Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Gamified Cybersecurity Awareness System: An Interactive Approach to Digital Safety

Mitali Chopade
Department of Artificial Intelligence and Data Science
A. C. Patil College of Engineering, University of Mumbai

Samiksha Patil
Department of Artificial Intelligence and Data Science
A. C. Patil College of Engineering, University of Mumbai

Dr. (Mrs) Jaya Terdale
Department of Artificial Intelligence and Data Science
A. C. Patil College of Engineering, University of Mumbai

Sakshi More
Department of Artificial Intelligence and Data Science
A. C. Patil College of Engineering, University of Mumbai

Mayuri Gote
Department of Artificial Intelligence and Data Science
A. C. Patil College of Engineering, University of Mumbai

Abstract **- In the present digital era, cybercrimes such as phishing, ransomware, and social engineering are rapidly increasing, yet user unawareness remains a leading cause of data breaches. Traditional cybersecurity awareness programs often fail to hold learners' attention, resulting in poor knowledge retention and minimal behavioural change. To overcome this limitation, this paper proposes a Gamified Cybersecurity Awareness System, a dynamic platform designed to educate users through engaging gamification techniques. The system transforms theoretical concepts into practical challenges, utilizing a chatbot-based tutor to guide users in identifying threats. By integrating game mechanics like points, badges, and leader boards, the system fosters motivation and healthy competition. Designed to be inclusive and scalable, it aims to cultivate a culture of cybersecurity awareness, empowering individuals to navigate the online world safely.**

Keywords**— Gamification, Cybersecurity, Awareness, Interactive Learning, Chatbot, Phishing, Social Engineering.**

I. INTRODUCTION

Cybersecurity has emerged as a critical concern globally. According to CERT-In, incidents of phishing and digital fraud have risen exponentially. While security software exists, the "human element" remains the weakest link, with over 90% of breaches attributed to human error.

In digital ecosystem, the integration of internet-based services into financial, professional, and personal domains has expanded the attack surface for malicious actors Empirical studies indicate that a significant majority of cybersecurity breaches often exceeding 90% are precipitated by human error rather than technical failures, with users frequently falling victim to social engineering, phishing, and weak credential management. Consequently, cybersecurity awareness has transitioned from a specialized requirement to a fundamental digital literacy skill.

Despite the urgency of this requirement, conventional approaches to cybersecurity training are characterized by passive lectures, static documentation, and compliance-based workshops that often fail to foster active engagement or long-term knowledge retention. These traditional models prioritize theoretical memorization over practical application, leaving users ill-equipped to identify and neutralize sophisticated real-world threats. To address these limitations, this research presents a Gamified Cybersecurity Awareness System, a web-based platform that synthesizes Security Education, Training, and Awareness (SETA) principles with interactive game mechanics.

Moreover, this research addresses the critical need for an inclusive and actionable safety tool. Recognizing that digital threats target individuals across all age groups and technical backgrounds, the system is designed to be accessible to a diverse demographic, including students and senior citizens who are often disproportionately vulnerable. Uniquely, the platform extends beyond education by integrating direct pathways to national incident reporting mechanisms, thereby empowering users to translate their awareness into real-world remedial action.

A. Motivation

The primary motivation for this research stems from the persistent disconnect between theoretical cybersecurity knowledge and its practical application. A notable real-world incident involving employees at a pharmaceutical company, who were deceived by fraudulent HR emails during salary increments, illustrates that even educated professionals remain vulnerable to social engineering. This example underscores that traditional, passive awareness methods are insufficient against sophisticated psychological manipulation, highlighting a critical need for training that focuses on behavioural change rather than simple memorization.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

The project is driven by the potential of gamification to transform security education from a passive obligation into an active, immersive experience. By replacing static content with interactive challenges and immediate feedback, the system aims to build the "muscle memory" required for threat detection. The ultimate goal is to democratize digital safety, creating an accessible tool that empowers users of all backgrounds—from students to confidently recognize and neutralize online threats.

B. Problem Statement

In the rapidly digitizing landscape of India, a significant portion of the population particularly youth and non-technical users struggles to identify and respond to online threats in real-life situations. While technological security measures have advanced, studies indicate that the majority of successful cyberattacks are facilitated by human error and a lack of awareness rather than technical deficiencies.

The core of the problem lies in the inadequacy of existing educational methodologies. Traditional cybersecurity training, often delivered through static lectures, text-heavy courses, or passive workshops, fails to capture learner attention or simulate the pressure of actual decision-making. This passive approach results in poor engagement and low knowledge retention, leaving users vulnerable to sophisticated attacks such as social engineering and phishing. Consequently, there is an urgent need for a smarter, more relatable, and engaging pedagogical approach that not only imparts theoretical knowledge but actively transforms how individuals think, respond, and act when facing digital threats.

C. Objectives

The primary objective of this project is to develop an interactive Gamified Cybersecurity Awareness System that bridges the gap between theoretical knowledge and real-world application. The specific objectives are as follows:

- To design an interactive web-based platform that utilizes gamification to enhance user engagement and motivation.
- To integrate an intelligent Chatbot tutor that provides real-time guidance and corrective feedback during challenges.
- To implement realistic simulations of critical threats, such as phishing and malware, for safe, hands-on practice.
- To employ a structured pre-test and post-test framework to quantifiably measure knowledge retention and improvement.
- To bridge the gap to real-world action by integrating a direct SOS link to CERT-In for reporting cyber incidents.

II. LITERATURE SURVEY

Women's safety has emerged as a critical social and techno-logical concern due to the increasing number of harassments, assault, and violence-related incidents worldwide.

Sr no.	Paper Name	Publication Year	Advantages	Disadvantages	Technologies Used	Future Scope
1	Cyber-Hero: A Gamification Framework for Cyber Security Awareness for High School Students	May 2021	Three-phase approach (Pre-test, Gamified Training, Post-test) ensures learning assessment and progress tracking. Works on any browser and operating system. Improves cybersecurity skills such as strong password creation.	Focuses mainly on password generation; other cyber threats are not covered.	Construct3 game development toolkit	Extend framework to include phishing, malware, plagiarism, and other cyber threats.
2	A Novel SETA-Based Gamification Framework to Raise Cybersecurity Awareness	August 2021	Covers multiple threats such as passwords, phishing, social engineering, and physical security. Simulates real workplace threats. Pre- and post-survey results show 51% improvement in awareness.	Basic design with limited graphics and interactivity. Tested on only 10 employees.	Python (PyCharm IDE), HTML, CSS, JavaScript, SQLite3	Integrate chatbot for real-time feedback. Add advanced levels such as remote-work security and email security.
3	Gamification-Based Cybersecurity Awareness Course for Self-Regulated Learning	April 2023	Implemented on Moodle LMS. Structured learning ensures practice and reflection. Supports self-regulated learning environment.	Depends heavily on learner self-motivation. Gamification elements may lose effectiveness over time.	Moodle LMS and gamification plugins	Continuous topic updates for emerging cyber threats. Full-scale Moodle implementation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Sr no.	Paper Name	Publication Year	Advantages	Disadvantages	Technologies Used	Future Scope
4	AI-Powered Personalized Learning Platforms for Enhancing Cybersecurity Education	2025	Provides personalized learning paths. Improves motivation using adaptive gamification. Includes virtual labs and simulations. Highly scalable.	Privacy concerns due to sensitive data collection. Risk of AI bias. Requires strong internet connectivity and devices.	Artificial Intelligence, Machine Learning, NLP, Predictive Analytics, Adaptive Learning Systems	Apply deep learning for better personalization. Improve transparency and fairness in AI models.
5	A Serious Game for Simulating Cyberattacks to Teach Cybersecurity	2023	Learners experience attacks as attackers, increasing engagement. Covers phishing, SQL injection, and USB attacks. Safe environment for practice.	No evidence of long-term learning. Limited scenarios. Complex 3D design may confuse non-gamers.	Nmap, Metasploit, SocialPhish; NIST Cybersecurity Framework	Add ransomware scenarios. Simplify visuals using 2D interfaces.
6	CyberMoraba – A Game-Based Approach Enhancing Cybersecurity Awareness	2023	Combines traditional African board game with cybersecurity concepts. Encourages strategy, competition, and interaction. Positive student feedback.	Tested only with students. Cultural impact not measured. Basic graphics and interaction. Desktop-dependent setup.	Morabaraba game logic, Visual Studio IDE, C#, GUI with attacker/defender tokens	Introduce 3D levels and complex challenges. Use ML to analyze gameplay. Validate with professionals and diverse users.
7	Learning Cyber Security Through Gamification	2015	Enhances student engagement through game-based learning. Provides practical cybersecurity training using real attack-defense scenarios. Improves problem-solving and hands-on security skills.	Limited long-term learning evaluation. Requires technical infrastructure setup. Mainly focused on competition environment.	MongoDB, Memcached, Flask Framework, Virtual Machines, Game Server	Integrate AI-driven adaptive learning, improve scalability, and include real-world cyberattack simulations.
8	Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review	2024	Increases cybersecurity awareness among non-IT users. Improves motivation and participation using storytelling and leaderboards. Encourages behavioral change and better knowledge retention. Makes training more interactive than traditional methods.	Lack of long-term effectiveness analysis. Limited empirical validation. Individual game element impact not clearly measured	Learning Management Systems, Gamification Models, Behavioral Theories (SDT), Interactive Platforms	Develop personalized gamification strategies and conduct long-term engagement studies.
9	Raising Cybersecurity Awareness in an Engaging Way Using Gamification and AI Tips	2025	Improves threat detection accuracy using AI nudging. Reduces risky online behavior among social media users. Provides real-time guidance for safer decisions. Enhances engagement through interactive gamified learning.	Requires continuous AI model updates. Engagement sustainability challenges. Legal awareness integration still developing.	AI Nudging System, NLP, TensorFlow Lite, Gamification Engine, Firebase, SQLite	Add personalization engine, multilingual support, offline access, and long-term behavioral analysis.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Sr no.	Paper Name	Publication Year	Advantages	Disadvantages	Technologies Used	Future Scope
10	Cybersecurity Education Using Gamification: Systematic Literature Review	2025	Enhances learner engagement through interactive game elements such as points, badges, and leaderboards. Improves cybersecurity knowledge retention and motivation. Supports personalized and adaptive learning environments.	Over-reliance on rewards may reduce intrinsic motivation. Limited implementation in corporate training environments. Requires proper game design for effectiveness. Long-term behavioral impact still needs evaluation.	Web-based Platforms, Application-based Systems, Tabletop Games, PRISMA Methodology, Publish or Perish Tool, Scopus & Semantic Scholar Databases	Develope adaptive personalized gamification systems, expand usage in industry training, conduct long-term effectiveness studies, and improve scalable cybersecurity awareness platforms.

A. Limitations of Existing Systems

Despite the growing popularity of gamified learning, current cybersecurity awareness platforms exhibit several critical limitations:

- **Limited Threat Coverage:** Most existing systems focus narrowly on specific topics, such as password security or phishing, while neglecting broader and equally critical threats like malware, ransomware, and social engineering.
- **Simplistic Gamification:** Many platforms rely solely on basic game mechanics like points and badges. They lack advanced engagement features such as adaptive difficulty, real-time interactive challenges, or intelligent chatbot-based guidance, which reduces long-term user motivation.
- **Small-Scale Evaluations:** A significant number of studies are validated on small groups (fewer than 30 participants), often limited to students or employees of a single organization. This makes it difficult to generalize their effectiveness to a wider, diverse population.
- **Platform Dependency:** Many solutions are confined to specific environments like Moodle LMS or desktop applications. This restricts accessibility for users who prefer flexible, cross-platform access via mobile devices and web browsers.
- **Lack of Real-World Integration:** Perhaps the most significant limitation is the disconnect between theory and action. Very few systems link awareness training to practical real-world outcomes, such as incident reporting mechanisms (e.g., CERT-In), limiting the translation of awareness into protective behavior.

III. METHODOLOGY

A. Proposed System Overview

The proposed system, the Gamified Cybersecurity Awareness System, is an interactive web-based educational platform designed to provide active learning, real-time threat simulation, and intelligent guidance for users of all technical backgrounds. The system integrates Gamification mechanics, Natural Language Processing (NLP), Heuristic Analysis, and Procedural Generation to ensure engaging and effective cybersecurity training.

Unlike conventional cybersecurity training methods that rely primarily on passive lectures and static text-based content, the proposed system supports multiple active learning modules such as algorithmic password strength analysis, collision-based phishing detection, and arcade-style malware defense. Upon encountering difficulty, an intelligent Chatbot Tutor provides real-time hints and corrective feedback, while a dedicated SOS feature allows users to immediately report actual incidents to national cybersecurity authorities (CERT-In).

B. System Architecture

The overall architecture of the proposed system is illustrated in Fig. 1. The application adopts a modular client-server structure to ensure scalability and cross-platform accessibility. The system initializes by loading the user dashboard and activating the core game engine powered by the HTML5 Canvas and Web Audio API. User interactions are continuously processed by the backend logic, and based on the selected module, specific algorithms (such as Regex-based heuristics or Euclidean distance formulas) are executed.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

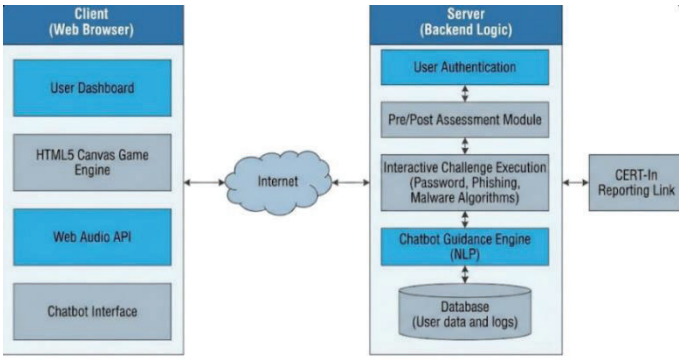

Fig. 1. System Architecture Gamified Cybersecurity Awareness System

The architecture supports User Registration, Pre-Assessment, Interactive Challenge Execution (Password, Phishing, Malware), Chatbot Guidance, and Post-Assessment evaluation. The system is designed to operate seamlessly on standard web browsers, ensuring widespread accessibility without specialized hardware.

C. Data Flow Diagram

To better understand system interactions, data flow diagrams (DFD) are used to represent information movement within the system.

1) Level 0 Data Flow Diagram: Fig. 2 illustrates the Level 0 DFD, which provides a high-level view of the interaction between the user, the safety application, emergency services, family members, and the legal database.

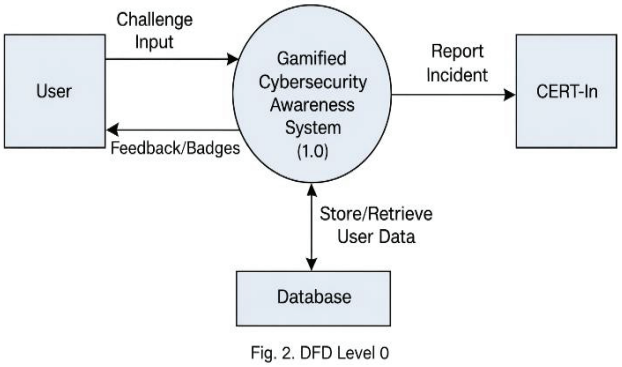

Fig. 2. DFD Level 0

Fig. 2. DFD Level 0

A System Development Approach Level 1 and Level 2 Data Flow Diagram: Fig. 3 and Fig. 4 illustrate the detailed functioning of the Gamified Cybersecurity Awareness System, including user management, challenge execution, gamified feedback, and incident reporting processes. These diagrams demonstrate how user interactions activate different system modules and how data flows between users, databases, and external authorities such as CERT-In.

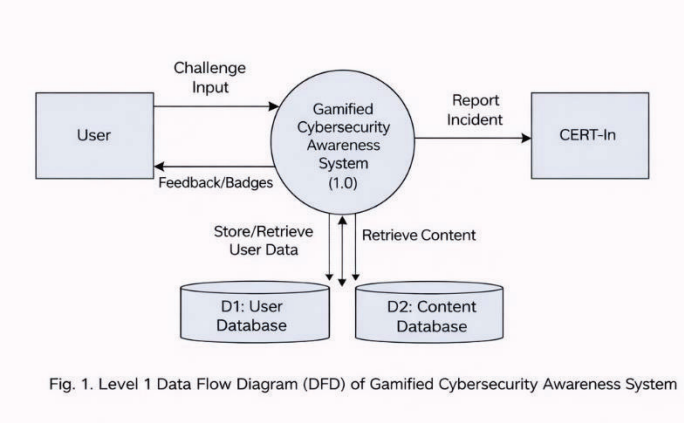

Fig. 1. Level 1 Data Flow Diagram (DFD) of Gamified Cybersecurity Awareness System

Fig. 3. DFD Level 1

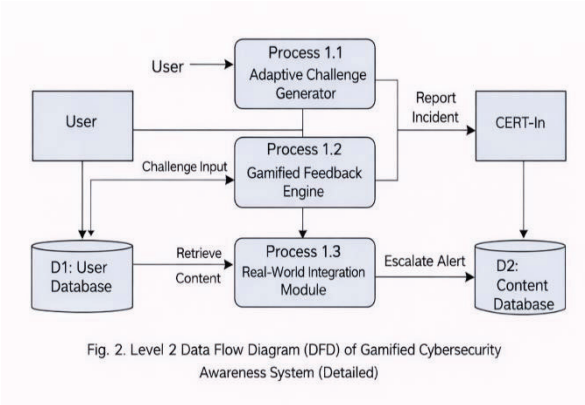

Fig. 2. Level 2 Data Flow Diagram (DFD) of Gamified Cybersecurity Awareness System (Detailed)

Fig. 4. DFD Level 2

The development of the proposed Gamified Cybersecurity Awareness System follows the Software Development Life Cycle (SDLC) methodology to ensure system reliability, scalability, and effective performance. The major phases involved include requirement analysis, system design, implementation, testing, deployment, and maintenance.

The system adopts a modular client–server architecture in which components such as user authentication, interactive cybersecurity challenge execution, gamification and feedback management, chatbot-based guidance, and incident reporting operate independently while maintaining seamless coordination. This modular approach enhances system flexibility, enables efficient data processing, and supports future expansion for incorporating advanced cybersecurity scenarios and adaptive learning mechanisms.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

B. Operational Algorithm

The operational flow of the proposed system is summarized as follows:

1. The system initializes core services including user authentication, database connectivity, and game engine modules.
2. The user registers or logs into the platform to access cybersecurity learning modules and assessments.
3. Based on user selection, the system loads interactive cybersecurity challenges such as phishing detection, password strength analysis, or malware awareness simulations.
4. User responses during challenges are continuously monitored and evaluated by the backend processing module.
5. The gamification engine calculates performance scores and generates rewards such as points, badges, and leaderboard rankings.
6. An intelligent chatbot module provides real-time guidance, hints, and corrective feedback to enhance user understanding.
7. User progress and performance data are stored in the database for analysis and future learning recommendations.
8. In case of real-world cyber incidents, users can report threats through the integrated CERT-In reporting feature.

The system operates continuously during user interaction to ensure active learning, performance tracking, and effective cybersecurity awareness training.

IV. RESULTS AND DISCUSSION

The proposed **Gamified Cybersecurity Awareness System** was evaluated based on its functionality, user engagement, and learning effectiveness during interactive cybersecurity training sessions. The evaluation focused on key features such as gamified challenge execution, real-time feedback generation, performance assessment, and cybersecurity incident reporting integrationUser interaction analysis indicated improved engagement levels compared to traditional awareness methods. The platform efficiently tracked user progress through continuous performance monitoring. Additionally, the system maintained stable responsiveness during multiple user interactions, ensuring uninterrupted learning experiences. The overall evaluation confirmed the system's capability to enhance cybersecurity awareness and promote secure online behavior among users.

A. Functional Evaluation

The system was tested on web-based platforms under different user interaction scenarios to evaluate its functionality and performance. The gamified learning modules successfully executed cybersecurity challenges such as phishing detection, password strength analysis, and malware awareness simulations. The system accurately evaluated user responses and generated real-time feedback along with scores, badges, and leaderboard updates. The chatbot module effectively provided guidance and corrective suggestions during challenges, improving user understanding. Additionally, user performance data was securely stored in the database, and the incident reporting feature enabled users to submit cybersecurity threats through the integrated CERT-In link, ensuring practical applicability of learned concepts.

B. Response Time Analysis

Response time was measured from the moment a user initiated a cybersecurity challenge to the generation of system feedback and performance results. The system demonstrated minimal delay in loading interactive simulations and evaluating user responses under stable internet connectivity. Real-time feedback and score updates were generated efficiently, ensuring smooth user interaction during learning activities. The chatbot guidance module responded promptly to user queries, providing instant hints and corrective suggestions. Efficient backend processing and database communication reduced system latency, thereby enhancing overall user experience and maintaining continuous engagement throughout the training process.

C. AI-Based Chatbot Assistance Performance

The AI and NLP-based chatbot module processed user queries related to cybersecurity threats and provided relevant guidance based on contextual understanding. The chatbot assisted users during interactive challenges by offering real-time hints, explanations, and corrective feedback for identified mistakes. This feature enhanced user learning by simplifying complex cybersecurity concepts and improving threat recognition skills. The intelligent assistance mechanism promoted better decision-making and increased user confidence in identifying and responding to potential cyber risks.

D. Comparative Discussion

Compared to traditional cybersecurity awareness methods, the proposed system offers several improvements:

• Interactive gamified learning instead of passive lecture-based training.
• Real-time feedback and performance evaluation through game-based challenges.
•Direct cybersecurity incident reporting through CERT-In integration.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

These improvements contribute to enhanced user engagement, better knowledge retention, and respond to real-world cybersecurity threats.

E. Discussion

The results indicate that integrating gamification techniques, artificial intelligence, and NLP-based chatbot assistance into a unified cybersecurity learning platform significantly enhances user engagement and learning effectiveness. The interactive challenge-based approach improves users' ability to recognize and respond to common cyber threats in a practical environment. While the current implementation focuses on web-based deployment, further enhancements such as adaptive learning models and mobile platform integration can improve accessibility and scalability.

Overall, the proposed Gamified Cybersecurity Awareness System demonstrates strong potential as an effective, intelligent, and user-centric solution for promoting cybersecurity awareness and safe online behavior.

V. CONCLUSION AND FUTURE WORK

This paper presented the **Gamified Cybersecurity Awareness System**, which successfully achieves its objective of enhancing cybersecurity awareness through an interactive and engaging learning approach. The developed web-based platform provides an effective solution for educating users about cyber threats by incorporating gamified challenges, real-time feedback, and performance evaluation mechanisms. During system testing, the platform effectively simulated real-world cybersecurity scenarios such as phishing detection, password security analysis, and malware awareness training, enabling users to improve their threat recognition and decision-making skills.

The user interface was designed to be simple, interactive, and accessible, ensuring usability for individuals with varying technical backgrounds. Furthermore, the inclusion of a CERT-In reporting feature bridges the gap between cybersecurity awareness and real-world action, making the system practical and impactful. Overall, the proposed system offers an intelligent, scalable, and user-centric solution for promoting safe digital behavior and strengthening cybersecurity awareness.

Future work includes integrating adaptive learning algorithms for personalized training experiences, expanding cybersecurity scenarios to address emerging threats, developing mobile application support for improved accessibility, and incorporating advanced analytics to monitor long-term improvement in user cybersecurity behavior

REFERENCE

[1] C. Scherb, L. B. Heitz, F. Grimberg, H. Grieder, and M. Maurer, "A serious game for simulating cyberattacks to teach cybersecurity," *arXiv preprint arXiv:2305.03062*, May 2023.

[2] M. Nkongolo, "CyberMoraba: A game-based approach enhancing cybersecurity awareness," University of Pretoria, Faculty of Informatics, South Africa, 2023.

[3] W. Wayz, A. Rajuroy, and M. Ganz, "AI-Powered Personalized Learning Platforms for Enhancing Cybersecurity Education," Jan. 2025.

[4] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, "A novel SETA-based gamification framework to raise cybersecurity awareness," *International Journal of Information Technology*, Aug. 2021.

[5] K. Boopathi, S. Sreejith, and A. Bithin, "Learning cyber security through gamification," *Indian Journal of Science and Technology*, vol. 8, no. 7, pp. 642–649, Apr. 2015.

[6] T. M. Tran, R. Beuran, and S. Hasegawa, "Gamification-based cybersecurity awareness course for self-regulated learning," *International Journal of Information and Education Technology*, vol. 13, no. 4, Apr. 2023.

[7] H. Qusa and J. Tarazi, "Cyber-Her9o: A gamification framework for cyber security awareness for high school students," in *Proc. IEEE International Conference on Computing and Communication*, 2021.

[8] T. Tan, R. S. Abdullah, and Z. Mas'ud, "Cybersecurity education using gamification: Systematic literature review," *International Journal of Academic Research in Business and Social Sciences*, vol. 15, no. 10, 2025.

[9] A. K. Gwenhure and F. S. Rahayu, "Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review," *International Journal of Serious Games*, vol. 11, no. 1, Mar. 2024.

[10] P. A. Gandhi, "Raising cybersecurity awareness in an engaging way: How gamification and AI tips can help social media users stay safe from AI threats," *International Journal of Scientific Research and Engineering Development*, vol. 8, no. 3, May–Jun. 2025.