CyberAware: A Gamified Approach To Increase Cybersecurity Awareness

Marwan Altamimi[1] and Erisa Karafili*[1] [0000−0002−8250−4389]

School of Electronics and Computer Science,
University of Southampton
{ma1u20, e.karafili}@soton.ac.uk

Abstract. Social engineering attacks remain a continuous threat to cybersecurity. Traditional assessment methods often fall short in changing user behaviour to effectively prevent social engineering threats. In this paper, we introduce CyberAware, a novel serious game for cybersecurity training, designed to improve users' cybersecurity awareness through active learning. Built on Unity WebGL and core game design principles, CyberAware features interactive challenges in phishing, password strength, and social engineering. Our evaluation analysis showed an average knowledge gain of 41.6% after only one session of gameplay and revealed that 67% of the users found the game highly engaging. Our analysis showed that CyberAware offering is similar to existing games, making it a highly competitive alternative serious game for cybersecurity training.

Keywords: Gamification · Cybersecurity awareness · Serious Games · Game Design Development

1 Introduction

Social engineering attacks remain a continuous and evolving threat in the cybersecurity landscape[10]. Often, these attacks exploit people-centered vulnerabilities and leverage human psychology to help intruders bypass sophisticated technological defenses[29,7]. They are either used as attacks on their own or as part of well-orchestrated, bigger attacks[12]. SMEs and MEs are even more susceptible to such attacks, with respect to bigger organisations, given the low resources they have for training and raising cybersecurity awareness among their employees [3,16,11].

Current cybersecurity training often falls short in changing user behavior to effectively prevent social engineering threats [31,13] or in fostering robust security postures [24]. Such training is often too generic, missing the critical nuances of how human biases and cultural contexts influence security breaches. As these attacks typically involve tricking individuals into breaching security protocols, traditional training methods find it challenging to effectively counteract

* Corresponding Author: Erisa Karafili, e.karafili@soton.ac.uk
Acknowledgement: Erisa Karafili was partially supported by the UKRI HetMEPS project (UKRI257).

how human biases, cultural influences, and cognitive preferences contribute to security vulnerabilities [1]. There is a growing need for cybersecurity training approaches that both inform and engage users to support motivation, retention, and behavioural change.

Gamification emerges as a strategy to bridge this gap. By integrating game-like elements into training environments, gamification enhances engagement, facilitates deeper learning, and encourages the practical application of knowledge in simulated scenarios that mirror real-world challenges [14,25,23]. This approach is particularly effective in transforming theoretical knowledge into practical skills, enabling users to respond to dynamic cybersecurity threats.

In this paper, we introduced a novel open-source serious game for cybersecurity training, called *CyberAware* [1][2]. This gamified training promotes active learning through interactive scenarios and structured challenges, teaching cybersecurity concepts by engaging players in realistic threat responses. CyberAware is a low-resource, flexible gamified approach that engages users while improving their cybersecurity awareness and enabling knowledge tracking through pre- and post-game quizzes.

CyberAware is a cybersecurity awareness serious (online) game for a generic public from different industries (e.g., education, health) with low-medium cybersecurity knowledge. It is built on key game design features: structured learning, direct feedback, and adaptive progression, to ensure players retain knowledge and develop practical skills. These elements form the foundation of the gameplay, guiding learners through an engaging and effective learning experience. CyberAware is structured into four stages: pre-quiz, introduction, scenario-based challenges, and post-quiz. The pre- and post-quizzes benchmark learning through aligned domains and formats, while the introduction stage establishes core concepts and supports incremental learning. Players then progress to increasingly complex, problem-solving scenarios that require active application of knowledge.

In CyberAware, we use challenges as learning mechanisms. Specifically, we developed three challenges designed to address the most relevant cybersecurity threats encountered by users [9]: phishing, password strength, and social-engineering attacks. These challenges are an effective alternative in engaging users and simulating real-life scenarios [5], as they require active decision-making, ensuring that players learn through experience rather than passive instruction.

We evaluated CyberAware with a usability study, where fifteen participants were recruited from our Institution. The participants completed the game and a post-game questionnaire, allowing for both objective measurement of knowledge gains and subjective assessments of engagement and usefulness. Overall, CyberAware was well received, with 67% of participants finding the game *very* or *extremely* engaging. We used the results of the pre- and post-game quizzes to evaluate the usefulness and the knowledge gain of the users. CyberAware helped the users achieve an average increase of 41.6% of the users cybersecurity knowledge after playing one session of our game. Our comparative analysis of

[1] `https://ma1u20.itch.io/cyberaware`
[2] `https://github.com/MarwanTamimi/CyberAware`

CyberAware with respect to existing solutions showed that CyberAware supports almost all evaluation features, making it a highly competitive solution. Formal ethical approval for the study was obtained from our Institution.

This work makes three key contributions. First, it integrates structured learning, adaptive progression, and direct feedback within a short, self-contained game session to support active application of cybersecurity concepts. Second, CyberAware implements these principles through scenario-based challenges with adaptive hints and immediate feedback. Third, aligned pre- and post-game assessments enable objective measurement of learning gains within a single session.

The paper is organised as follows. Section 2 reviews related work on game-based cybersecurity training. Section 3 presents CyberAware's design and implementation, followed by the game flow in Section 4. Section 5 reports the evaluation and results, Section 6 discusses the findings, and Section 7 concludes with future work.

2 Related Work

In this section, we review the state of gamified cybersecurity training, highlighting limitations where relevant. Traditional methods face challenges that game-based learning addresses by improving effectiveness, boosting engagement, and making learning enjoyable, motivating deeper study of cybersecurity concepts [30]. It provides immediate feedback, helping users learn from mistakes and reinforcing correct behavior [27]. Additionally, it is scalable and accessible, making it a flexible and cost-effective solution for widespread cybersecurity training [6]. Game-based learning approaches facilitate rapid progress and provide a safe, nonpunishing environment for learning from mistakes [19,28,15]. They immerse learners through self-paced, engaging experiences that feel like play rather than training, while remaining low-cost, easily scalable across platforms, and effective through rewards and realistic, work-relevant scenarios. Some of the game mechanics in cybersecurity training include conflict, strategy and chance, aesthetics, theme and story, rewards, mystery, challenge, penalty, opportunity for mastery, visibility of progress, and emotional content [21].

We identified and analysed key cybersecurity training games, summarised in Table 1 with brief descriptions, target audiences, and core game mechanisms. NOVA Cybersecurity Lab Game [22] is a virtual laboratory that immerses learners in realistic, enterprise-level scenarios such as configuring firewalls, detecting intrusions, and analysing malware, with immediate feedback in a controlled environment. While this realism makes it effective for practising real-world defensive skills, it requires prior technical knowledge and may be less accessible to beginners. CyberAwareness Challenge [26] is a quiz-based program that engages users with fast-paced, scenario-driven questions on common security issues, reinforced through badges and rewards. While effective for promoting awareness and best practices, it emphasises recall and recognition rather than deeper problem-solving and may feel superficial to learners seeking more advanced, hands-on training. Cyberland [8] is an adventure and role-playing game where players

Name of the Game	Description of the Game	Target Audience	Mechanics
NOVA Cybersecurity Lab Game [22]	A virtual lab where users practice cybersecurity skills through hands-on activities and realistic scenarios.	IT professionals, students	Conflict, strategy and chance, rewards, visibility of progress, opportunity for mastery
CyberAwareness Challenge [26]	An interactive quiz game challenging users on cybersecurity practices and concepts.	General public, employees	Rewards, challenge, visibility of progress, penalty, mystery
Cyberland [8]	A role-playing game where players protect digital assets from cyber threats through missions.	Students, young professionals	Theme and story, conflict, challenge, emotional content, aesthetics
Hacknet [18]	A hacking simulation game offering a realistic experience of system intrusion and puzzle-solving.	IT enthusiasts, gamers	Conflict, strategy and chance, mystery, challenge, opportunity for mastery
Riskio [15]	A serious game teaching cybersecurity risk and management through simulated scenarios.	General public, professionals	Risk assessment, strategy and decision-making, simulation, educational feedback

Table 1: Overview of Cybersecurity Training Games

navigate a fictional world, tasked with protecting digital assets from various cyber threats. Its fictional setting might not adequately prepare players for the specific, technical challenges faced in real-world cybersecurity contexts. Hacknet [18] is a simulation game with puzzle elements, providing players with a realistic hacking experience. This game offers in-depth technical challenges, but might not fully convey the ethical considerations and broader impacts of hacking, potentially leading to a one-sided understanding of cybersecurity. Riskio [15] is a serious game focused on cybersecurity risk assessment and decision-making through simulated environments, though it could benefit from more varied and unpredictable scenarios to better reflect real-world threats.

While existing games offer valuable educational tools, many, particularly quiz-based ones, lack depth, and even challenge-based or simulation games may oversimplify cybersecurity complexity. Additionally, narrow target audiences often leave more experienced learners under-challenged.

3 Introduction to CyberAware

Let us now introduce our solution, CyberAware, which is a gamified framework designed to improve the user's security awareness. Our game focuses on three main points: structured learning, direct feedback, and adaptive progression, to ensure that players retain knowledge and develop practical skills. We divide the game into four main stages: the pre-quiz, introduction stage, scenario-based challenges, and the post-quiz. The first and last stages are quizzes that we ask the users to take in order for them to understand their learning progress. The game itself is focused on the introduction and scenario-based challenges, where structured learning and adaptive progressions are used.

Our game introduces cybersecurity threats in a controlled and progressive way. This decision was taken to allow for incremental learning for the players. In

particular, players start with fundamental concepts before moving on to more complex problem solving tasks. The introduction stage establishes a foundation of knowledge and familiarizes players with key cybersecurity risks. This approach prevents information overload and builds player confidence by allowing them to apply their knowledge before encountering more difficult challenges. After the introduction stage, the game moves into a more active stage. The game presents dynamic, scenario-based challenges that simulate real cybersecurity threats and require players to make informed decisions that directly affect their progress. Through hands-on activities in phishing detection, password security, and social engineering, players apply best practices in an interactive and realistic setting.

CyberAware includes a *direct feedback* system that responds to player actions in real-time. If a player makes a mistake, the game provides an explanation rather than a simple right/wrong response. This approach helps players understand why an answer is incorrect and how to recognize similar threats in the future. By integrating feedback into the game, the game reinforces cybersecurity principles through direct application rather than passive instruction. To maintain engagement and encourage continuous learning, the game *adapts* its difficulty based on player performance. If a player demonstrates proficiency, the challenges become more complex. If they struggle, the game offers additional guidance. This system keeps the game accessible to beginners while ensuring that experienced players remain challenged. The game also includes an *achievement system* that tracks progress and rewards players for completing cybersecurity challenges. These milestones motivate engagement while reinforcing key concepts, with achievements marking meaningful learning progress rather than serving purely as extrinsic rewards.

3.1 CyberAware Design

CyberAware was developed using a user-centered, iterative design process with regular testing and feedback to ensure accessibility, effectiveness, and alignment with user needs and learning objectives. Our game is structured around the mechanics, dynamics, and aesthetics (MDA) framework [17], a common approach in educational game design. We describe below how these three components are mapped in CyberAware:

- **Mechanics**: Players tackle bite-sized, scenario-based missions such as spotting phishing emails, hardening device settings, or triaging incidents; every action is scored instantly, with the correct choices unlocking the next tier of challenges.
- **Dynamics**: Our scenarios use a dynamic difficulty for every player (adapting to each player's capability), a countdown timer, and a point scoring loop, to add urgency to the game. A hint button is available to help learners move forward if they become stuck on a specific part.
- **Aesthetics**: A clean, comic-style interface, blue-to-red risk-level palette shifts, and an in-game mentor who delivers narrative feedback cultivate a feeling of watchful urgency while keeping the overall tone friendly and approachable.

CyberAware structures its content as progressively challenging levels. For example, the first challenge requires learners to achieve 80% accuracy in two consecutive attempts before advancing, with optional on-demand supporting hints. Players can seamlessly continue their progress across sessions, maintaining a continuous and personalised learning experience. Through this adaptive structure and real-time feedback, CyberAware effectively builds both understanding of cybersecurity threats and practical response skills for everyday situations.

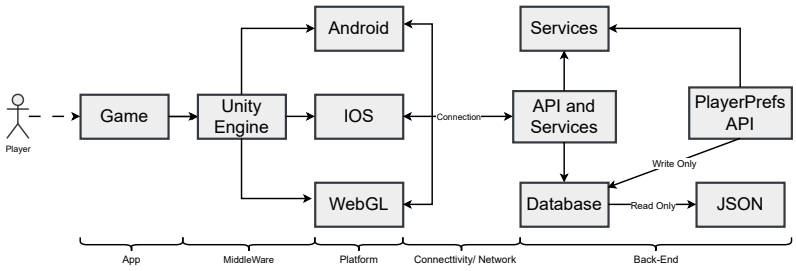

Fig. 1: CyberAware System Architecture

3.2 CyberAware Implementation

In this section, we briefly introduce the implementation of CyberAware, with a detailed system architecture shown in Figure 1. *Unity* was selected for its adaptability and WebGL deployment, enabling cross-platform, browser-based access without additional installation and supporting broad accessibility. As a cybersecurity education game, CyberAware was designed to provide a continuous and personalised learning experience through a straightforward implementation strategy. Initial game configurations are managed using JSON, while Unity's PlayerPrefs handle persistent browser-based storage of user progress, quiz results, and achievements, addressing WebGL platform constraints. This approach allows players to resume exactly where they left off, supporting continuity and reinforcing learning over time.

4 CyberAware Game Flow

Let us now provide an overview of the CyberAware game flow, as presented in Figure 2. Before starting the game, the player is asked to answer a pre-game quiz, and after the game, a post-game quiz is provided as well. The pre- and post-game quizzes were designed as integral components of CyberAware to ensure a structured and objective assessment of cybersecurity learning outcomes.

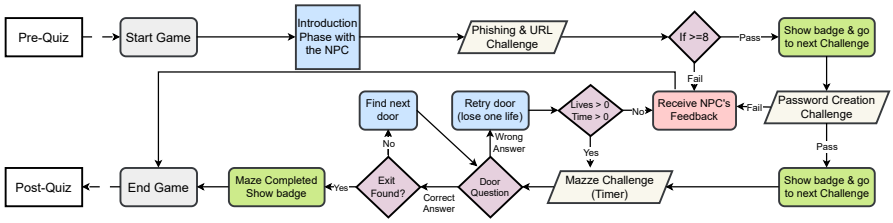

Fig. 2: CyberAware Game Flow

4.1 Pre- and Post-Game Quizzes

The pre-game quiz assesses players' baseline knowledge and identifies gaps in core cybersecurity concepts before gameplay. Both pre- and post-game quizzes use a consistent format of multiple-choice and scenario-based questions reflecting real-world challenges. Questions cover key domains such as phishing, password security, and social engineering, which are central to everyday digital interactions and are reinforced during gameplay.

After completing the interactive challenges, the post-game quiz assesses how effectively players have retained and applied the cybersecurity principles learned during gameplay. While it follows a similar format to the pre-game quiz, it introduces more complex, context-rich scenarios that emphasise analysis and real-world decision-making. This approach measures not only knowledge retention but also deeper conceptual understanding.

The pre-game quiz establishes a measurable knowledge baseline, enabling accurate comparison with post-game results to assess learning gains. Combined with post-game performance, the collected quiz data supports a comparative analysis that provides quantifiable evidence of the game's educational impact. These results can be visualised through performance trend graphs to highlight areas of improvement and remaining gaps in cybersecurity awareness.

4.2 Cybersecurity Challenges

The game begins with introductory interactions, where players are guided by non-player characters (NPCs) to their first challenge. This NPC-guided walk-through forms the concluding part of the introduction phase and acts as the bridge into the subsequent scenario-based challenges.

Upon reaching the first challenge, Phishing and URL Identification (see Figure 3 for an example), players must correctly distinguish between legitimate and malicious emails and URLs. If they achieve a minimum score threshold, they receive an achievement badge and unlock the next stage. However, if they do not meet the requirement, they are given the opportunity to either retry the challenge or receive additional guidance from an NPC. This reinforcement mechanism ensures that players are not merely progressing through trial and error but are actively learning from mistakes.

(a) Phishing challenge (b) Password creation challenge

Fig. 3: Examples of the CyberAware challenges

Following the successful completion of the first challenge, players proceed to the Password Creation Challenge (see Figure 3), where they engage with interactive elements that teach them best practices for generating strong passwords. The game dynamically adapts to the player's performance, providing immediate feedback and awarding a second achievement badge upon successful completion.

The final stage before completing the game is the Maze Challenge, which integrates various cybersecurity concepts with social engineering awareness. The players navigate a structured environment while answering questions related to cybersecurity threats. Incorrect answers prompt immediate feedback, and if the timer expires before completing the challenge, players must restart from the beginning. This mechanism adds an element of urgency while reinforcing key cybersecurity principles.

The *achievement system* in CyberAware plays a crucial role in structuring the player's progression through various cybersecurity challenges. Each challenge builds on the knowledge gained at previous levels, ensuring a gradual and meaningful learning experience. Upon completing all challenges, players reach the post-game quiz, which assesses knowledge retention and measures improvements based on their performance in the pre-game quiz. The structured progression, as illustrated in the game flow (Figure 2), ensures a clear educational pathway while maintaining player engagement through gamification techniques.

The role of NPCs. In CyberAware, NPCs provide guidance through explanations and hints, offering targeted advice when players make mistakes. This supports learning through error correction and embeds cybersecurity lessons naturally within the game narrative. For example, when a player fails to identify a phishing email, an NPC highlights suspicious cues such as urgent language or misleading links, encouraging critical thinking rather than rote memorisation. NPC guidance adapts to player performance, providing more detailed explanations after repeated failures and brief confirmations as proficiency improves.

5 Game Evaluation

In this section, we evaluate CyberAware by measuring learning outcomes, player engagement, and feedback effectiveness using pre- and post-game quizzes and a post-game questionnaire.

5.1 Evaluation Study Design

Our evaluation was designed to assess whether CyberAware can improve cybersecurity awareness through interactive gameplay and whether it is perceived as a useful and engaging learning tool by participants. Before the main study, the game was internally tested to assess instruction clarity, game logic, and interface usability, leading to final refinements of its content and structure.

The study participants were asked to complete the full game experience, beginning with a pre-game quiz, followed by gameplay, and ending with a post-game quiz and a structured feedback questionnaire. Questionnaire topics are summarised in Table 2, with the full list in Appendix A. The study examined changes in users' understanding of core cybersecurity concepts and gathered feedback on game features, e.g., feedback mechanisms, engagement, and challenge value. It used a short, single-session design and combined self-reported data with quiz results to capture both perceived learning and measurable knowledge gains.

Focus Area	**Example Questions**
Effectiveness of Learning	Was the game effective at teaching cybersecurity concepts?
Understanding of Concepts	Rate your understanding of: - Social Engineering - Phishing Emails - Suspicious URLs - Password Creation
Challenge Feedback	What could be improved in each challenge?
NPC Feedback	Was NPC feedback effective for completing the challenges?
Engagement and Enjoyment	What part of the game was most engaging? Did you enjoy the game? Would you recommend it?
Real-World Confidence	Do you feel confident applying what you learned in real life?
Behavioural Impact	Are you more likely to take cybersecurity precautions after playing?

Table 2: Summary of the Questionnaire Topics

Study Realisation For our evaluation study, we recruited fifteen participants from our Institution (all being undergraduate students in the Engineering or Computer Science fields). Participants were recruited via students' communication

channels, and no preselection was applied. Students were selected as they typically have mixed but non-expert levels of cybersecurity knowledge, which reflects the intended target audience for CyberAware. We obtained formal Ethical approval for this study through the University's Ethics and Research Governance Online (ERGO) system. All participants gave informed consent in line with university requirements. No personal or sensitive data were collected, and all data were stored securely in accordance with ERGO guidelines. Participants accessed the game from their own devices and completed the evaluation independently. The study required no supervision and was designed to run in a single sitting. The estimated total time for completion was around 20 to 30 minutes.

5.2 Evaluation Study Results

The results from the questionnaire and the comparison between pre- and post-game quizzes' scores provide insight into the effectiveness of CyberAware as a cybersecurity awareness tool. Our analysis focuses on four areas: knowledge improvement, concept understanding, engagement, and impact.

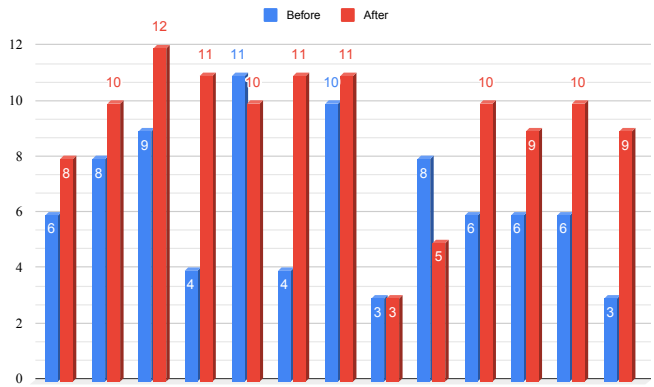

Fig. 4: Pre- and Post-game Quizzes

Knowledge Improvement: Participants demonstrated a measurable improvement in cybersecurity knowledge. Pre- and post-game quizzes showed an average *knowledge improvement* of 41.6% after a single session (see Figure 4), with correct responses increasing from 53.8% to 76.2% (for 13 participants[3]). This result suggests that the game's interactive format helped reinforce learning.

[3] Two participants were excluded from the final average due to identical low scores in both quizzes and indications of disengagement during their pre- and post-game quizzes. If we were to count also these two participants, the knowledge improvement remains 41.6%, with correct responses increasing from 46.6% to 66%.

Concept Understanding: Figure 5 shows self-rated concept understanding after gameplay: 40% reported significant improvement, 30% moderate improvement, 30% slight improvement, and none reported no improvement. Improvements were observed across all four domains: social engineering, phishing emails, suspicious URLs, and password creation, with the strongest gains in phishing recognition and password creation, where challenges were scenario-based and tied to real-world decisions.

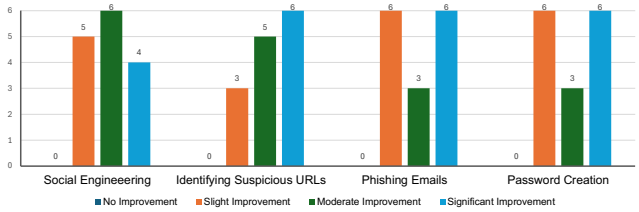

Fig. 5: Improvement of Cybersecurity Understanding After Playing CyberAware

Game Engagement: The feedback of the participants on the engagement and enjoyment was positive (see Table 3). In particular, two-thirds of the users found the challenge-based structure to be the most engaging feature. This supports our focus on tight hands-on tasks rather than narrative-heavy content. Furthermore, two-thirds of the users found the game "very" or "extremely" engaging, while more than half of the users found the overall experience "very" or "extremely" enjoyable, and no participants found the game not engaging or not enjoyable.

Game Impact: After the study, 93.3% of participants (14 out of 15) reported being more likely to take protective steps against cybersecurity threats (answering "yes" to the *Intent to adopt safer behaviour* question), and 12 of them expressed confidence in applying their new knowledge in real-world situations.

Most-Engaging Game Aspect			Self-Reported Engagement			Overall Enjoyment		
Aspect	Count	%	Rating	Count	%	Rating	Count	%
Challenges	10	66.7	Extremely engaging	3	20.0	Extremely enjoyable	4	26.7
Exploring the world	2	13.3	Very engaging	7	46.7	Very enjoyable	4	26.7
Visual design	2	13.3	Moderately engaging	3	20.0	Slightly enjoyable	4	26.7
Story	1	6.7	Slightly engaging	2	13.3	Moderately enjoyable	3	20.0
			Not engaging	0	0.0	Not enjoyable	0	0.0

Table 3: Feedback on Game Engagement ($n = 15$)

5.3 Summary of Findings

Across the fifteen participants, *CyberAware* produced a mean post-quiz score that was 41.6% higher than the pre-quiz baseline, indicating substantial short-term knowledge improvements. The self-rated scores showed improvements in concept understanding for the four targeted domains: phishing identification, suspicious URL detection, social engineering awareness, and password creation, with the greatest perceived growth in phishing recognition and password skills (Figure 5). The engagement metrics were also encouraging: 67% of the respondents selected the challenge-based structure as the most engaging element, and 67% rated the game *"very"* or *"extremely"* engaging (Table 3). Finally, 93% reported they are *more likely* to adopt safer online practices after playing. Additionally, all participants reported that NPC-provided information supported task completion, with open comments noting that adaptive guidance enhanced immersion rather than disrupting gameplay.

6 Discussion

In this section, we further discuss CyberAware main components, its limitations, and compare it with other existing game-based security training.

CyberAware showed a 41.6% average score of knowledge increase through the pre- and post-game quizzes. As both quizzes used identical domains and formats, the gains reflect genuine concept uptake within a single session. All participants reported that NPC-provided information supported task completion, and the adaptive system effectively balanced guidance for novices with pacing for advanced players. CyberAware's challenges showed varied learning outcomes. The phishing and URL identification challenge produced the largest post-quiz gains, though about 20% still misclassified at least one spear-phishing email. The password-creation challenge reinforced rules through enforced iteration and was highly motivating, despite some frustration with retries. The hybrid maze challenge combined navigation and decision-making, ranking lowest in ease but highest in engagement, suggesting time-bounded tasks can boost attention when restarts are fair. In addition, CyberAware shows strong real-world transfer, with 93% of participants reporting increased likelihood of adopting safer online habits. While self-reported intent is not direct evidence of behaviour change, it aligns with gains in quiz scores and self-rated confidence.

Game / Feature	**Multi-platform**	**Educational**	**Hints & Tips**	**Accessible**	**Multiple Audiences**	**Flexible**
NOVA Cybersecurity Lab Game[22]	✓	✓	✓	✓		
Cyber Awareness Challenge[26]		✓	✓	✓		
Cyberland[8]	✓	✓	✓	✓	✓	✓
Hacknet[18]	✓	✓				
Riskio[15]	✓	✓	✓	✓	✓	
CyberAware		✓	✓	✓	✓	✓

Table 4: Analysis of the Game-Based Features

We now analyse how CyberAware compares with other game-based security training, using the following six evaluation features[4]: (1) **Multi-platform Accessibility**: Availability across platforms such as PC and web; (2) **Educational Integration**: Embeds structured learning within gameplay; (3) **Hints & Tips**: Provides in-game guidance to support learning; (4) **Accessibility**: Free and easily accessible online; (5) **Multiple Audiences**: Suitable for diverse ages and occupations; (6) **Flexibility**: Supports adding new scenarios and gamified topics. Table 4 compares CyberAware with existing game-based training approaches (Section 2) using the evaluation features described above. Cyberland is the only game supporting all evaluated features, engaging a broad age range, and using more extensive resources than CyberAware. CyberAware supports all features except multi-platform deployment, primarily due to resource constraints, and thus remains a comprehensive game-based cybersecurity training solution.

Furthermore, we analyse CyberAware using the Learning Mechanics–Game Mechanics (LM–GM) framework [20,2,4] as a post hoc analysis to clarify the relationship between gameplay and learning. The analysis shows how scenario-based challenges, NPC feedback, and structured progression support applied decision-making, reflection, guidance and progression, while aligned pre- and post-game quizzes provide quantitative evidence of short-term learning gains (see Appendix B).

7 Conclusion and Future Work

In this paper, we presented CyberAware, a free and open-source online serious game for cybersecurity awareness, and demonstrated how a human-centered, adaptive gamification approach can support engagement and learning. CyberAware addresses common daily threats (phishing, password creation, and social engineering) within a single 30-minute browser-based session, using hands-on challenges. Learning is reinforced through real-time NPC feedback and achievement based rewards that maintain engagement while supporting meaningful learning. CyberAware has pre- and post-game quizzes for the users, in order for them to immediately evaluate their progress. Our evaluation shows a 41.6% average knowledge gain, with two-thirds of participants rating the game as very or extremely engaging, indicating the effectiveness of our scenario-based training. Compared with existing game-based trainings, CyberAware matches key strengths in educational focus, feedback, accessibility, and flexibility, while offering shorter playtime and no installation requirements.

Future work includes extending CyberAware with additional scenarios covering broader cybersecurity areas, evaluating the game with larger and more diverse participant groups (e.g., by age, experience, and sector), and exploring integration with existing cybersecurity training platforms. We also plan to package the WebGL build into lightweight Android, iOS, and desktop wrappers to improve multi-platform support without sacrificing browser accessibility.

[4] Another interesting evaluation feature was *supporting online matchmaking with multiplayer*. We omitted this feature as none of the analysed games supported it.

References

1. Aldawood, H., Skinner, G.: Reviewing cyber security social engineering training and awareness programs - Pitfalls and ongoing issues. Future internet **11**(3), 73 (2019)
2. Arnab, S., Lim, T., Carvalho, M.B., Bellotti, F., De Freitas, S., Louchart, S., Suttie, N., Berta, R., De Gloria, A.: Mapping learning and game mechanics for serious games analysis. British Journal of Educational Technology **46**(2), 391–411 (2015)
3. Bada, M., Nurse, J.R.: Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security **27**(3), 393–410 (2019)
4. Callaghan, M., Savin-Baden, M., McShane, N., Eguiluz, A.G.: Mapping learning and game mechanics for serious games analysis in engineering education. IEEE Transactions on Emerging Topics in Computing **5**(1), 77–83 (2015)
5. Canham, M., Posey, C., Constantino, M.: Phish derby: Shoring the human shield through gamified phishing attacks. In: Frontiers in Education. vol. 6, p. 807277. Frontiers (2022)
6. Connolly, T.M., Boyle, E.A., MacArthur, E., Hainey, T., Boyle, J.M.: A systematic literature review of empirical evidence on computer games and serious games. Computers & education **59**(2), 661–686 (2012)
7. Corbett, J., Karafili, E.: Private data harvesting on alexa using third-party skills. In: International Workshop on Emerging Technologies for Authorization and Authentication. pp. 127–142 (2021)
8. Cyber Games UK: Cyber Games UK, `https://cybergamesuk.com/`
9. Ferro, L.S., Sapio, F.: Another week at the office (awato) – an interactive serious game for threat modeling human factors. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and Trust. pp. 123–142 (2020)
10. Fuertes, W., Arévalo, D., Castro, J.D., Ron, M., Estrada, C.A., Andrade, R., Peña, F.F., Benavides, E.: Impact of social engineering attacks: A literature review. In: Rocha, Á., Fajardo-Toro, C.H., Rodríguez, J.M.R. (eds.) Developments and Advances in Defense and Security. pp. 25–35 (2022)
11. Gokkaya, B., Aniello, L., Karafili, E., Halak, B.: A methodology for cybersecurity risk assessment in supply chains. In: European Symposium on Research in Computer Security. pp. 26–41. Springer (2023)
12. Gokkaya, B., Karafili, E., Aniello, L., Halak, B.: Global supply chains security: a comparative analysis of emerging threats and traceability solutions. Benchmarking: An International Journal **32**(3), 917–942 (2025)
13. Gwenhure, A.K., Rahayu, F.S.: Gamification of cybersecurity awareness for non-it professionals: A systematic literature review. International Journal of Serious Games **11**(1), 83–99 (2024)
14. Hakak, S., Noor, N.F.M., Ayub, M.N., Affal, H., Hussin, N., Imran, M., et al.: Cloud-assisted gamification for education and learning–recent advances and challenges. Computers & Electrical Engineering **74**, 22–34 (2019)
15. Hart, S., Margheri, A., Paci, F., Sassone, V.: Riskio: A serious game for cyber security awareness and education. Computers & Security **95**, 101827 (2020)
16. Hoad, T., Karafili, E.: A web browser plugin for users' security awareness. In: Proceedings of the 19th International Conference on Availability, Reliability and Security. pp. 1–7 (2024)

17. Hunicke, R., LeBlanc, M., Zubek, R., et al.: Mda: A formal approach to game design and game research. In: Proceedings of the AAAI Workshop on Challenges in Game AI. vol. 4, p. 1722. San Jose, CA (2004)
18. itch.io: Hacknet educational license by fellow traveller, https://fellowtraveller.itch.io/hacknet-edicational-license
19. Jøsang, A., Stray, V., Rygge, H.: Threat poker: Gamification of secure agile. In: IFIP WG 11.8 World Conference Information Security Education. pp. 142–155 (2020)
20. Lim, T., Carvalho, M.B., Bellotti, F., Arnab, S., De Freitas, S., Louchart, S., Suttie, N., Berta, R., De Gloria, A.: The lm-gm framework for serious games analysis. Pittsburgh: University of Pittsburgh (2015)
21. Onduto, B., Ali, R., Smed, A.: Gamification of cyber security awareness–a systematic review of games. Computing, Faculty of Technology (2021)
22. Pbs.org: NOVA Labs, https://www.pbs.org/wgbh/nova/labs/lab/cyber/
23. Pramod, D.: Gamification in cybersecurity education; a state of the art review and research agenda. Journal of Applied Research in Higher Education **17**(4), 1162–1180 (2025)
24. Prümmer, J., van Steen, T., van den Berg, B.: A systematic review of current cybersecurity training methods. Computers & Security **136**, 103585 (2024)
25. Reyssier, S., Hallifax, S., Serna, A., Marty, J.C., Simonian, S., Lavoué, E.: The impact of game elements on learner motivation: Influence of initial motivation and player profile. IEEE Transactions on Learning Technologies **15**(1), 42–54 (2022)
26. Serious Games Showcase & Challenge: Cyber Awareness Challenge - Serious Games Showcase & Challenge, https://sgschallenge.org/game/cyber-awareness-challenge/
27. Shute, V.J.: Focus on formative feedback. Review of educational research **78**(1), 153–189 (2008)
28. Tioh, J.N., Mina, M., Jacobson, D.W.: Cyber security training a survey of serious games in cyber security. In: 2017 IEEE Frontiers in Education Conference (FIE). pp. 1–5. IEEE (2017)
29. Valenza, F., Karafili, E., Steiner, R.V., Lupu, E.C.: A hybrid threat model for smart systems. IEEE Transactions on Dependable and Secure Computing **20**(5), 4403–4417 (2022)
30. Whitton, N.: The place of game-based learning in an age of austerity. Electronic Journal of e-Learning **10**(2), pp249–256 (2012)
31. Wilcox, H., Bhattacharya, M.: Countering social engineering through social media: An enterprise security perspective. In: ICCCI. pp. 54–64 (2015)

A Questionnaire

This section presents the questions asked to users after playing CyberAware.

1. Do you believe the game was effective at teaching cybersecurity concepts?
2. How effectively did the game convey the risks associated with social engineering attacks?
3. After playing the game, rate your understanding of the following cybersecurity concepts: **Social Engineering**
4. After playing the game, rate your understanding of the following cybersecurity concepts: **Identifying Suspicious URLs**

5. After playing the game, rate your understanding of the following cybersecurity concepts: **Phishing Emails**
6. After playing the game, rate your understanding of the following cybersecurity concepts: **Password Creation**
7. What could be improved in the Phishing Email challenge?
8. What could be improved in the Identifying Suspicious URLs challenge?
9. What could be improved in the Password Creation challenge?
10. What could be improved in the Maze Quiz challenge?
11. What could be improved for feedback given by the NPCs?
12. Was the feedback given by the NPC effective to pass the challenges?
13. Which aspect of the game did you find most engaging?
14. Did you find the game engaging?
15. Did you find overall enjoyment of playing the game?
16. After completing the game, do you feel confident enough to apply it in real-world situations?
17. Are there any improvements that could be made to make the game more engaging, or improve its enjoyment?
18. Are you more likely to take actions to protect yourself from these attacks after playing the game?
19. Was the game ever laggy or slow to respond during your playthrough?
20. How would you rate the overall performance of the game (e.g., loading times, responsiveness, smoothness of gameplay)?
21. Do you believe the game could benefit from performance and stability improvements?

B LM-GM Analysis of CyberAware

We provide in this appendix a post hoc analysis of CyberAware using the LM-GM framework [20,2,4] to make explicit the relationship between gameplay mechanics and learning processes.

Learning Mechanics	**Game Mechanics in CyberAware**
Assessment	Aligned pre- and post-game quizzes measuring the same cybersecurity domains to capture short-term learning gains.
Guidance / Progression	Structured progression from introductory content to increasingly complex challenges, supported by adaptive difficulty.
Repetition /Action	Scenario-based challenges requiring repeated application of phishing, password creation, and social engineering concepts.
Feedback / Reflection	Immediate, explanatory feedback delivered via non-player characters (NPCs).
Adaptation	Performance-based hints and guidance, adjusting to player proficiency.
Motivation	Achievement milestones and progress tracking, reinforcing meaningful learning outcomes.

Table 5: Post hoc LM-GM mapping for CyberAware