Fostering Cybersecurity Awareness and Learning Engagement Using Serious Games

Rahayu Ahmad [1,*] and Mohammed Mohammed-Ramzi [2]

[1] School of Computing, Universiti Utara Malaysia, Sintok, Kedah, Malaysia
[2] Information Technology Department, Tishk International University, Kurdistan Region, Iraq
Email: rahayu@uum.edu.my (R.A.); mohammed.nawzad@tiu.edu.iq (M.M.-R.)
*Corresponding author
Manuscript received October 10, 2025; revised November 20, 2025; accepted March 2, 2026; published August 18, 2026

***Abstract*—Serious games provide an effective approach to cybersecurity education by situating learners in interactive environments that support skill acquisition and knowledge retention. This study introduces SecureCyberQuest (SCQ), a theory-driven serious game designed to enhance cybersecurity awareness and learner engagement. The game design integrates principles from Cognitive Load Theory to structure-focused mini games targeting specific cybersecurity concepts, and Flow Theory to guide the progression of challenges and game mechanics. An experimental evaluation with 44 undergraduate students demonstrated improvements in cybersecurity awareness following gameplay. Additionally, perceived learning effectiveness, usability, and overall gameplay experience were positively associated with user engagement. These findings empirically support Flow Theory, indicating well-balanced challenges and game elements foster learners' competence and autonomy. The results further confirm the effective application of Cognitive Load Theory, as progressively increasing difficulty contributed to positive learning experiences and outcomes.**

***Keywords*—learning engagement, cognitive load theory, flow theory, serious games, cybersecurity**

I. Introduction

Cyberattacks pose significant risks to business continuity, data security, and personal identity integrity. Despite the urgency of these issues, there remains a gap in knowledge about effective cybersecurity strategies [1]. Cybersecurity is the practice of protecting computer systems, networks, and data from unauthorized access and attacks.

In today's digital landscape, cybersecurity is a crucial concern across all sectors. As cybercriminals continually advance their techniques to exploit vulnerabilities, the number of cyberattacks has increased significantly over the past decade [2]. One method to consider in enhancing cybersecurity skills is training through serious games. Serious games are a type of educational tool that use game-like elements to create an engaging and immersive learning experience. These games are designed to teach specific skills—in this case, cybersecurity skills. This is achieved by immersing users in simulated environments where they can practice and improve their abilities.

There are a number of studies that shed light on problems with the existing approaches of cybersecurity training. Bodea [3] highlighted the need for more effective pedagogical techniques. They argued that there is a discrepancy between the skill sets that are developed in cybersecurity training programs and the demands that are placed on organizations from such programs. Hatzivasilis [4] addressed the issues that arise when training a diverse target audience that possesses varied degrees of experience. Chowdhury [5] underlined the importance of strengthening cybersecurity training and is advocating approaches that are based on simulation and practical experience.

This study focuses on the ongoing problem of inadequate security knowledge and awareness in the face of an increasing number of cyber threats. Popescul [6] emphasized on employees' lack of awareness and comprehension of security issues in organizational environments. In another study, Woldemichael [2] found that many employees demonstrated insufficient knowledge, training, and awareness, making them susceptible to emerging cyber threats.

Present training methods often fail to engage learners effectively, leading to insufficient readiness to handle the ever-changing cybersecurity environment [7]. Specifically, these methods may lack engaging elements, relevance to real-world scenarios, and personalized feedback, all of which are critical for maintaining learner engagement [8]. Without engagement, learners are less likely to retain critical information or develop the necessary skills, thereby undermining the overall effectiveness of the training [9].

While various serious games have been developed to enhance cybersecurity training, they are often limited by a lack of diversity in game genres and formats. For instance, "CyberCIEGE" [10] and "CyberCity" provide detailed simulations of cyber-attacks using a complex scenario-based approach. While this high-fidelity simulation emphasizes realistic contexts, it can inadvertently increase the cognitive load of learners [11], potentially overwhelming novices. In contrast, SecureCyberQuest (SCQ) distinguishes itself by adopting modular mini-game architecture. This design choice mitigates cognitive overload by compartmentalizing complex concepts into manageable, focused tasks, ensuring knowledge acquisition without overwhelming the learner. Similarly, platforms like "Hack the Box" [12] and "Phishd" [13], while effective for skill enhancement, often suffer from the limitations of linear gameplay modes. While platforms like "Hack the Box" remain industry leaders as evidenced by their 2024 Cyber Attack Readiness Report, they are primarily designed for technical skill acquisition rather than general awareness. Recent evaluations suggest that their steep learning curve creates a barrier for undergraduate novices, validating the need for a simplified, narrative-driven approach as proposed in this study. These games typically consist of single, repetitive tracks which may lead to diminished engagement over time. SCQ addresses this limitation by incorporating broader experience-based learning and motivational elements derived from Flow Theory. By integrating a cohesive virtual office narrative,

SCQ fosters sustained engagement [14] distinct from the purely drill-based or linear progressions of its predecessors.

To address these issues, this study explores the integration of multiple theories such as Flow Theory and Cognitive Load theory in the design of serious games for cybersecurity training. While each theory offers valuable insights, their limitations underscore the need for a more comprehensive approach. For instance, Flow Theory highlights the importance of balancing challenge and skill to achieve optimal learning outcomes but may require additional elements for full engagement [15]. The research explores how serious games can foster a sense of ownership and personal relevance in learners, thereby increasing their motivation to engage with cybersecurity content. This theory is particularly relevant in the context of cybersecurity education, where learners must be motivated to continuously update their knowledge and skills to keep pace with emerging threats.

The significance of this research lies in its potential to improve cybersecurity awareness and training by addressing the limitations of existing approaches and integrating a more robust theoretical framework. By doing so, it aims to enhance the readiness of individuals and organizations to navigate the complexities of the modern cybersecurity landscape, ultimately reducing the risk of cyberattacks and their associated consequences. The objective of this study is to design serious games for promoting engagement amongst participants. In addition, this study aims to analyze the impact of serious games in improving cybersecurity awareness.

II. Literature Review

A. Serious Games in Cybersecurity and Awareness Capabilities

Serious games are immersive and engaging educational tools designed to impart knowledge, improve skills, and enhance problem-solving abilities [16] in an immersive environment. In the context of cybersecurity, these games serve dual purposes: they raise awareness of cybersecurity risks and responses while also honing practical skills for effectively addressing these threats. Serious games captivate learners by immersing them in engaging environments. A study by Hainey *et al.* [17] demonstrates that serious games significantly enhance learner engagement and retention compared to traditional methods.

There are several appealing features of serious games that can facilitate the learning and skills development process. Firstly, serious games facilitate adaptability and innovation, where advances in technology have made serious games more adaptable for various educational contexts. For example, Rebah and Slama [18] discuss how modern serious games utilize advanced graphics and simulations to provide dynamic learning experiences. Secondly, serious games support learning through simulation to create realistic learning scenarios. Research shows that structured cybersecurity simulations, especially when combined with live competitive activities, significantly improve learning outcomes compared to traditional classroom instruction [19]. Thirdly, serious games promote better engagement and consequently enhance learning effectiveness. Jayakrishnan *et al.* [20] analyzed 15 serious games and found that they effectively improved participants' understanding of security practices, although challenges remain in measuring long-term effects. Similarly, Alqahtani and Kavakli-Thorne [21] developed CybAR, an augmented reality serious game that increased participants' engagement and comprehension of cybersecurity concepts.

These examples highlight the potential of serious games to transform cybersecurity education. By providing a more engaging and hands-on approach, these games not only improve practical cybersecurity skills but also foster a heightened sense of responsibility and vigilance. As digital threats continue to grow, the importance of these qualities in both individuals and organizations cannot be overstated.

Recent Advances in Gamified Cybersecurity (2023–2025), recent literature has shifted focus toward reducing cognitive load in gamified training. Nkongolo introduced "CyberMoraba", [22] a game utilizing indigenous board game mechanics to lower entry barriers for non-technical users, demonstrating that culturally familiar formats significantly increase engagement. Similarly, the "CyberVigilance" project employed a multi-agent system to provide real-time, personalized feedback during card-based gameplay, which was found to improve decision-making speed by 15% compared to static training methods [23]. A systematic review of further emphasized that while competitive elements (leaderboards) are common, they fail to sustain long-term behavior change without the narrative immersion that newer frameworks prioritize [24]. These findings confirm a growing trend away from purely technical drills toward narrative-driven, low-cognitive-load environments.

Despite the success of games like CybAR in utilizing augmented reality, other established platforms reveal specific pedagogical limitations. For instance, CyberCIEGE [10] and CyberCity employ high-fidelity, scenario-based simulations. While these effectively model complex real-world environments, research indicates that such dense information can induce excessive cognitive load, potentially impeding the learning process for novices [11]. Conversely, skill-building platforms such as Hack the Box [12] and Phishd [13] often rely on linear progression models. Although effective for drilling specific technical tasks, these linear formats often lack the narrative immersion and diverse gameplay mechanics necessary to sustain long-term engagement and motivation [14]. This highlights a critical gap for a solution that balances manageable cognitive load with engaging, non-linear narrative elements.

In the proposed serious game, various aspects were addressed such as giving the participant ample time to tackle challenges, immediate feedback after each engaging action for better awareness rising, having focused concepts instead of content feeding them with various different levels of cybersecurity concepts, multimedia elements, NPCs to interact with, immersive office setting, and enough challenges and difficulty to keep engagement and enjoyment at satisfactory levels.

B. Learning Theories Used in Game Development

In the development of this serious game, two theories were used as reference: Flow Theory and Cognitive Load Theory (CLT). Flow Theory, developed by Mirvis and

Csikszentmihalyi [25], states that players are most motivated when they encounter challenges and require skills higher than average [26]. Based on this theory, games should be designed to contain clear goals, balanced challenges and immediate feedback [27]. Having these elements in games can enhance learners' engagement and motivation. This has been confirmed in numerous empirical studies and systematic reviews. Additionally, the flow elements in the game such as feedback and immersion also enhance the learners personalized learning through self-regulation and progress monitoring. Meanwhile, the Cognitive Load Theory proposed by Sweller *et al*. [28] is a fundamental principle in the development of serious games, as it impacts the efficiency of learning and performance. Studies have found that when games are designed based on CLT, students will have better retention compared to traditional learning methods [28]. As such, educational games are designed to align with CLT to facilitate incremental learning experience and appropriate cognitive load at a given time.

III. Prototype Development and Hypotheses Development

Based on the Flow and Cognitive Load theories, the objectives of the solution are formulated as follows. The game that was developed is named SecureCyberQuest" (SCQ). The main objective of this game is to promote engagement and immersion. This was achieved through balancing and skills within both the main game and mini games. Secondly, the game was designed to promote suitable cognitive load in supporting users learning progress. These approaches employed in designing SCQ specifically address the limitations of existing serious games, such as CyberCIEGE and CyberCity, which rely on scenario-based approaches that may heighten the cognitive load of learners [11] and hamper the objective of acquiring knowledge. Unlike these expansive simulations, SCQ's innovation lies in its theory-driven decomposition of complex security topics into distinct mini-games. This structure provides a broader, diversified learning experience that continuously engages learners, offering a distinct alternative to the linear game approaches found in titles like Hack the Box [12]. By integrating CLT, SCQ ensures that educational content is delivered in digestible segments, optimizing the learning curve compared to traditional linear or heavy-simulation formats.

These theories underpin the game design, ensuring a comprehensive educational experience that enhances cybersecurity awareness through a carefully crafted serious game. The integration of these theoretical frameworks ensures that the game is engaging, educational, and effective in improving cybersecurity awareness among undergraduate students.

Prior to commencing development, a comprehensive evaluation and examination of both the game's narrative and prototype was carried out to guarantee alignment with educational goals and player engagement. This strategic design is crucial for addressing the limitation of linearity and restricted learning experiences observed in existing games. SCQ differs fundamentally from existing platforms in its instructional design strategy, specifically in how it manages learner scaffolding and feedback loops. Platforms like Hack The Box [12] predominantly utilize a "Discovery Learning" mechanic, where learners are presented with a problem (e.g., a vulnerable server) and must externally research solutions with minimal in-game guidance. In contrast, SCQ employs a "Guided Scaffolding" mechanic. Before each mini-game, SCQ utilizes pre-training principles providing bite-sized theoretical context (e.g., key indicators of phishing) before the user engages with the mechanic.

In this phase, the game's concept was formulated with a focus on innovation in gameplay design: creating a compelling narrative of a virtual office that situates the learner in a relatable professional environment. This narrative context differentiates SCQ from the abstract technical challenges of Hack the Box or the resource-heavy simulations of CyberCIEGE. CLT was central to the design, driving the development of isolated mini games that test distinct cybersecurity issues to facilitate optimal cognitive load management. The game's structure including levels, challenges, and mechanics were carefully strategized to align with the educational objectives identified in the analysis phase. Storyboards and flowcharts were developed to visualize this progression, ensuring the design was not only educational but also engaging, immersive, and enjoyable. Additionally, design decisions were made to incorporate theories such as Flow Theory to maximize user engagement, creating a balance between challenge and skill that is often difficult to achieve in purely linear formats. The feedback granularity in SCQ is designed for formative assessment rather than the summative assessment found in Phishd [13] While Phishd typically provides binary feedback (caught/not caught), SCQ integrates explanatory feedback loops: when a user fails a challenge, the game explicitly highlights the specific missed cue (e.g., "mismatched URL domain") rather than just assessing a penalty, thereby reinforcing the schema acquisition required for long-term retention.

The serious game was developed to provide students with cybersecurity basics in an engaging manner. Social engineering, password management, phishing and hacking were chosen as concepts for this serious game as they are the basic entry points of cybersecurity for beginners. For the study, undergraduates were chosen because social engineering, the act of influencing individuals to take actions that may not be in their best interests, is a key tactic in cyberattacks [27]. It exploits the human element, which is often the weakest aspect of an organization's security [28]. Moreover, beginners should learn about password management for several reasons. Firstly, password managers can help them handle their passwords more effectively, reducing the risk of password reuse and making it easier to manage multiple strong and unique passwords [29]. Additionally, gamification can be a useful tool for phishing and hacking, but current solutions often lack basic knowledge and are not adaptable to different contexts [30].

The first mini game is called the Social Engineering Mini-Game. In this mini-game, players must identify security breaches in various office rooms, including offices, printing areas, and server rooms. They look for vulnerabilities such as unattended computers, open server room doors, and exposed documents before they can begin the search for items. In the second mini-game called the Password Vault Management Mini-Game, players have to create strong passwords for five

different accounts. They must use their knowledge of password best practices to ensure each password is secure. A password generator is available, but points will be deducted if used. This encourages players to manually create robust passwords and understand the elements of strong password creation. Flow Theory is used by engaging players in the challenge of creating secure passwords within a time limit. The feedback provided on password strength enhances the players' sense of competence. The last mini game is a quiz that tests the player's overall knowledge gained throughout the game. It serves as a comprehensive review of all the topics covered, including social engineering (Fig. 1), phishing (Fig. 2) hacking, and password management. Players answer multiple-choice questions and receive feedback on their performance, reinforcing their learning and identifying areas for improvement.

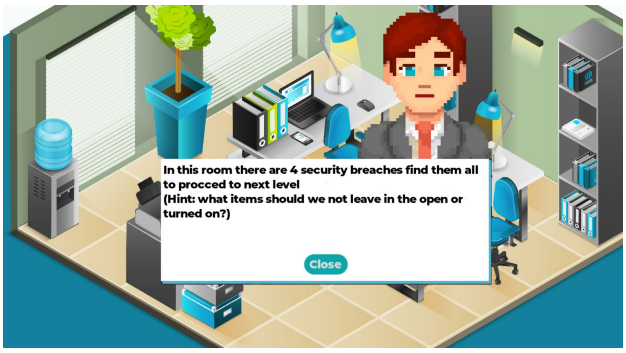

Fig. 1. Social engineering minigame.

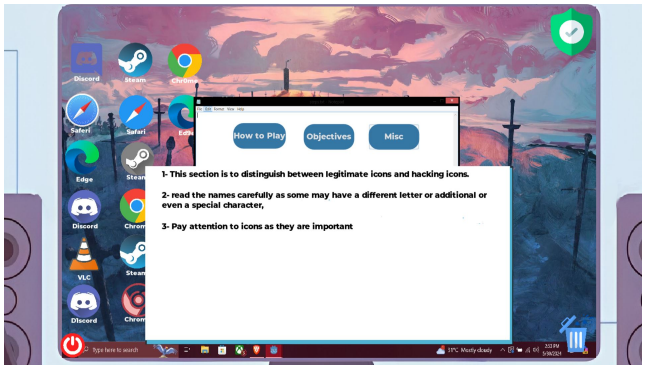

Fig. 2. Malicious software minigame.

This study builds on previous research to explore the effectiveness of serious games in cybersecurity education. The hypotheses are derived from studies that highlight the potential of serious games to enhance learning and engagement. Specifically, research by Rebah and Slama [18] emphasized on the role of serious games in actively engaging learners and creating immersive educational environments. The hypotheses are further informed by the findings of Moizer *et al.* [31], which underscore the impact of game design on educational outcomes.

Serious games are recognized for their potential to enhance learning outcomes by combining educational content with engaging gameplay. Research supports the idea that these games can improve knowledge retention and understanding of complex subjects. For instance, Hainey *et al.* [18] found that serious games facilitate deeper learning by engaging users in realistic scenarios that reinforce theoretical concepts. Similarly, Chennamaneni *et al.* [32] demonstrated that serious games can effectively convey cybersecurity concepts, leading to improved awareness and skills among users. Hence:

H1: There is a significant difference in the knowledge of cybersecurity awareness in pre- and post-game intervention.

The design elements of serious games, including gaming experience, learning experience, and usability, play crucial roles in determining user engagement. Previous studies highlight the importance of these factors. Research by Bowman [33] indicates that a well-designed gaming experience, characterized by compelling gameplay mechanics and challenges, enhances user engagement and motivation. Additionally, according to Hall *et al.* [34], the alignment of educational content with engaging gameplay significantly improves the learning experience and consequently increases user engagement. The usability of serious games, including intuitive interfaces and ease of navigation, is critical for maintaining user interest. Nadolski and Hummel [35] emphasize that high usability is associated with greater user enjoyment and engagement. Based on the arguments, the following hypotheses are proposed:

H2: The design of the serious game will significantly correlate with levels of engagement among the users.

H2a: Gaming Experience will significantly correlate with levels of engagement among the users.

H2b: Learning Experience will significantly correlate with levels of engagement among the users.

H2c: Usability will significantly correlate with levels of engagement among the users.

IV. Methodology

A. Sample and Sampling Technique

The target demographic for this study on increasing cybersecurity awareness is undergraduate students. Undergraduates from different majors, aside from information technology and computer science students, were suitable candidates for this study due to their relatively lower level of understanding of cybersecurity issues. Undergraduates were suitable for this purpose as students currently studying in universities and their role as future employees in organizations who may be exposed to cybersecurity issues. This strategy was chosen to ensure ease of access and participation, allowing for the efficient collection of data. Purposive sampling enabled the study to gather a diverse range of participants quickly, facilitating a practical and accessible approach to understanding the impact of the serious game on cybersecurity awareness.

Appointments were made with some lecturers from business schools to carry out experiments using the CyberQuest game. A short presentation about the fundamental concepts of cybersecurity was conducted. The participants were informed that the objective of this study is purely for academic purposes and no identifiable information such as student matric numbers were collected. Additionally, this study is not graded and treated as part of coursework, hence there was no obligation for the students to give favorable responses that may potentially lead to self-desirability bias. After the students declared their agreement to voluntarily participate in the study, they were asked to play the game for 30 min (Fig. 3).

Initially, a pre-test survey was distributed before the

experiment, and a post-test survey was given later. The objective of the survey is to measure cybersecurity awareness/knowledge before playing the game and after. In addition, their perception of engagement, learning experience and usability score of the game was also measured. During the experiment, there was no interference with the player by either helping them with the system or how they would play the game. This gave the participants the liberty of testing every aspect of the prototype by themselves at their own pace. The total number of participants involved in the experiment was 44 students. As this was a pilot experimental study, the sampling size was deemed appropriate following the recommended threshold size of 30 participants to achieve certain minimum detectable effect sizes. A priori power analysis indicated that a sample size of 44 participants per group provides approximately 60–65% power to detect a medium effect size (Cohen's $d = 0.5$) using an independent-samples t test with $\alpha = 0.05$.

Fig. 3. Participants during the experiment.

B. Data Collection Instruments

Questionnaire-based methodologies were employed to conduct surveys for assessing players prior to and after the game. These questionnaires are crucial tools for systematically gathering quantitative data on participants' attitudes, knowledge, engagement and perceptions regarding cybersecurity awareness.

Prior to the introduction of serious game intervention, the pre-test established a foundational understanding of the participants' knowledge and perspectives. This baseline data is essential for evaluating the efficacy of the serious game approach. It allowed us to evaluate the initial understanding levels of the participants and identify any underlying misunderstandings or areas of weakness. We examined the participants' changes in knowledge and engagement by administering a post-test after they had interacted with serious game intervention. The impact of serious game intervention on participants' learning outcomes can be assessed by comparing the responses from the pre- and post-tests. Through this comparative analysis, we identified specific areas where serious games have effectively enhanced awareness, as well as areas that require further exploration or enhancement.

The survey included measurements of the following:

(1) **Gaming Experience:** This is a composite factor involving elements like design of challenge, gameplay experience and goal achievement that influence how players perceive and interact with the game [36].

(2) **Learning Experience:** Measures the instructional effectiveness of the game in enhancing participants' knowledge of cybersecurity awareness. It includes understanding the goals of the game, cybersecurity awareness relevancy, and the value of serious games as a learning tool.

(3) **Engagement**: This quantifies the degree of active participation and enthusiasm during serious game play, assessing the game's ability to maintain players' interest and facilitate learning. Examples include how the contents of the game keep them going and their concentration levels while playing the game.

(4) **Usability** refers to the ease of use and effectiveness of an interface and the way users interact with it. The System Usability Scale (SUS) was utilized to find the usability of the proposed serious game, which ranges from 1–5 (1 being strongly disagree, 2 disagree, 3 neutral, 4 agree, and 5 strongly agree). The use of the SUS scale to measure usability is a useful tool for assessing the quality of serious games [36]. A SUS score above 68 is generally considered above average and indicative of good usability. Scores below this threshold suggest that there may be usability issues that need to be addressed. The interpretation of SUS scores follows these general guidelines.

V. Results and Discussion

A. Demographic Information

The demographic information of the participants provides insight into the composition of the sample and its relevance to the target population. The gender distribution was balanced, with a slight majority of male participants (59.1%) compared to female participants (40.9%). The participants consist of 62% from Business and Management, 22% students from Quantitative degrees and 4% from Social Science 4%, while the rest were studying different fields.

B. Reliability Analysis

The reliability of the six factors (Gaming Experience, Learning Experience, Usability and Engagement) was assessed using Cronbach's alpha. All factors demonstrate reliability (ranging from 0.65 to 0.87). Refer to Table 1.

Table 1. Table Cronbach's alpha value

Factors	Cronbach' Alpha value
Gaming Experience	0.68
Learning Experience	0.83
Usability	0.79
Engagement	0.87

C. Usability (SUS Score)

In this study, participants rated their experience with the serious game, resulting in an overall SUS score of 78.6. This score falls within the "good" range [36] suggesting that most participants found the game to be user-friendly and easy to navigate. The high SUS score indicates that the game's design effectively facilitated user interaction and contributed to a positive user experience as shown in (Fig. 4).

This high usability is crucial for engaging users and ensuring that the educational objectives of the serious game

are met effectively. The usability score for this game is relatively good compared to previous serious games, which had a 72-usability score for the "Guess who?" game. Additionally, another game called "SherLOCKED" by Jaffray *et al.* [37], which is situated in the context of an undergraduate cyber security course and is used to consolidate students' knowledge of foundational security concepts, had a SUS score of 77.

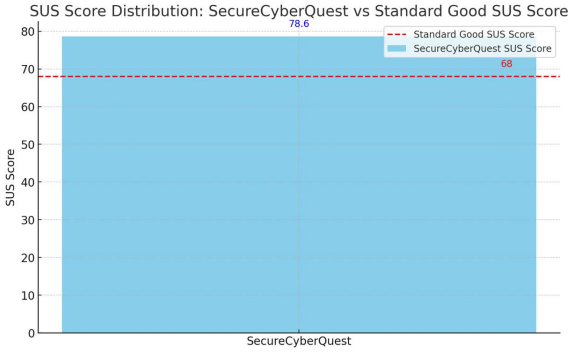

Fig. 4. SUS score distribution.

D. Knowledge of Cybersecurity Awareness

To measure the effectiveness of the serious game in improving cybersecurity awareness, participants completed a pre-test before playing the game and a post-test after completing it.

1) Pre and post test result

The average pre-test score was 7.59 out of 15, reflecting a baseline level of cybersecurity knowledge. This translates to a 50.6% average score, indicating the participants' initial understanding of cybersecurity concepts.

The average post-test score increased to 12 out of 15, demonstrating a significant improvement in cybersecurity awareness. This translates to an 80% average score, showing a notable increase in participants' knowledge. The percentage increase in average scores from pre-test to post-test is approximately 29.4%. (Fig. 5) visualizes the comparison.

A paired sample t-test was conducted to compare the pre-test and post-test scores of the 44 participants. The purpose of this test was to determine whether there was a statistically significant improvement in cybersecurity awareness before and after engaging with the serious game.

The pre-test and post-test results showed a significant mean difference of 4.41 points, with the pre-test average being 7.59 and the post-test average increasing to 12. This indicates a substantial improvement in participants' cybersecurity knowledge. The paired t-test results were highly significant, with a paired t-test value of (0.00000000850259) and supported H1. This strong statistical significance confirms that the observed improvement in scores is not due to chance, but rather a result of the intervention provided by the serious game.

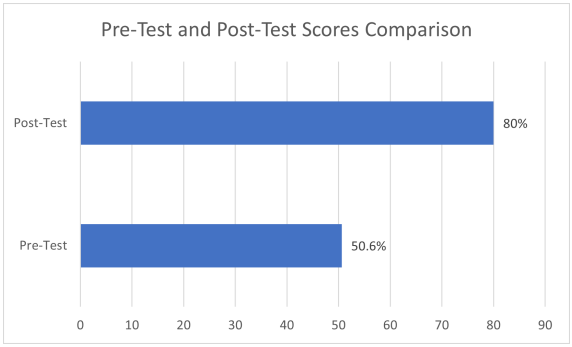

Fig. 5. Pre-test and post-test scores comparison.

To further quantify the impact of the serious game, Cohen's *d* was calculated to measure the effect size. The resulting value of 1.07 indicates a large effect size, demonstrating that the serious game had a substantial impact on improving participants' cybersecurity awareness. The findings suggest that serious games can be a valuable tool in cybersecurity education, providing an engaging, immersive and enjoyable learning experience that traditional methods may lack. The integration of theoretical frameworks, such as Flow Theory and CLT, contributed to the game's success in enhancing knowledge and skills. Table 2 shows the results.

Table 2. Statistical results

Statistic	Value
Mean Difference	4.41
Standard Deviation	4.11
Paired T-test	0.00000000850259
Cohen's d	1.07

2) Regression analysis of factors with engagement

Simple linear regression analysis conducted for this study revealed several significant relationships among the factors, highlighting important associations within the serious game intervention (see Table 3).

Table 3. Linear regression

Hypothesis	R^2	F-Statistic	Significance F (*p*-value)	*ß* (Coefficient)
Gaming Experience → Engagement	0.152	7.55	0.00881	0.336
Learning Experience → Engagement	0.556	52.62	6.31×10^{-9}	0.675
Usability →Engagement	0.463	36.14	3.82×10^{-7}	0.678

The analysis revealed that gaming experience is significantly correlated with engagement (R^2 = 0.152, F= 7.55, p = 0.00881) supporting hypothesis H2a. The analysis shows that learning experience is strongly correlated with engagement. Specifically, the learning experience has a significant impact (R^2 = 0.556, F= 52.62, $p = 6.31 \times 10^{-9}$) supporting H2b.

Usability also plays a crucial role (R^2 = 0.463, F= 36.14, $p = 3.82 \times 10^{-7}$), underscoring the importance of intuitive design and usability for maintaining user engagement and supporting H2c. These findings align with the idea that gaming and learning experience keep users engaged in the learning process. The inclusion of multimedia elements, such as visuals, audio, and animations, caters to different learning styles and helps to make complex concepts more accessible and engaging. These design elements are on par with the games mentioned in the literature review such as "CyberCIEGE" and "CyberCity" where users gain better

insight based on the environment in the game and challenges as well as the reward the they gain from playing, using such elements also proved successful in the domain of SGs in healthcare [38].

VI. Discussion

The findings of this study provide initial empirical support that serious games (SCQ) can enhance learners' engagement.

First, one of the main ways that SCQ design promotes flow is through challenge-skill balance. The balance between player skill and task needs is maintained in SCQ as it gradually increases the difficulty levels (e.g., levels, adaptive challenges, knowledge level). This balance is a strong predictor of flow and persistent engagement in educational games, according to other empirical studies. This is because learners are motivated without getting bored or discouraged. Second, SCQ has clear goals and tasks. The game mechanics inclusive of mission, clear learning outcome and progress indicators enhance attentional focus. Third, the immediate feedback provided in SCQ through performance points, badges and scoreboards reinforces players' understanding of their progress. Research demonstrates that timely feedback strengthens perceived competence and control, which directly contributes to flow experience and higher engagement levels [39]. Finally, immersion through narrative and audiovisual design reduces self-consciousness and external distractions. Studies indicate that immersive environments facilitate deep cognitive absorption, enabling users to enter flow states more easily and remain engaged for longer durations.

SCQ was also found to be helpful in increasing cybersecurity awareness for non-technical students through positive engagement and learning experience in the serious game.

The findings of this study highlight SCQ's distinct position within the cybersecurity serious game landscape. While established games like CyberCIEGE and CyberCity offer high-fidelity, scenario-based simulations, they often risk overwhelming novice learners with complex, resource-intensive environments. SCQ's modular mini-game design successfully mitigates this by managing cognitive load, offering a more accessible entry point for undergraduates. Furthermore, unlike the linear progression models seen in Hack the Box and Phishd, which may suffer from repetitive gameplay loops, SCQ's integration of a narrative-driven environment and Flow Theory principles resulted in high engagement levels. This demonstrates that balancing theoretical foundations with diverse gameplay formats rather than relying solely on realistic simulation or linear drills is a critical innovation for fostering both cybersecurity awareness and sustained learner engagement.

VII. Conclusion and Future Research

"SecureCyberQuest" (SCQ) represents a significant step forward in the realm of cybersecurity education through the innovative use of serious gaming. This study has demonstrated the effectiveness of SCQ in enhancing cybersecurity awareness among undergraduate students as evidenced by the marked improvement in post-test scores. The thoughtful integration of Flow Theory and CLT into the game's mechanics was central to achieving these outcomes. By embedding these theoretical frameworks into the gameplay, SCQ not only engaged participants but also provided a dynamic and immersive learning environment. This environment enabled students to apply complex cybersecurity concepts in simulated scenarios, fostering a deeper understanding and retention of the material.

Despite the positive findings, this study has several limitations that can be addressed in future research. The study was conducted among a sample of undergraduate students in a public university. Several other factors may be considered in expanding this study, such as the consideration of player style [40] that may influence the effectiveness of serious games. Social achiever players, for example, prefer collaborative play to achieve meaningful goals, enjoy team strategy and competition, and dislike solo play. Meanwhile, explorer players are inclined towards games with storylines and solo exploration. Additionally, in future, different levels of expertise such as novice and intermediate learners need to be considered as moderating factors in experimental design.

This study employed pre and post-tests on the participants before playing the game to examine the effect of gamification on their cybersecurity knowledge. In the future, a longitudinal classroom study in which the modules of the games are increased progressively may help to better assess engagement, satisfaction, effort, and performance over time.

In conclusion, SCQ provides a promising approach for educating essential skills, especially in the cybersecurity domain. Organizations can employ this approach to provide a flexible and individualized phased approach for staff to acquire different levels of fundamental knowledge regarding cybersecurity, which can help them to prevent issues such as hacking and phishing. Furthermore, the concept of serious games can be contextualized to other important domains such as basic artificial intelligence issues.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

R.A. designed the research study and game design framework. M.M.-R. conducted the study. This report is co-jointly produced. All authors had approved the final version.

References

[1] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing industry 4.0 cybersecurity challenges," *IEEE Eng. Manag. Rev.*, vol. 47, no. 3, pp. 79–86, Jul. 2019. doi: 10.1109/emr.2019.2927559

[2] H. T. Woldemichael, "Emerging cyber security threats in organization," *Int. J. Inf. Commun. Sci.*, vol. 5, no. 2, 19, Jan. 2020. doi: 10.11648/j.ijics.20200502.12

[3] C.-N. Bodea, M.-I. Dascalu, and M. Cazacu, "Increasing the effectiveness of the cybersecurity teaching and learning by applying activity theory and narrative research," *Issues Inf. Syst.*, Jan. 2019. doi: 10.48009/3_iis_2019_186-193

[4] G. Hatzivasilis *et al.*, "Modern aspects of Cyber-Security training and continuous adaptation of programmes to trainees," *Appl. Sci.*, vol. 10, no. 16, 5702, Aug. 2020. doi: 10.3390/app10165702

[5] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Comput. Sci. Rev.*, vol. 40, 100361, Feb. 2021. doi: 10.1016/j.cosrev.2021.100361

[6] D. Popescul, "Information security awareness in contemporary organizations—challenges and solutions," *Secur. Future*, vol. 2, pp. 134–137, 2018.

[7] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and N. J. Jeu, "An effective cybersecurity training model to support an organizational awareness program," *IGI Global eBooks*, 2020, pp. 174–188. doi: 10.4018/978-1-7998-7705-9.ch008

[8] J. C. Dalgaard, N. A. Janssen, O. Kulyk, and C. Schürmann, "Security awareness training through experiencing the adversarial mindset," in *Proc. Symposium on Usable Security and Privacy*, San Diego, United States, Jan. 2023. doi: 10.14722/usec.2023.237300

[9] A. Giriraj, S. Haggag, and H. Haggag, "Human centric framework for customising and producing effective cybersecurity training materials," *DIVA*, pp. 69–77, 2022.

[10] M. Thompson and C. Irvine, "Active learning with the CyberCIEGE video game," Defense Technical Information Center, Aug. 2011. doi: 10.21236/ada547670

[11] J. L. Plass, B. D. Homer, and C. K. Kinzer, "Foundations of game-based learning," *Educ. Psychol.*, vol. 50, no. 4, pp. 258–283, Oct. 2015.

[12] M. M. Yamin, B. Katt, and M. Nowostawski, "Serious games as a tool to model attack and defense scenarios for cyber-security exercises," *Comput. Secur.*, vol. 110, 102450, Aug. 2021. doi: 10.1016/j.cose.2021.102450

[13] G. Jayakrishnan, V. Banahatti, and S. Lodha, "PickMail: A serious game for email phishing awareness training," in *Proc. 2022 Symp. Usable Secur.*, 2022. doi: 10.14722/usec.2022.23059

[14] W. Westera, "Why and how serious games can become far more effective: Accommodating productive learning experiences, learner motivation and the monitoring of learning gains," *J. Educ. Technol. Soc.*, vol. 22, no. 1, pp. 59–69, 2019.

[15] M. Dixon, N. A. G. Arachchilage, and J. Nicholson, "Engaging users with educational games," in *Proc. Hum. Factors Comput. Syst.*, May 2019. doi: 10.1145/3290607.3313026

[16] M. Sasupilli and P. Bokil, "Understanding the elements of challenge and skills in educational games," in *Proc. Eur. Conf. Games Based Learn.*, Sep. 2022, vol. 16, no. 1, pp. 500–507. doi: 10.34190/ecgbl.16.1.655

[17] T. Hainey *et al.*, "Serious games as innovative formative assessment tools for programming in higher education," in *Proc. Eur. Conf. Games Based Learn.*, Sep. 2022, vol. 16, no. 1, pp. 253–262. doi: 10.34190/ecgbl.16.1.756

[18] H. B. Rebah and R. B. Slama, "The educational effectiveness of serious games," *Médiations Et Médiatisations*, no. 2, pp. 131–155, Nov. 2019. doi: 10.52358/mm.vi2.97

[19] M. D. Workman, J. A. Luevanos, and B. Mai, "A study of cybersecurity education using a Present-Test-Practice-Assess model," *IEEE Trans. Educ.*, vol. 65, no. 1, pp. 40–45, Jun. 2021. doi: 10.1109/te.2021.3086025

[20] G. Jayakrishnan, V. Banahatti, and S. Lodha, "Design and execution challenges for cybersecurity serious games: An overview," arXiv preprint, arXiv:2307.09401, Jan. 2023.

[21] H. Alqahtani and M. Kavakli-Thorne, "Design and evaluation of an augmented reality game for cybersecurity Awareness (CYBAR)," *Information*, vol. 11, no. 2, 121, Feb. 2020. doi: 10.3390/info11020121

[22] M. Nkongolo, "CyberMoraba: A game-based approach enhancing cybersecurity awareness," arXiv preprint, arXiv:2403.10118, 2024.

[23] M. W. Nkongolo, T. Sithole, and J. Sewnath, "Cybersecurity awareness through interactive learning using the CyberVigilance game," in *Proc. Int. Conf. Cyber Warfare Secur.*, 2025, vol. 20, no. 1, pp. 501–510. doi: 10.34190/iccws.20.1.3207

[24] A. Gwenhure and F. Rahayu, "Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review," *Int. J. Serious Games*, vol. 11, no. 1, pp. 83–99, 2024. doi: 10.17083/ijsg.v11i1.719

[25] P. H. Mirvis and M. Csikszentmihalyi, "Flow: the psychology of optimal experience," *Acad. Manage. Rev.*, vol. 16, no. 3, 636, Jul. 1991. doi: 10.2307/258925

[26] D. J. Acland, "An investigation of flow theory in an online game," *Rev. Behav. Econ.*, vol. 7, no. 4, pp. 317–336, Jan. 2020. doi: 10.1561/105.00000127

[27] A. Perttula, K. Kiili, A. Lindstedt, and P. Tuomi, "Flow experience in game based learning—A systematic literature review," *Int. J. Serious Games*, vol. 4, no. 1, Mar. 2017. doi: 10.17083/ijsg.v4i1.151

[28] J. Sweller, P. Ayres, and S. Kalyuga, *Cognitive Load Theory*, New York, NY: Springer, 2011. doi: 10.1007/978-1-4419-8126-4

[29] J. S. Davis, "Game framework analysis and cognitive learning theory providing a theoretical foundation for efficacy in learning in educational gaming," *Int. J. Learn. Teach. Educ. Res.*, vol. 19, no. 7, pp. 159–175, Jul. 2020. doi: 10.26803/ijlter.19.7.9

[30] A. Rege, K. Williams, and A. Mendlein, "A social engineering course project for undergraduate students across multiple disciplines," in *Proc. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Jun. 2019. doi: 10.1109/cybersecpods.2019.8885085

[31] J. Moizer *et al.*, "An approach to evaluating the user experience of serious games," *Comput. Educ.*, vol. 136, pp. 141–151, Apr. 2019. doi: 10.1016/j.compedu.2019.04.006

[32] S. Chennamaneni et al., "Designing cybersecurity AI based awareness games for citizens: best practices and future directions," in *Proc. 2022 Int. Conf. Sustain. Comput. Data Commun. Syst. (ICSCDS)*, Mar. 2023. doi: 10.1109/icscds56580.2023.10104800

[33] N. D. Bowman, J.-H. T. Lin, and K. Koban, "Demanding on many dimensions: Validating the interactivity-as-demand measurement model for VR-Based video games," in *Proc. TMS 2021*, May 2022. doi: 10.1037/tms0000041

[34] J. Hall, P. Wyeth, and D. Johnson, "Creating authentic experiences within a serious game context: evaluation of engagement and learning," *Lecture Notes in Computer Science*, 2016, pp. 55–66. doi: 10.1007/978-3-319-45841-0_5

[35] R. J. Nadolski and H. G. K. Hummel, "Retrospective cognitive feedback for progress monitoring in serious games," *Br. J. Educ. Technol.*, vol. 48, no. 6, pp. 1368–1379, Aug. 2016. doi: 10.1111/bjet.12503

[36] L. Shoukry, J. Konert, and S. Göbel, "The evaluation of learner experience in serious games," *Advances in Educational Technologies and Instructional Design*, 2018, pp. 122–148. doi: 10.4018/978-1-5225-4206-3.ch005

[37] A. Jaffray, C. Finn, and J. R. C. Nurse, "SherLOCKED: A Detective-Themed serious game for cyber security education," *IFIP Advances in Information and Communication Technology*, pp. 35–45, 2021. doi: 10.1007/978-3-030-81111-2_4

[38] Y. Wang *et al.*, "Application of serious games in health care: Scoping review and bibliometric analysis," *Front. Public Health*, vol. 10, Jun. 2022. doi: 10.3389/fpubh.2022.896974

[39] J. Hamari *et al.*, "Challenging games help students learn," *Comput. Hum. Behav.*, vol. 54, pp. 170–179, 2016. doi: 10.1016/j.chb.2015.07.045

[40] A. E. J. Van Gaalen, J. Schönrock-Adema, R. J. Renken, A. D. C. Jaarsma, and J. R. Georgiadis, "Identifying player types to tailor game-based learning design to learners: Cross-sectional survey using Q methodology," *JMIR Serious Games*, vol. 10, no. 2, e30464, 2022. doi: 10.2196/30464

Copyright © 2026 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).