INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 10, (2025) E-ISSN: 2222-6990

Cybersecurity Education Using Gamification: Systematic Literature Review

Tony Tan, Raihana Syahirah Abdullah, Zaki Mas'ud

[1]Department of Information System, Universitas Internasional Batam, Jl. Gajah Mada, Batam, 29426, Indonesia, [2,3]Fakulti Kecerdasan Buatan dan Keselamatan Komputer, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Melaka, 76100 Durian Tunggal, Malaysia

Email: tony@uib.ac.id

Corresponding Author Email: rasyahb@gmail.com

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v15-i10/26583

Published Date: 18 October 2025

Abstract

This systematic research investigates gamification in cybersecurity education, focusing on its effectiveness, implementation, and adoption. The study consolidates existing literature and concludes that the majority of cybersecurity gamification research emphasizes formal education, particularly at the university level, whereas business training and cybersecurity awareness remain inadequately addressed. In the study, gamification systems are categorized as web-based, application-based, or tabletop, each offering distinct advantages in accessibility and user engagement. Gamification has shown potential in enhancing cybersecurity awareness and training.

Keywords: Cybersecurity Education, Gamification, Systematic Review

Introduction

Cybersecurity knowledge is a vital component in developing a robust defensive plan against the rise of cyber-attacks(Erendor & Yildirim, 2022). As technology becomes more embedded in everyday life, people and businesses face an expanding range of threats(Shah et al., 2023). Awareness programs aim to educate users on identifying possible dangers, understanding security practices, and implementing proactive actions to safeguard sensitive information(Alyami et al., 2024). Such applications provide users with the information and skills necessary to serve as the first line of defense, therefore diminishing the probability of successful assaults that exploit human weaknesses, including social engineering approaches(Mendoza et al., 2023). However, the execution of effective cybersecurity awareness programs has significant hurdles(Alsobeh et al., 2023). A primary challenge is the material's intricacy, which may overwhelm listeners without technical understanding (Hulaj & Dreshaj, 2023). Traditional training methods sometimes fail to engage participants, leading to inadequate knowledge retention and restricted application of learned abilities (Ahmed et al., 2023). Moreover, developing systems that cater to the distinct requirements of various enterprises and their differing degrees of technical proficiency requires considerable

resource allocation and extensive customisation (Andreasson et al., 2024). Another problem is to address complacency or reluctance to change, since some personnel may see cybersecurity training as superfluous or monotonous(Alshammari & Eyadat, n.d.). To overcome these obstacles, organizations must invest in interactive, accessible, and engaging training methods that replicate real-world scenarios, thereby cultivating a culture of continuous learning and awareness of cyber threats(Ruoslahti et al., 2021).

Gamification represents an innovative strategy that integrates game-design elements into non-gaming contexts(Laine & Lindberg, 2020), such as education(Chen et al., 2023), with the objective of enhancing motivation(Shortt et al., 2023) and engagement(Kalogiannakis et al., 2021). By capitalizing on the psychological processes that contribute to the enjoyment of games, gamification strives to develop effective and engaging learning experiences(Sailer & Sailer, 2021). Notable characteristics include the provision of rewards, such as points, badges, leaderboards, and virtual goods(Rosmansyah et al., 2020), which offer immediate feedback and a sense of accomplishment(Suh et al., 2018). Thereby, appealing to both intrinsic and extrinsic motivations(Cheng et al., 2019). This approach encourages learners to remain engaged over time, motivating them to attain milestones and sustain their interest in the educational process(Behl et al., 2022; Hassan et al., 2021). Furthermore, gamification encourages collaboration and teamwork(Khaldi et al., 2023), which are essential skills in both educational and professional settings. The incorporation of multiplayer or team-based gamified activities has the potential to foster stronger interpersonal connections(Subhash & Cudney, 2018), enhance problem-solving abilities(Aparicio et al., 2019), and raise collective awareness(Garcia-Iruela & Hijon-Neira, 2020), which can be particularly advantageous in addressing social engineering challenges. Another noteworthy advantage of gamification is its capacity to facilitate personalized learning(Mazlan et al., 2023a). Adaptive game mechanics are designed to adjust the level of difficulty based on an individual's performance, ensuring that tasks remain appropriately challenging while providing feedback and progress tracking. However, despite these advantages, gamification also presents certain challenges(Morillas Barrio et al., 2016). An overemphasis on external rewards may potentially undermine intrinsic motivation, while poorly designed gamified elements may risk causing frustration and disengagement(Khodabandelou et al., 2023). For gamification to succeed, it requires a thoughtful design and execution that balances rewards, ensures fairness, and maintains focus on the educational value of the content(Torresan & Hinterhuber, 2023; Wanick & Bui, 2019). Gamification provides the benefit of presenting complex materials in an engaging manner(Kusuma et al., 2018). This study seeks to examine previous research on the use of gamification to enhance cybersecurity and to collect insights pertinent to future investigations**.**

Motivation

The growing importance of cybersecurity knowledge, as technology becomes increasingly integrated into everyday life, has led to a demand for effective awareness programs to educate users on threat identification and security practices. However, traditional training methods often fail to engage participants, resulting in inadequate knowledge retention. Gamification presents an innovative strategy to enhance motivation and engagement in cybersecurity education by incorporating game elements. Despite its potential benefits, gamification also presents challenges, such as the risk of undermining intrinsic motivation if poorly designed. This study aims to examine previous research on the use of gamification to

enhance cybersecurity education and gather insights relevant to future investigations. There is a need to systematically review the existing literature to understand the current state of gamification in cybersecurity education.

Contribution

The study conducts a comprehensive systematic review of 20 relevant papers on cybersecurity education through gamification, analyzing aspects such as objectives, methodologies, contexts, platforms, game elements employed, and the cybersecurity topics addressed. It elucidates the current focus areas, preferred platforms, and common gamification elements utilized in this domain. The review identifies key trends and gaps in the existing research, indicating that gamification in cybersecurity education predominantly targets formal higher education settings, with limited emphasis on employee training. The study also assesses the suitability of various gamification platforms (web-based, app-based, tabletop) for different implementation contexts. Furthermore, it categorizes cybersecurity topics into five principal groups to facilitate a systematic examination of this expansive field. The paper concludes by proposing research questions to guide future investigations in this area.

Metodhology

A comprehensive search was conducted using the Publish or Perish software program, which retrieves and analyzes academic citations. The program utilizes a variety of data sources to obtain the raw citations. The Scopus, Semantic Scholar, and Crossref databases were queried for the period between 2014 and 2024 to create a systematic review. To identify and gather raw material, the following keywords were searched: "Gamification", "Cybersecurity", "Education" and PRISMA protocol proposed by (Herman et al., 2024) was utilized to find relevant papers.

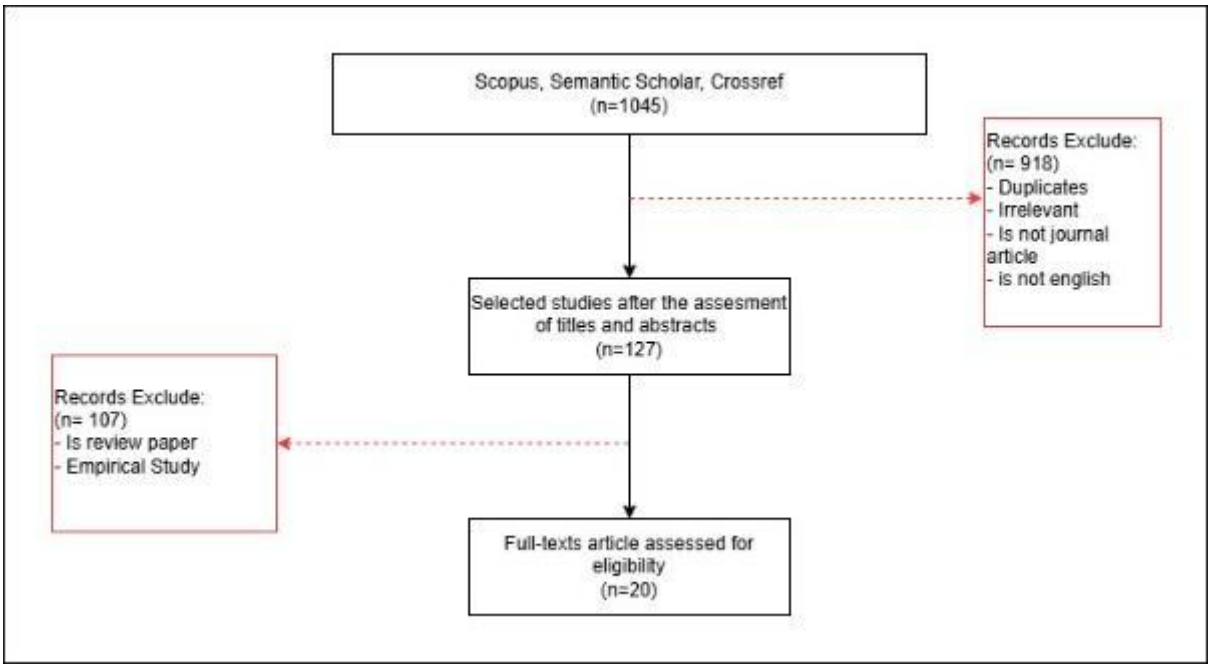

Fig. 1. PRISMA Flow Diagram

The performed search retrieved 1045 papers. During screening stage, the titles and abstracts were examined to eliminate irrelevant, duplicate, not journal article, not English, review paper, and empirical study. After screening, authors retreives 20 papers eligible.

Result

A comprehensive search was conducted using the Publish or Perish platform with Scopus, Semantic Scholar and Crossref Database, utilising established keywords. This yielded a total of 1045 publications. From the initial list, 918 items were removed due to various reasons, including duplication, non-compliance with the journal article format, and non-English language. A total of 127 articles underwent title and abstract assessment, with 107 exclusions due to their empirical or review-oriented nature. The final selection comprised 20 articles deemed suitable for the current objective. For table and indicator, Author use (Mazlan et al., 2023b) summary table, and adding one indicator from (Quayyum et al., 2021) for cybersecurity education topics.

Tabel 1
Summary Of Cybersecurity Education Using Gamification

Source	Objective	Methodology	Context	Platform	Game Element	Cybersecurity Education Topics	Conclusion
(Tobarra et al., 2021)	To develop a cloud-based game educational platform (CyberScratch) with a modular, flexible architecture that integrates gamification into the instructional process, while ensuring robust data privacy management compliant with GDPR, ISO/IEC standards, and Learning Analytics (LA) recommendations	Experimental (Development and Implementation)	Higher Education	Web-based	Points and Reward, Badges and Achievements, Narrative and Storytelling, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Privacy Awareness	CyberScratch successfully develops a modular, cloud-based gaming platform for cybersecurity teaching using gamification and lightweight container architecture.
(Haziq et al., 2021)	To introduce secondary school students to various cybersecurity topics and to inculcate their interest in cybersecurity	Multi Method (Experimental, Quantitative And Qualitative)	School	Virtual Lab	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback	Safety Protocols, Technical Risks, Non-technical Risks, Privacy Awareness	The scenario-based Capture the Flag (CTF) tournament engaged secondary school students in cybersecurit

Source	Objective	Methodology	Context	Platform	Game Element	Cybersecurity Education Topics	Conclusion
					and Progress Tracking, Narrative and Storytelling, Social Interaction		y in a competitive setting, sparking their enthusiasm.
(Jing et al., 2024)	To design and develop a cybersecurity skill training framework for teaching and learning (T&L) cybersecurity through a Capture the Flag (CTF) game	Experimental (Development and Implementation)	Higher Education	Apps-based	Points and Reward, Levels and Progression, Challenges and Quests, Feedback and Progress Tracking, Narrative and Storytelling, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Privacy Awareness,	The projected result is creating a revolutionary CTF-based cybersecurity teaching framework to greatly improve undergraduate cybersecurity knowledge and abilities
(Muhly et al., 2022)	Focus on observing and evaluating various aspects of participant engagement and the serious game (SG) approach in a business environment	Experimental (Development and Implementation)	Training	Tabletop	Levels and Progression, Challenges and Quests, Social Interaction	Cybersecurity Technology, Technical Risks, Non-technical Risks, Privacy Awareness	The research found that the SG technique may help create Social Engineering awareness and that iterative modifications based on participant input improve educational results.
(Karagiannis & Magkos, 2020)	To develop and maintain live exercises using Capture the Flag (CTF) challenges in a classroom setting for educational purposes	Multi Method (Experimental, Quantitative And Qualitative)	Higher Education	Virtual Lab	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Narrative and Storytelling, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-technical Risks, Privacy Awareness	The research found that CTF challenges boost student learning, engagement, and abilities, making them a viable cybersecurity instructional tool.

Source	Objective	Methodology	Context	Platform	Game Element	Cybersecurity Education Topics	Conclusion
(Ros et al., 2020)	To analyze students' self-perception of success and the effectiveness of learning in a gamified educational setting, particularly in the context of cybersecurity courses	Multi Method (Experimental, and Quantitative)	Higher Education	Web-based	Levels and Progression, Badges and Achievements, Challenges and Quests, Feedback and Progress Tracking, Narrative and Storytelling	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-technical Risks, Privacy Awareness	Gamification in education improves student engagement, learning, and achievement, according to the research.
(Abu-Amara et al., 2021)	To enhance employee awareness regarding cybersecurity threats through the development of an interactive video game	Multi Method (Experimental, and Quantitative)	Training	Web-based	Levels and Progression, Feedback and Progress Tracking, Narrative and Storytelling, Social Interaction	Cybersecurity Technology, Technical Risks, Non-technical Risks	Interactive and engaging training approaches promote cybersecurity awareness in enterprises.
(Paculanan et al., 2024)	To create awareness of the necessity of the importance and function of cyber security such as password security, phishing awareness, identity theft, encryption, and network security among others, to distinguish between	Multi Method (Experimental, and Quantitative)	School	Apps-bassed	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-technical Risks, Privacy Awareness	Cyberverse can educate cybersecurity basics and improve cognitive abilities via games.
(Srivatanakul, 2024)	To see how well escape room activities help students understand cybersecurity concepts, especially in web and software security and encourage teamwork and collaboration among students	Multi Method (Experimental, Quantitative And Qualitative)	Higher Education	Web-based	Levels and Progression, Challenges and Quests, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-technical Risks, Privacy Awareness	Cybersecurity is taught well via educational escape rooms. They simplify hard topics and interest students.

Source	Objective	Methodology	Context	Platform	Game Element	Cybersecurity Education Topics	Conclusion
(Abdul Razack & Mat Saad, 2024)	To enhance cybersecurity awareness among Multimedia University students through the design and implementation of an interactive, gamified learning platform	Experimental (Development and Implementation)	Higher Education	Web-based	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-technical Risks, Privacy Awareness	Multimedia University's gamified cybersecurity platform improves cybersecurity instruction. Interactive learning engages students and is economical.
(Jin et al., 2018)	To help high school students learn about cybersecurity, understand safe online behavior, and grow their interest in the field	Multi Method (Experimental, and Quantitative)	School	Apps-based	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-technical Risks	Students learned social engineering, internet safety, and cybersecurity from the games. This method encourages more students to consider cybersecurity education while choosing a major.
(Tran et al., 2023)	To design a cybersecurity awareness course that uses gamification to help students recognize cybersecurity threats and motivate them to learn more about information security on their own	Experimental (Development and Implementation)	Higher Education	LMS	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Social Interaction	Cybersecurity Technology, Technical Risks, Non-technical Risks	The approach might make cybersecurity teaching more engaging and successful, according to study.
(L. Williams et al., 2024)	To enhance students's understanding and mastery of crucial cybersecurity skills while also	Multi Method (Experimental, and Quantitative)	Higher Education	Web-based	Points and Reward, Levels and Progression, Badges and Achievements,	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-	When designed and developed according to pedagogical theories, CTF

Source	Objective	Methodology	Context	Platform	Game Element	Cybersecurity Education Topics	Conclusion
	igniting interest in cybersecurity among non-cybersecurity students				Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Narrative and Storytelling, Social Interaction	technical Risks, Privacy Awareness	events may improve student engagement, critical thinking, teamwork, problem-solving, and cybersecurity awareness.
(Moon et al., 2020)	A Game to train users in recognizing and preventing malware threats	Experimental (Development and Implementation)	School	App-based	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking	Cybersecurity Technology, Safety Protocols, Technical Risks	Emphasizes the importance of using educational games as effective tools for enhancing users's awareness and understanding of malware
(T. Williams et al., 2023)	To create a guided learning experience for students to interact with Cyber-Physical Systems (CPS), Industrial Control Systems (ICS), and IoT devices in practice environments	Experimental (Development and Implementation)	Higher Education	Web-based	Challenges and Quests, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-technical Risks, Privacy Awareness	Promotes adversarial thinking skills for critical infrastructure to prepare the next generation of cybersecurity experts.
(Abu-Amara et al., 2024)	To propose a low-cost cybersecurity awareness program aimed at training employees to follow their company's policies and procedures, improve their response to cyberattacks, and enhance their overall information security awareness level	Multi Method (Experimental, and Qualitative)	Training	Web-based	Points and Reward, Levels and Progression, Challenges and Quests, Feedback and Progress Tracking	Cybersecurity Technology, Technical Risks, Non-technical Risks, Privacy Awareness	Gamification boosts staff cybersecurity awareness. The program was more fun than standard training for employees.

Source	Objective	Methodology	Context	Platform	Game Element	Cybersecurity Education Topics	Conclusion
(Van Steen & Deeleman, 2021)	To investigate the effectiveness of an online serious game in enhancing participants' attitudes.	Multi Method (Experimental, and Quantitative)	Higher Education	App-based	Points and Reward, Levels and Progression, Challenges and Quests, Feedback and Progress Tracking, Narrative and Storytelling	Cybersecurity Technology, Safety Protocols, Technical Risks, Non-technical Risks, Privacy Awareness	Serious games may improve cybersecurity-related TPB variables.
(Kim et al., 2023)	To explore the process and impact of gamification on cybersecurity hands-on lab exercises.	Multi Method (Experimental, and Quantitative)	Higher Education	Virtual Lab	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Narrative and Storytelling	Cybersecurity Technology, Safety Protocols, Technical Risks	Gamified cybersecurity lab activities boosted student engagement, learning, and results.
(Alothman et al., 2023)	To enhance cybersecurity awareness through a gamification escape room methodology that educates users on both the basics and complexities of cybersecurity via interactive gameplay	Experimental (Development and Implementation)	Higher Education	Virtual Lab	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Social Interaction	Cybersecurity Technology, Safety Protocols, Technical Risks, Privacy Awareness	Promotes cybersecurity awareness via gamification escape rooms.
(Weanquoi et al., 2018)	To educate students about phishing attacks in a fun and engaging environment	Multi Method (Experimental, and Quantitative)	Higher Education	App-based	Points and Reward, Levels and Progression, Badges and Achievements, Leaderboards, Challenges and Quests, Feedback and Progress Tracking, Narrative and Storytelling	Safety Protocols, Technical Risks, Privacy Awareness	Playing the game helped most students comprehend phishing.

The existing research on the topic indicates that several insights may be derived from the aforementioned experiments. The use of gamification in cyber security education mostly emphasizes formal education, particularly at the tertiary level, with over fifty percent of the research conducted in higher education environments. The use of gamification in employee training remains somewhat restricted, prompting inquiries on the demography for whom the gamification of cybersecurity is most suitable. The current research asserts that kids are mostly influenced by Generation Z and Generation Alpha at this level. These kids engage with and assimilate the internet and its culture from a young age. It is anticipated that Generation Z and Generation Alpha possess a greater comprehension of the internet than of real-life scenarios, including cybersecurity. The workforce comprises people from several generations, with older generations being more acquainted with the digital lifestyle and its related concerns, including cyberattacks. In contrast, gamification is intended for those who get pleasure from a fun method of engaging with educational content. In this setting, younger generations are anticipated to exhibit greater ability. Consequently, owing to the extensive popularity of video games and the industry's development, early adopters of video games have attained a prominent place in the workforce. This acquaintance with gamification may promote its use in cybersecurity awareness training for workers. The scarcity of research about the use of gamification in cybersecurity awareness training is an interesting avenue for further investigation.

Further insight acquired from this study is the platform used for gamification. Prior research has classified platforms as either application-based or web-based, both with distinct advantages and disadvantages. App-based systems may operate without disruption from network connectivity problems; but, their performance is heavily reliant on the capabilities of the client's device. In contrast, web-based solutions provide universal accessibility and adaptability regarding device types. Nonetheless, their need on an operational server and network connection presents a considerable risk, since any interruption or failure may result in the total inaccessibility of the program. Previous research has shown a preference for online platforms because of their intrinsic durability and omnipresence. A notable characteristic is the tabletop platform, where the gamification process transpires without a computer, using cards and dice instead. This underscores the substantial influence of the platform on the implementation of gamification. In situations when consumers primarily possess a mobile or unstable connection, application-based solutions are more advantageous. Conversely, in instances when users are mostly sedentary, other platforms may be more suitable. In these instances, web-based systems are often the favored choice. Nonetheless, if users own devices capable of executing the gamification and maintain dependable connection, application-based systems with client-server data synchronization represent the superior option. The choice of a platform ultimately depends on the implementation circumstances. In educational institutions, such as schools or universities without immediate access to computers, web-based platforms are often the preferred choice. The ideal platform selection depends on the particular implementation circumstances. In situations when educational institutions offer computer laboratories and students may use internet-enabled devices, the optimal platform is the app-based choice. In business environments, the choice of a platform should be guided by considerations such as employee mobility, the functionality of office-provided devices, and the dependability of network connections.

Gamification may manifest in several ways, with points and rewards systems being one of the most direct and effective implementations. These systems often give prizes to users following the completion of certain activities, so enhancing user engagement and fostering a feeling of achievement. (Weanquoi et al., 2018) demonstrated the use of video games for teaching persons in recognizing phishing attempts, with job completion leading to point accumulation. (Haziq et al., 2021) similarly discovered that integrating prizes into cybersecurity education significantly enhanced user engagement. Besides points and incentives, gamification includes other crucial components that improve user experiences. The notions of levels and development, as shown by studies like (Van Steen & Deeleman, 2021), foster a feeling of achievement as users progress. Such accomplishments are often validated via the use of badges or other kinds of acknowledgment, as shown by the research done by (Al-Karaki et al., 2023) and (Paculanan et al., 2024). Additional gamification features augment user engagement by including competition, cooperation, and immersive experiences. Leaderboards serve as an efficient mechanism for incentivizing participants to surpass their competitors, especially within the framework of extended programs. The integration of social interaction, whether via competitive or cooperative play, sustains user interest by adding a dynamic, relational aspect to gamified activities. Moreover, challenges and quests provide structure and direction, therefore guaranteeing that users stay motivated to attain certain goals. Moreover, the delivery of feedback and progress monitoring is crucial, as it provides participants with direction and guidance as they engage with the program. Narrative and storytelling have become new techniques for greater immersion, allowing consumers to form an emotional connection with the information. The research by (Kim et al., 2023) and (L. Williams et al., 2024) demonstrates the effectiveness of narrative in enhancing engagement and memory retention in cybersecurity education settings. The appropriateness of gamification features depends on the goals of the gamification system. In the realm of awareness enhancement, time-constrained problem-solving activities, such as daily challenges and quests, are a favored gamification strategy. Incorporating gamification within an educational context, especially for assessments, may improve the learning experience via the use of badges, awards, and leaderboards. In a professional environment, due to the differing availability of workers, the incorporation of progress monitoring inside the gamification system is crucial.

The field of cybersecurity comprises a wide range of interrelated subjects, each with its own specialized emphasis and intrinsic difficulties. To enable a systematic examination of this vast domain, we have condensed the previously described aspects into five principal groups. The primary area is Cybersecurity Technology, which focuses on the latest advancements in hardware, software, and systems aimed at improving digital security. The second category pertains to Safety Protocol, which includes the established methods and rules necessary for addressing cyberattacks or managing security issues. These procedures include optimal practices for incident response, such as isolating compromised systems and preserving evidence, along with preventive strategies like routine system audits and penetration testing. The third category, Technical Risks, addresses the vulnerabilities and threats that capitalize on intrinsic deficiencies inside digital infrastructures. This includes the spread of harmful software, such as viruses, ransomware, and spyware, which may jeopardize systems and lead to substantial data breaches. To effectively mitigate these risks, it is essential to adopt a multifaceted strategy that encompasses the implementation of strong encryption, the introduction of efficient patch management protocols, and the establishment of a system for

ongoing network activity monitoring. The fourth category, Non-Technical Risks, pertains to the human dimensions of cybersecurity concerns. Social engineering attacks, such as phishing, pretexting, and fraudulent profiling, use psychological manipulation to mislead people into revealing sensitive information or providing unauthorized access. The need for a culture of alertness, bolstered by extensive training programs aimed at improving awareness and critical thinking among staff and users, is essential in addressing these risks. The fourth category, Privacy Awareness, is a crucial element of several cybersecurity instructional programs. In digital economies that depend on the monetization of personal data, it is essential to understand both the value and susceptibility of this information. Promoting privacy awareness fosters the use of security practices, such as using strong passwords, activating two-factor authentication, and meticulously reviewing permissions provided to programs.

Discussions

Gamification has been shown to offer a transformative approach to learning that significantly enhances both engagement and the retention of information. In contrast to more traditional learning methods, which often rely on passive absorption of material, gamification introduces interactive elements such as points, rewards and progress tracking, transforming learning into an active and enjoyable experience. The incorporation of game-based strategies within educational frameworks provides immediate feedback and recognition for achievements, thereby fostering a sense of confidence and reinforcing learning objectives. Furthermore, gamification aligns seamlessly with the learning styles of contemporary digital natives, who are well-accustomed to interactive technology and instantaneous gratification. The inherent competitive and collaborative features of many gamified platforms, such as leaderboards and group challenges, tap into innate human instincts, propelling learners to challenge their boundaries while fostering a sense of community and teamwork. This dynamic environment not only renders the educational process more engaging but also facilitates the retention of complex concepts, as learners are more likely to remember content that is associated with a positive and stimulating experience. Sceptics may argue that gamification might oversimplify educational content or distract from core learning objectives. This dynamic environment not only renders the educational process more engaging but also facilitates the retention of complex concepts, as learners are more likely to remember content that is associated with a positive and stimulating experience. Critics may argue that gamification might oversimplify educational content or distract from core learning objectives. However, when designed thoughtfully, gamified learning platforms can be structured to balance educational rigor with interactive play, ensuring that the fun elements serve as conduits to deeper understanding rather than mere entertainment. In light of the present age, which is characterised by the need for adaptability and innovation, gamification emerges as a potent instrument capable of redefining the learning experience. This redefinition renders the learning experience more responsive to the requirements of contemporary learners, thereby ensuring their effective preparation for a digitally driven future. Albeit major breakthroughs in adopting gamification as learning platform already achieved by previous studies, further application in certain learning demographics or specific implementation in industries should be pursued to gather a more holistic and comprehensive understanding while testing the limit of gamification utilization for the advancement of humanity and learning experience.

In the modern day, cybersecurity knowledge has transitioned from a discretionary luxury to a crucial and indispensable foundation, protecting people' personal digital identities and financial resources. A thorough comprehension and awareness of cybersecurity in society is essential for maintaining digital economic stability and prosperity.As technology grows more ubiquitous, the interchange and storage of extensive sensitive and personal data online has significantly heightened the potential danger of cyberattacks. Consequently, corporations and countries are dedicating resources to the development of sophisticated cybersecurity protocols and the recruitment of adept specialists to ensure data protection. The advancement of cybersecurity knowledge has become an essential element of any thorough cyber protection plan, acting as the foremost line of defense against cyber assaults. By educating users about potential threats like phishing scams and social engineering attacks, which remain common entry points for cybercriminals, organizations can enable their workforce to serve as an additional layer of defense, augmenting technological safeguards. Although the cost burden of deploying complete cybersecurity systems and training programs may be significant, especially for small organizations, it must be considered against the potentially catastrophic damages resulting from a single breach. In this context, such investments are not just reasonable but also essential. The rapid advancement of cyber dangers requires continuous education and adaptation; in the absence of cybersecurity knowledge, even the most advanced technology safeguards may be compromised by human mistake. The objective of gamification in cybersecurity is to make the learning process exceptionally entertaining, especially for certain groups. It has the capacity to enhance information acquisition for people with poor IT literacy, allowing them to converge with technologically skilled individuals. The efficacy, acceptability, and, most importantly, the sustainability of these systems need thorough investigation to determine their impact and ideal implementation.

Based on this Systematic Literature Review, the author identifies research questions for future investigation.

1. What is the long-term impact of gamification on cybersecurity behavior and knowledge retention in a corporate environment compared to traditional training methods?
2. How can adaptive gamification platforms be designed to personalize cybersecurity training for diverse generational and technical skill levels within a workforce?
3. Which specific combinations of gamification elements are most effective for teaching complex, non-technical cybersecurity risks like social engineering versus technical risks like malware identification?

Conclusion

Gamification is a new approach to cybersecurity education that effectively bridges the divide between traditional teaching techniques and the evolving digital landscape. While existing academic material mostly focuses on its use in formal educational environments, the potential for its use in business training and general cybersecurity awareness has yet to be thoroughly investigated. Selecting an optimal gamification platform is crucial, since web-based, application-based, and tabletop options each provide unique benefits regarding accessibility and particular user requirements. Moreover, essential gamification elements like as incentives, competitive leaderboards, narrative development, and motivating challenges augment engagement, foster motivation, and reinforce retention, thereby making cybersecurity training more effective. As cyber risks continue to evolve, gamification can

effectively educate people of all ages with the necessary skills to manage and mitigate online vulnerabilities. To establish gamification as a sustainable and widely used instrument in cybersecurity education, more study must examine its long-term efficacy, flexibility, and scalability across various learning and professional environments. By enhancing and expanding applications, gamification may serve as a powerful catalyst for cybersecurity awareness, promoting a more secure and digitally literate society.

References

Abdul Razack, A. K., & Mat Saad, M. F. (2024). Enhancing Cybersecurity Awareness through Gamification: Design an Interactive Cybersecurity Learning Platform for Multimedia University Students. *Journal of Informatics and Web Engineering*, *3*(3), 21–40. https://doi.org/10.33093/jiwe.2024.3.3.2

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 (Singapore)*, *13*(6), 2371–2380. https://doi.org/10.1007/s41870-021-00760-5

Abu-Amara, F., Hosani, R. Al, Tamimi, H. Al, & Hamdi, B. Al. (2024). Spreading cybersecurity awareness via gamification: zero-day game. *International Journal of Information Technology (Singapore)*, *16*(5), 2945–2953. https://doi.org/10.1007/s41870-024-01810-4

Ahmed, A. A., Elmi, A. H., Abdullahi, A., & Ahmed, A. Y. (2023). Cybersecurity awareness among university students in Mogadishu: a comparative study. *Indonesian Journal of Electrical Engineering and Computer Science*, *32*(3), 1580–1588. https://doi.org/10.11591/ijeecs.v32.i3.pp1580-1588

Al-Karaki, J. N., Itradat, A., & Mekonen, S. (2023). Immersive Cybersecurity Teaching/Training Using Gamification on the Metaverse: A Hands-On Case Study. In *2023 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Tec* (pp. 101–108). https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361297

Alothman, B., Al-Khulifa, K., Al-Shammari, R., Joumaa, C., & Khan, M. (2023). Towards Enhancing Cyber Security Awareness Using Gamification Escape Room. *International Conference on Ubiquitous and Future Networks, ICUFN*, *2023-July*, 828–830. https://doi.org/10.1109/ICUFN57995.2023.10199673

Alshammari, F. Z., & Eyadat, W. M. (n.d.). Social Media Users and Cybersecurity Awareness: An International Perspective. In *International Journal of Innovation, Creativity and Change. www.ijicc.net* (Vol. 16, Issue 1). www.ijicc.net

Alsobeh, A. M. R., Alazzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies*, *13*(2). https://doi.org/10.30935/ojcmt/12942

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2024). Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. *Information and Computer Security*, *32*(1), 53–73. https://doi.org/10.1108/ICS-08-2022-0133

Andreasson, A., Artman, H., Brynielsson, J., & Franke, U. (2024). Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval. *Cognition, Technology and Work*. https://doi.org/10.1007/s10111-024-00779-1

Aparicio, M., Oliveira, T., Bacao, F., & Painho, M. (2019). Gamification: A key determinant of massive open online course (MOOC) success. *Information and Management*, *56*(1), 39–54. https://doi.org/10.1016/j.im.2018.06.003

Behl, A., Jayawardena, N., Pereira, V., Islam, N., Giudice, M. Del, & Choudrie, J. (2022). Gamification and e-learning for young learners: A systematic literature review, bibliometric analysis, and future research agenda. *Technological Forecasting and Social Change*, *176*. https://doi.org/10.1016/j.techfore.2021.121445

Chen, C. M., Ming-Chaun, L., & Kuo, C. P. (2023). A game-based learning system based on octalysis gamification framework to promote employees' Japanese learning. *Computers and Education*, *205*. https://doi.org/10.1016/j.compedu.2023.104899

Cheng, V. W. S., Davenport, T., Johnson, D., Vella, K., & Hickie, I. B. (2019). Gamification in apps and technologies for improving mental health and well-being: Systematic review. *JMIR Mental Health*, *6*(6). https://doi.org/10.2196/13717

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity Awareness in Online Education: A Case Study Analysis. *IEEE Access*, *10*, 52319–52335. https://doi.org/10.1109/ACCESS.2022.3171829

Garcia-Iruela, M., & Hijon-Neira, R. (2020). What Perception Do Students Have about the Gamification Elements? *IEEE Access*, *8*, 134386–134392. https://doi.org/10.1109/ACCESS.2020.3011222

Hassan, M. A., Habiba, U., Majeed, F., & Shoaib, M. (2021). Adaptive gamification in e-learning based on students' learning styles. *Interactive Learning Environments*, *29*(4), 545–565. https://doi.org/10.1080/10494820.2019.1588745

Haziq, A., Hanafi, A., Rokman, H., Dahaqin Ibrahim, A., Ibrahim, Z.-A., Zawawi, N. A., & Rahim, F. A. (2021). A Scenario CTF-Based Approach in Cybersecurity Education for Secondary School Students 1. In *Journal of Computer Science and Information Technology (eJCSIT)* (Vol. 7, Issue 1).

Herman, H., Jaya Kumar, Y., Yong Wee, S., & Kumar Perhakaran, V. (2024). A Systematic Review on Deep Learning Model in Computer-aided Diagnosis for Anterior Cruciate Ligament Injury. *Current Medical Imaging Reviews*, *20*. https://doi.org/10.2174/0115734056295157240418043624

Hulaj, A., & Dreshaj, A. (2023). The impact of educational training on improving the vigilance of public officials against cyber-attacks. *Online Journal of Communication and Media Technologies*, *13*(4). https://doi.org/10.30935/ojcmt/13784

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Game based cybersecurity training for High School Students. *SIGCSE 2018 - Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, *2018-Janua*, 68–73. https://doi.org/10.1145/3159450.3159591

Jing, K. L., Yatim, M. H. M., & Seng, W. Y. (2024). A Preliminary Concept on Cybersecurity Skill Training Framework for a Capture-the-Flag Game using 5-Step Gamification Approach. *The International Journal of Multimedia & Its Applications*, *16*(4), 17–28. https://doi.org/10.5121/ijma.2024.16402

Kalogiannakis, M., Papadakis, S., & Zourmpakis, A. I. (2021). Gamification in science education. A systematic review of the literature. *Education Sciences*, *11*(1), 1–36. https://doi.org/10.3390/educsci11010022

Karagiannis, S., & Magkos, E. (2020). Adapting CTF challenges into virtual cybersecurity learning environments. *Information and Computer Security*, *29*(1), 105–132. https://doi.org/10.1108/ICS-04-2019-0050

Khaldi, A., Bouzidi, R., & Nader, F. (2023). Gamification of e-learning in higher education: a systematic literature review. In *Smart Learning Environments* (Vol. 10, Issue 1). Springer. https://doi.org/10.1186/s40561-023-00227-z

Khodabandelou, R., Roghanian, P., Gheysari, H., & Amoozegar, A. (2023). A systematic review of gamification in organizational learning. In *Learning Organization* (Vol. 30, Issue 2, pp. 251–272). Emerald Publishing. https://doi.org/10.1108/TLO-05-2022-0057

Kim, J. B., Zhong, C., & Liu, H. (2023). Teaching Tip: What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges. *Print) Journal of Information Systems Education*, *34*(4), 2023.

Kusuma, G. P., Wigati, E. K., Utomo, Y., & Putera Suryapranata, L. K. (2018). Analysis of Gamification Models in Education Using MDA Framework. *Procedia Computer Science*, *135*, 385–392. https://doi.org/10.1016/j.procs.2018.08.187

Laine, T. H., & Lindberg, R. S. N. (2020). Designing Engaging Games for Education: A Systematic Literature Review on Game Motivators and Design Principles. *IEEE Transactions on Learning Technologies*, *13*(4), 804–821. https://doi.org/10.1109/TLT.2020.3018503

Mazlan, A., Ahmad, I., & Salam, S. (2023a). A Systematic Literature Review in Gamification Implementation and Game Elements in Malaysia Education. *13th IEEE Symposium on Computer Applications and Industrial Electronics, ISCAIE 2023*, 25–31. https://doi.org/10.1109/ISCAIE57739.2023.10165134

Mazlan, A., Ahmad, I., & Salam, S. (2023b). A Systematic Literature Review in Gamification Implementation and Game Elements in Malaysia Education. *13th IEEE Symposium on Computer Applications and Industrial Electronics, ISCAIE 2023*, 25–31. https://doi.org/10.1109/ISCAIE57739.2023.10165134

Mendoza, A. L., Hernández, R. V. R., Quezada, M. T. P., & Hernández, R. S. (2023). Cybersecurity among University Students from Generation Z: A Comparative Study of the Undergraduate Programs in Administration and Public Accounting in two Mexican Universities. *TEM Journal*, *12*(1), 503–511. https://doi.org/10.18421/TEM121-60

Moon, T., Abegaz, T., Payne, B., & Salimi, A. (2020). MalAware Defensive: A Game to Train Users to Combat Malware. *Journal of Cybersecurity Education, Research and Practice*, *2020*(1). https://doi.org/10.62915/2472-2707.1065

Morillas Barrio, C., Munoz-Organero, M., & Sanchez Soriano, J. (2016). Can Gamification Improve the Benefits of Student Response Systems in Learning? An Experimental Study. *IEEE Transactions on Emerging Topics in Computing*, *4*(3), 429–438. https://doi.org/10.1109/TETC.2015.2497459

Muhly, F., Leo, P., & Caneppele, S. (2022). A Serious Game For Social Engineering Awareness Creation. In *Research and Practice Journal of Cybersecurity Education, Research and Practice* (Vol. 2022, Issue 1).

Paculanan, R. S., Tadeo, R. L., Caliliw, M. T., Atal, C. P., & Sadol, J. N. (2024). *Cyberverse: A Game-Based Learning Application for Cyber Security*. https://doi.org/10.51583/IJLTEMAS

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. In *International Journal of Child-Computer Interaction* (Vol. 30). Elsevier B.V. https://doi.org/10.1016/j.ijcci.2021.100343

Ros, S., Gonzalez, S., Robles, A., Tobarra, L. L., Caminero, A., & Cano, J. (2020). Analyzing Students' Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course. *IEEE Access*, *8*, 97718–97728. https://doi.org/10.1109/ACCESS.2020.2996361

Rosmansyah, Y., Isdiyanto, I., Hardi, A. B., & Putri, A. (2020). Using gamification for engaging surveyors: a case study in Statistics Indonesia. *Interactive Technology and Smart Education*, *17*(4), 377–391. https://doi.org/10.1108/ITSE-08-2019-0042

Ruoslahti, H., Coburn, J., Trent, A., & Tikanmäki, I. (2021). Cyber Skills Gaps – A Systematic Review of the Academic Literature. *Connections*, *20*(2), 33–45. https://doi.org/10.11610/Connections.20.2.04

Sailer, M., & Sailer, M. (2021). Gamification of in-class activities in flipped classroom lectures. *British Journal of Educational Technology*, *52*(1), 75–90. https://doi.org/10.1111/bjet.12948

Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance. *IEEE Access*, *11*, 87970–87984. https://doi.org/10.1109/ACCESS.2023.3296580

Shortt, M., Tilak, S., Kuznetcova, I., Martens, B., & Akinkuolie, B. (2023). Gamification in mobile-assisted language learning: a systematic review of Duolingo literature from public release of 2012 to early 2020. *Computer Assisted Language Learning*, *36*(3), 517–554. https://doi.org/10.1080/09588221.2021.1933540

Srivatanakul, T. (2024). Designing Cybersecurity Escape Rooms: A Gamified Approach to Designing Cybersecurity Escape Rooms: A Gamified Approach to Undergraduate Learning Undergraduate Learning Designing Cybersecurity Escape Rooms: A Gamified Approach to Undergraduate Learning. In *Research and Practice Journal of Cybersecurity Education*. https://digitalcommons.kennesaw.edu/jcerp

Subhash, S., & Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. *Computers in Human Behavior*, *87*, 192–206. https://doi.org/10.1016/j.chb.2018.05.028

Suh, A., Wagner, C., & Liu, L. (2018). Enhancing User Engagement through Gamification. *Journal of Computer Information Systems*, *58*(3), 204–213. https://doi.org/10.1080/08874417.2016.1229143

Tobarra, L., Utrilla, A., Robles-Gómez, A., Pastor-Vargas, R., & Hernández, R. (2021). A cloud game-based educative platform architecture: The cyberscratch project. *Applied Sciences (Switzerland)*, *11*(2), 1–22. https://doi.org/10.3390/app11020807

Torresan, S., & Hinterhuber, A. (2023). Continuous learning at work: the power of gamification. *Management Decision*, *61*(13), 386–412. https://doi.org/10.1108/MD-12-2020-1669

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

Van Steen, T., & Deeleman, J. R. A. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 593–598. https://doi.org/10.1089/cyber.2020.0526

Wanick, V., & Bui, H. (2019). Gamification in Management: analysis and research directions. *International Journal of Serious Games*, *6*(2), 57–74. https://doi.org/10.17083/ijsg.v6i2.282

Weanquoi, P., Johnson, J., & Zhang, J. (2018). Using a Game to Improve Phishing Awareness. *Journal of Cybersecurity Education, Research and Practice*, *2018*(2). https://doi.org/10.62915/2472-2707.1040

Williams, L., Anthi, E., & Javed, A. (2024). *Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students*. www.cisse.info

Williams, T., Fuhrmann, T., & Haney, M. (2023). *RADICL CTF: Low-Cost Capture the Flag Platform for Industrial Control Systems Education*. www.cisse.info