 11, no. 2, Feb. 2020, doi: https://doi.org/10.3390/info11020121.

[18] Y. Petrykina, H. Schwartz-Chassidim, and E. Toch, "Nudging users towards online safety using gamified environments," Comput Secur, vol. 108, Sep. 2021, doi: https://doi.org/10.1016/j.cose.2021.102270.

[19] P. Shah and A. Agarwal, "Cyber Suraksha: a card game for smartphone security awareness," Information and Computer Security, 2023, doi: https://doi.org/10.1108/ICS-05-2022-0087.

[20] C. Brady and A. M'manga, "Gamification of Cyber Security Training-EnsureSecure," in 2022 IEEE International Conference on e-Business Engineering (ICEBE), Bournemouth, United Kingdom: IEEE, Sep. 2022. doi: https://doi.org/10.1109/ICEBE55470.2022.00010.

[21] R. C. T. Panga, J. Marwa, and J. D. Ndibwile, "A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania," Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 466–489, Jun. 2022, doi: https://doi.org/10.3390/jcp2030024.

[22] C. Scherb, L. Bryan Heitz, F. Grimberg, H. Grieder, and M. Maurer, "EPiC Series in Computing A Cyberattack Simulation for Teaching Cybersecurity," in Proceedings of Society 5.0 Conference 2023, 2023, pp. 1–12. [Online]. Available: https://www.ubisoft.com/en-us/game/watch-dogs/watch-dogs

[23] Scholl Margit, "Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect January 3-6, 2023," 56th Hawaii International Conference on System Sciences (HICCS), Hyatt Regency Maui, , pp. 1–10, 2023.

[24] C. Decusatis, E. Alvarico, and O. Dirahoui, "Gamification of cybersecurity training," in Gamify 2022 - Proceedings of the 1st International Workshop on Gamification of Software Development, Verification, and Validation, co-located with ESEC/FSE 2022, Association for Computing Machinery, Inc, Nov. 2022, pp. 10–13. doi: https://doi.org/10.1145/3548771.3561409.

[25] K. H. Sharif and S. Y. Ameen, "A Review of Security Awareness Approaches with Special Emphasis on Gamification," in 3rd International Conference on Advanced Science and Engineering, ICOASE 2020, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 151–156. doi: https://doi.org/10.1109/ICOASE51841.2020.9436595.

[26] Brehmer Martin, "Gamifying a Learning Management System: Narrative and Team Leaderboard in the Context of Effective Information Security EducationJanuary 3-6, 2023," in Proceedings of the 56th Hawaii International Conference on System Sciences, University of Hawaii at Manoa, 2023, pp. 1–10.

[27] S. Fischer and A. Barabasch, 5 Gamification. A Novel Didactical Approach for 21 st Century Learning. Verlag Barbara Budrich, 2020. Accessed: Nov. 25, 2023. [Online]. Available: https://www.jstor.org/stable/j.ctv18dvv1c.8

[28] S. A. Triantafyllou and C. K. Georgiadis, “Gamification of MOOCs and Security Awareness in Corporate Training,” in International Conference on Computer Supported Education, CSEDU - Proceedings, Science and Technology Publications, Lda, 2022, pp. 547–555. doi: https://doi.org/10.5220/0011103000003182.

[29] J. C. Nwokeji, R. Matovu, and B. Rawal, “The Use of Gamification to Teach Cybersecurity Awareness in Information Systems,” 2020. [Online]. Available: https://aisel.aisnet.org/siged2020/29

[30] R. M. Ryan and E. L. Deci, “Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being Self-Determination Theory,” Department of Clinical and Social Sciences in Psychology, University of Rochester, Rochester, NY 14627, USA, pp. 1–11, 1985, doi: https://doi.org/10.1037//0003-066X.55.1.68.

[31] B. Fatokun Faith, Z. A. Long, S. Hamid, O. Fatokun Johnson, C. I. Eke, and A. Norman, “An Intelligent Gamification Tool to Boost Young Kids Cybersecurity Knowledge on FB Messenger,” in Proceedings of the 2022 16th International Conference on Ubiquitous Information Management and Communication, IMCOM 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: https://doi.org/10.1109/IMCOM53663.2022.9721733.

[32] T. D. Ashley, R. Kwon, S. N. G. Gourisetti, C. Katsis, C. A. Bonebrake, and P. A. Boyd, “Gamification of Cybersecurity for Workforce Development in Critical Infrastructure,” IEEE Access, vol. 10, pp. 112487–112501, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3216711.

[33] A. Antonaci, R. Klemke, and M. Specht, “The effects of gamification in online learning environments: A systematic literature review,” Informatics, vol. 6, no. 3, Aug. 2019, doi: https://doi.org/10.3390/informatics6030032.

[34] R. F. Thompson, “Habituation: A history,” Neurobiol Learn Mem, vol. 92, no. 2, pp. 127–134, Sep. 2009, doi: https://doi.org/10.1016/j.nlm.2008.07.011.

[35] C. H. Rankin et al., “Habituation revisited: An updated and revised description of the behavioral characteristics of habituation,” Neurobiol Learn Mem, vol. 92, no. 2, pp. 135–138, Sep. 2009, doi: https://doi.org/10.1016/j.nlm.2008.09.012.

[36] R. Smiderle, S. J. Rigo, L. B. Marques, J. A. Peçanha de Miranda Coelho, and P. A. Jaques, “The impact of gamification on students’ learning, engagement and behavior based on their personality traits,” Smart Learning Environments, vol. 7, no. 1, Dec. 2020, doi: https://doi.org/10.1186/s40561-019-0098-x.

[37] A. Wigfield and J. S. Eccles, “Expectancy-value theory of achievement motivation,” Contemp Educ Psychol, vol. 25, no. 1, pp. 68–81, 2000, doi: https://doi.org/10.1006/ceps.1999.1015.

[38] B. Ann Kitchenham, D. Budgen, and P. Brereton, Evidence-Based Software Engineering and Systematic Review. Accessed: Nov. 02, 2023. [Online]. Available: http://www.crcpress.com

[39] B. Kitchenham, “Guidelines for performing Systematic Literature Reviews in Software Engineering,” 2007. [Online]. Available: https://www.researchgate.net/publication/302924724

[40] B. Kitchenham, “Procedures for Performing Systematic Reviews,” Keele, Staffs, 2004.

[41] R. J. Piper, “How to write a systematic literature review: a guide for medical.” Accessed: Nov. 02, 2023. [Online]. Available: http: //sites.cardiff.ac.uk/curesmed/files/2014/10/NSAMR-Systematic-Review.pdf students

[42] A. Perttula, K. Kiili, A. Lindstedt, and P. Tuomi, “Flow experience in game based learning – a systematic literature review,” International Journal of Serious Games, vol. 4, no. 1, Mar. 2017, doi: https://doi.org/10.17083/ijsg.v4i1.151.

[43] R. Armstrong, B. J. Hall, J. Doyle, and E. Waters, “‘Scoping the scope’ of a cochrane review,” Journal of Public Health, vol. 33, no. 1. Oxford University Press, pp. 147–150, 2011. doi: https://doi.org/10.1093/pubmed/fdr015.

[44] R. B. Briner and D. Denyer, “Systematic Review and Evidence Synthesis as a Practice and Scholarship Tool,” in The Oxford Handbook of Evidence-Based Management, Oxford University Press, 2012. doi: https://doi.org/10.1093/oxfordhb/9780199763986.013.0007.

[45] vanDooren Marierose M.M, Visch Valentijn T., Spijkerman Renske, Goossens Richard H.M., and Hendriks Vincent M., “Personalization in Game Design for Healthcare: a Literature Review on its Definitions and Effects,” International Journal of Serious Games, vol. 1, no. 4, Oct. 2014, doi: https://doi.org/10.17083/ijsg.v1i4.47.

[46] V. Rikkers and D. K. Sarmah, "A story-driven gamified education on USB-based attack," J Comput High Educ, 2023, doi: https://doi.org/10.1007/s12528-023-09392-z.

[47] M. Canham, C. Posey, and M. Constantino, "Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks," Front Educ (Lausanne), vol. 6, Jan. 2022, doi: https://doi.org/10.3389/feduc.2021.807277.

[48] G. Barata, S. Gama, J. Jorge, and D. Gonçalves, "Studying student differentiation in gamified education: A long-term study," Comput Human Behav, vol. 71, pp. 550–585, Jun. 2017, doi: https://doi.org/10.1016/j.chb.2016.08.049.

[49] M. Sailer, J. U. Hense, S. K. Mayr, and H. Mandl, "How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction," Comput Human Behav, vol. 69, pp. 371–380, Apr. 2017, doi: https://doi.org/10.1016/j.chb.2016.12.033.

[50] N. Pilcher and M. Cortazzi, "'Qualitative' and 'quantitative' methods and approaches across subject fields: implications for research values, assumptions, and practices," Qual Quant, 2023, doi: https://doi.org/10.1007/s11135-023-01734-4.

[51] L. Yuan, J. Li, R. Li, X. Lu, and D. Wu, "Mapping the evaluation results between quantitative metrics and meta-synthesis from experts' judgements: evidence from the Supply Chain Management and Logistics journals ranking," Soft comput, vol. 24, no. 9, pp. 6227–6243, May 2020, doi: https://doi.org/10.1007/s00500-019-03837-3.

[52] S. Hallifax, A. Serna, J. C. Marty, G. Lavoué, and E. Lavoué, "Factors to consider for tailored gamification," in CHI PLAY 2019 - Proceedings of the Annual Symposium on Computer-Human Interaction in Play, Association for Computing Machinery, Inc, Oct. 2019, pp. 559–572. doi: https://doi.org/10.1145/3311350.3347167.

[53] S. Hallifax, A. Serna, J. C. Marty, and É. Lavoué, "Adaptive Gamification in Education: A Literature Review of Current Trends and Developments," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 2019, pp. 294–307. doi: https://doi.org/10.1007/978-3-030-29736-7_22.

[54] C. Dichev and D. Dicheva, "Gamifying education: what is known, what is believed and what remains uncertain: a critical review," International Journal of Educational Technology in Higher Education, vol. 14, no. 1. Springer Netherlands, Dec. 01, 2017. doi: https://doi.org/10.1186/s41239-017-0042-5.

[55] R. Hirschheim, "Some guidelines for the critical reviewing of conceptual papers," Journal of the Association for Information Systems, vol. 9, no. 8. Association for Information Systems, pp. 432–441, 2008. doi: https://doi.org/10.17705/1jais.00167.

[56] E. Jaakkola, "Designing conceptual articles: four approaches," AMS Review, vol. 10, no. 1–2, pp. 18–26, Jun. 2020, doi: https://doi.org/10.1007/s13162-020-00161-0.

[57] E. T. Njoku, "Empirical Research," in Encyclopedia of Psychology and Religion, D. A. Leeming, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 1–2. doi: https://doi.org/10.1007/978-3-642-27771-9_200051-1.

[58] Kamunya Samuel, Mirirti Evans, Oboko Robert, and Maina Elizaphan, "An Adaptive Gamification Model for E-Learning," in IST-Africa 2020 Conference Proceedings, 2022, pp. 1–10. doi: https://doi.org/10.23919/ISTAFRICA.2019.8764879.

[59] S. Schöbel and M. Söllner, "How to Gamify Information Systems-Adapting Gamification to Individual User Preferences," in European Conference on Information Systems, 2016, pp. 1–13. [Online]. Available: https://www.researchgate.net/publication/301820359

[60] V. Naik and V. Kamat, "Adaptive and Gamified Learning Environment (AGLE)," in Proceedings - IEEE 7th International Conference on Technology for Education, T4E 2015, Institute of Electrical and Electronics Engineers Inc., Jan. 2016, pp. 7–14. doi: https://doi.org/10.1109/T4E.2015.23.