

Cybersecurity Defender: An AI-Enhanced Game-Based Tool for Improving Digital Threat Awareness and Protection Skills

Mariano, Jarred James C*, Solabo, Emmanuel F**, Rado, Nathan Keny Brook O***, Tabayag, John Michael M, Vivien A. Agustin*, Ronald B. Fernandez**

*(Department of Information Technology, Jesus Reigns Christian College, mjarredjames18.18@gmail.com)

** (Department of Information Technology, Jesus Reigns Christian College, nathankenybrook@gmail.com)

*** (Department of Information Technology, Jesus Reigns Christian College, emmanuelolabo061@gmail.com)

(Department of Information Technology, Jesus Reigns Christian College, johnmichaelmoralestabayag@gmail.com)

(Department of Information Technology, Jesus Reigns Christian College, 4vivien.agustin@email.lcup.edu.ph)

(Department of Information Technology, Jesus Reigns Christian College, 5ronald.fernandez@email.lcup.edu.ph)

Abstract: Cybersecurity has become one of the most critical concerns in today's digital age. Despite rising awareness campaigns, many individuals—particularly students and young professionals—still lack the skills to recognize and respond to cyber threats. Traditional approaches such as lectures and seminars are often unengaging and ineffective. This paper presents Cybersecurity Defender, an AI-enhanced, game-based learning tool designed to improve digital threat awareness and protection skills. The system incorporates adaptive difficulty, AI-generated threat simulations, and personalized feedback mechanisms to provide an interactive and learner-centered cybersecurity education experience. The study employs a developmental and descriptive research design with an Agile SDLC methodology, targeting students and young professionals as its primary audience.

Keywords — cybersecurity, game-based learning, artificial intelligence, digital threat awareness, gamification, adaptive learning.

I. INTRODUCTION

Cybersecurity has become one of the most critical concerns in today's digital age as individuals, organizations, and institutions are increasingly exposed to a wide range of online threats. With the rapid advancement of technology, malicious activities such as phishing, malware attacks, ransomware, and social engineering continue to evolve, putting sensitive data, financial resources, and personal privacy at risk.

Despite the rising number of awareness campaigns, many individuals, particularly students and young professionals, still lack the skills to properly recognize and respond to these threats. Traditional cybersecurity education methods—lectures, pamphlets, seminars, and text-heavy resources—are typically technical, monotonous, and difficult to retain.

This gap in accessibility and engagement highlights the need for more interactive, practical, and learner-centered strategies. In response, this study proposes the development of Cybersecurity Defender: An AI-Enhanced Game-Based Tool for Improving Digital Threat Awareness and Protection Skills. The system incorporates real-world cybersecurity scenarios, adaptive AI feedback, and gamified learning to make cybersecurity education more engaging, memorable, and accessible.

II. STATEMENT OF THE PROBLEM

In today's digital landscape, individuals and organizations face increasing risks from cyber threats such as phishing, malware, ransomware, and social engineering. Despite existing

awareness campaigns, many users remain vulnerable due to limited knowledge, lack of engagement, and insufficient practical application. Specifically, this study seeks to address:

- Traditional cybersecurity learning methods are unengaging and difficult to retain, often relying on text-heavy lectures and seminars.
- Existing learning approaches offer limited practical and experiential training, leaving learners unprepared to identify and respond to real-world threats.
- Current cybersecurity tools lack accessibility and do not utilize artificial intelligence to personalize learning or provide intelligent, real-time feedback.

III. OBJECTIVES OF THE STUDY

The general objective of this study is to develop an interactive game-based learning tool, Cybersecurity Defender, that aims to enhance digital threat awareness and protection skills among students and young professionals. Specifically, the study aims:

- To develop an engaging game-based learning system that addresses the limitations of traditional, text-heavy cybersecurity education methods and increases learner motivation and retention.
- To provide practical and experiential learning opportunities through simulated scenarios of common digital threats such as phishing, malware, ransomware, and social engineering.

- To integrate artificial intelligence features—including adaptive difficulty, personalized feedback, and automated threat generation—to enhance accessibility and tailor the learning experience.

IV. SCOPE AND LIMITATIONS

This study focuses on the design, development, and evaluation of Cybersecurity Defender, intended primarily for students and young professionals. The game covers common online security risks including phishing, malware, ransomware, and social engineering, presented through simulated real-world scenarios with three difficulty levels: Easy, Normal, and Hard.

The study is limited to email-based and general digital threat simulations and will not cover advanced hacking techniques, network penetration testing, or highly technical system vulnerabilities. Evaluation is restricted to a selected group of students and young professionals. The AI integration will be limited to lightweight machine learning techniques suitable for a game-based environment and will not analyze real user data outside the platform.

V. SIGNIFICANCE OF THE STUDY

The study benefits the following stakeholders:

Students and Young Professionals: Will gain accessible and engaging opportunities to strengthen their knowledge and skills in identifying and responding to cyber threats.

Educators and Academic Institutions: The study offers an alternative instructional tool that supplements traditional teaching methods.

Organizations and Employers: By equipping future professionals with practical cybersecurity awareness, the study contributes to safer work environments and reducing data breach risks.

Future Researchers: This project can serve as a reference for further studies exploring game-based learning applications in cybersecurity and digital literacy.

VI. DEFINITION OF TERMS

To enhance comprehension of the study, key terms are defined below.

A. I. Feedback System. An automated mechanism that analyzes player performance and provides personalized guidance or recommendations for improvement.

A. I.-Generated Threat Simulation. The use of artificial intelligence to create dynamic and realistic cyberattack scenarios that change according to user actions and behavior.

Adaptive Learning. A technology-driven approach where AI adjusts difficulty and content based on user performance.

Cybersecurity. The practice of protecting computers, networks, programs, and data from unauthorized access, attacks, or damage.

Digital Threat. Any potential danger that could exploit vulnerabilities in digital devices, networks, or online activities.

Game-Based Learning (GBL). An educational approach that uses games to deliver instructional content, enhance engagement, and improve knowledge retention.

Gamification. The application of game design elements such as points, levels, and rewards in non-game contexts to motivate users.

Malware. Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.

Phishing. A form of cyberattack where attackers impersonate legitimate entities to trick individuals into revealing sensitive information.

VII. REVIEW OF RELATED LITERATURE AND STUDIES

A. Related Literature

Artificial Intelligence has significantly improved the effectiveness of gamification in cybersecurity education by enabling more adaptive and personalized learning environments. Danyal Mahmood and Rabia Afzaal (2026) in their work Gamification Learning Framework for Cybersecurity Education demonstrate that AI-integrated gamified systems allow features such as adaptive challenge generation, real-time feedback, personalized learning paths, and intelligent assessment, transforming static educational games into dynamic data-driven platforms [1].

Muhammad Mudassar Yamin, Basel Katt, and Mariusz Nowostawski (2021) propose a serious game that serves as a platform for developing and simulating cybersecurity exercise scenarios where players assume attacker or defender roles, enabling real-time decision-making and evaluation of cyber-attack and defense mechanisms [2].

Rashed Nasser Almatrooshi et al. (2025) highlight gamification as an innovative approach that integrates game elements into training to improve user engagement and learning effectiveness, noting that while gamification enhances motivation and learning, limitations still need to be addressed [3].

Meera Humaid Alalawi (2024) emphasizes that combining gamification and AI can significantly improve awareness, strengthen user behavior, and support more effective cybersecurity education strategies by enabling personalized learning experiences [4].

Daniela Popescu and Raluca-Petronela Mahu highlight that integrating gamification and AI enhances student motivation, engagement, and knowledge retention in cybersecurity learning, making educational systems more interactive and adaptive [5].

Zhi Lian, Peng Shi, and Mou Chen (2024) provide a comprehensive survey of cyber-attacks affecting Cyber-Physical Systems (CPSs) and examine defense mechanisms, detection, and response strategies, contributing valuable insights into attack modeling and defense frameworks [6].

Stephen Hart et al. (2020) introduce 'Riskio,' a tabletop game designed to improve cybersecurity awareness, where players assume attacker and defender roles to better understand cyber threats in an active and engaging learning environment [7].

B. Related Studies

Nipuna Hiranya Weeratunge, Rune Hjelsvold, and Basel Katt (2026) conducted a scoping review of 230 studies showing that game-based methods are widely used and can enhance understanding of cybersecurity concepts, while emphasizing the need for standardized evaluation methods [8].

Barack Onduto (2021) highlights gamification as a powerful approach to enhance cybersecurity awareness through a systematic review following PRISMA guidelines. Most games are computer-based and target the general public using role-playing genres with demonstration-based learning strategies [9].

Iznora Aini Zolkifly, Norhaida Mohd Suaib, and Siti Hasnah Tanalol (2025) present a game-based learning framework evaluated among undergraduate students showing increased engagement, improved understanding of cybersecurity principles, and higher learner motivation [10].

Rhannel S. Paculanan et al. (2024) developed 'Cyberverse,' evaluated using ISO 25010 standards among 60 respondents, with findings revealing that the application effectively enhances cognitive abilities and applies cybersecurity concepts including password security, phishing awareness, and network security [11].

Deborah Richards et al. (Macquarie University) propose an AI-enhanced serious game for cybersecurity ethics training, integrating AI-driven intelligent ethical agents within a serious game to simulate complex social and ethical decision-making scenarios [12].

Andang Wijanarko and Aan Erlansari (2025) systematically reviewed gamification strategies for adolescent cybersecurity awareness training, finding that gamified environments significantly enhance learner engagement, intrinsic motivation, and knowledge retention [13].

C. Synthesis

The reviewed literature and studies collectively emphasize the increasing importance of innovative approaches in cybersecurity education. A significant theme identified is the effectiveness of game-based learning and gamification in enhancing cybersecurity awareness through mechanics such as challenges, rewards, role-playing, and simulations. Another key finding is the growing role of AI in enabling adaptive learning, personalized feedback, and intelligent assessment. These insights directly inform and justify the development of Cybersecurity Defender, which aims to provide an interactive, adaptive, and effective platform for improving digital threat awareness and protection skills.

VIII. DESIGN AND METHODOLOGY

A. Research Design

This study employs a developmental and descriptive research design with the implementation of the Agile methodology within the SDLC to develop Cybersecurity Defender. A mixed-method approach is adopted, with primary emphasis on quantitative data and supporting qualitative observations. Pre-tests and post-tests measure participants' cybersecurity knowledge, while surveys quantify user engagement, satisfaction, and perceived learning outcomes. Observational notes and open-ended responses provide insights into usability and the learning experience.

B. System Design

The proposed system is composed of four main modules: (1) User Module – handles player registration, login, and profile management; (2) Game Module – provides interactive cybersecurity challenges, simulations, and quizzes with AI-adaptive scenarios; (3) AI Analysis Module – monitors player actions, evaluates threat awareness, and generates feedback reports; and (4) Reporting Module – displays performance results and recommendations.

C. System Requirements

Hardware Requirements

Component	Specification
PC / Laptop	Intel Core i5+, 8GB RAM min, 256GB SSD/HDD, optional GPU
Internet	Stable Wi-Fi for downloads, testing, and online features

TABLE I: Hardware Requirements of the Proposed System

Software Requirements

Software	Purpose
Windows 10+	Operating system for development and execution
Python	Back-end development and AI functionalities
PyCharm	IDE for coding, debugging, and project management
Django	Web framework for user accounts, gameplay, and reporting
TensorFlow/Keras	AI framework for performance tracking and feedback
Draw.io / Canva	System diagrams, UI mockups, and visual elements
MySQL	Database for user data, scores, and progress
Chrome / Edge	Testing, research, and online resource access

TABLE II: Software Requirements of the Proposed System

D. Development Methodology (Agile SDLC)

The study adopts the Agile Software Development Life Cycle (SDLC), where development is carried out in iterative sprints allowing incremental system improvements based on continuous user feedback. The development phases are:

1. Planning Phase – Define objectives, scope, and system requirements through literature review and user needs analysis.
2. Design Phase – Create system architecture, UI/UX designs, DFDs, Use Case Diagrams, and ERDs.

3. Development Phase – Build game modules (phishing detection, password security, safe browsing) and AI components using Python, Django, and TensorFlow.

4. Testing Phase – Conduct unit testing, integration testing, and user acceptance testing (UAT).

5. Deployment Phase – Deploy the system as a web-based platform for user access.

6. Maintenance and Iteration Phase – Implement continuous improvements based on user feedback.

IX. CONCLUSIONS

This paper presents Cybersecurity Defender, an AI-enhanced, game-based learning tool designed to improve digital threat awareness and protection skills among students and young professionals. By combining gamification, adaptive AI features, and simulation-based learning, the system addresses the significant limitations of traditional cybersecurity education. The integration of adaptive difficulty, AI-generated threat scenarios, and personalized feedback aims to create a more engaging, effective, and accessible learning experience. Future work will involve full deployment, empirical evaluation using pre/post-test measures, and iterative improvements based on user data.

ACKNOWLEDGMENT

The authors wish to thank their academic institution for providing support and resources for this research, as well as the respondents who participated in the evaluation of the system.

REFERENCES

- [1] D. Mahmood and R. Afzaal, 'Gamification Learning Framework for Cybersecurity Education,' 2026.
- [2] M. M. Yamin, B. Katt, and M. Nowostawski, 'Serious games for cybersecurity exercise scenarios,' 2021.
- [3] R. N. Almatrooshi et al., 'Gamification in cybersecurity awareness training,' 2025.
- [4] M. H. Alalawi, 'Gamification and AI for cybersecurity education,' 2024.
- [5] D. Popescul and R. P. Mahu, 'Gamification and AI in higher education cybersecurity,' n.d.
- [6] Z. Lian, P. Shi, and M. Chen, 'Cyber-attacks on Cyber-Physical Systems: a survey,' 2024.
- [7] S. Hart, A. Margheri, F. Paci, and V. Sassone, 'Riskio: a tabletop game for cybersecurity awareness,' 2020.
- [8] N. H. Weeratunge, R. Hjelsvold, and B. Katt, 'Gamification and serious games for cybersecurity: a scoping review,' 2026.
- [9] B. Onduto, 'Gamification for cybersecurity awareness: a systematic review,' 2021.
- [10] I. A. Zolkifly, N. M. Suaib, and S. H. Tanalol, 'Game-based learning framework for cybersecurity,' 2025.
- [11] R. S. Paculanan et al., 'Cyberverse: a game-based learning application for cybersecurity awareness,' 2024.
- [12] D. Richards et al., 'AI-enhanced serious game for cybersecurity ethics training,' Macquarie University, n.d.
- [13] A. Wijanarko and A. Erlansari, 'Gamification on cybersecurity awareness training for adolescents,' 2025.