Phishing Quest: An AI-Driven Game-Based Learning System for Adaptive Email Threat Detection Training

Henmer Sanne Absalon[1]*, Margielyn G. Infante[2], Baron Valdez[3], Vivien A. Agustin[4], Ronald B. Fernandez[5]

Department of Bachelor of Science in Information Technology, Jesus Reigns Christian College, Philippines

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.100600278

Received: 22 May 2025; Accepted: 27 May 2026; Published: 22 June 2026

ABSTRACT

Phishing attacks remain one of the most widespread cybersecurity threats, exploiting users through deceptive emails that aim to steal sensitive information such as passwords, financial details, and personal data. Traditional cybersecurity awareness programs often fail to sustain user engagement and provide adaptive learning experiences. This study aims to develop Phishing Quest: An AI-Driven Game-Based Learning System for Adaptive Email Threat Detection Training, an interactive platform designed to enhance users' ability to identify and respond to phishing emails effectively. Specifically, the study seeks to create a game-based learning environment integrated with artificial intelligence that adapts training difficulty based on user performance, promotes engagement through interactive activities, and improves phishing detection skills.

The study employs a developmental research design involving the phases of planning, system design, development, implementation, and evaluation. The proposed system utilizes artificial intelligence algorithms to analyze user behavior and generate adaptive phishing scenarios tailored to individual learning progress. Game-based learning elements such as points, levels, rewards, challenges, and feedback mechanisms are integrated to encourage active participation and continuous learning. The system will be evaluated using usability testing and performance assessment questionnaires administered to selected participants. Data gathered will be analyzed to determine the effectiveness, usability, and user satisfaction of the developed system.

The expected results of the study indicate that the proposed system can significantly improve users' awareness and detection of phishing emails by providing engaging and adaptive cybersecurity training. Participants are anticipated to demonstrate increased accuracy in identifying phishing attempts, improved retention of cybersecurity concepts, and higher engagement compared to traditional learning approaches. Additionally, the integration of AI-driven adaptive learning is expected to provide personalized training experiences that address individual weaknesses and learning needs.

The study concludes that Phishing Quest has the potential to become an effective cybersecurity education tool that combines artificial intelligence and game-based learning to strengthen email threat detection skills. The system may contribute to reducing users' vulnerability to phishing attacks while promoting cybersecurity awareness in educational institutions, organizations, and online communities.

Keywords: Phishing Detection, Cybersecurity Awareness, Artificial Intelligence, Game-Based Learning, Adaptive Learning System, Email Threat Detection, Cybersecurity Training.

INTRODUCTION

Online communication and digital services are continuously growing, making email one of the most widely used tools for personal, academic, and business transactions. However, along with this growth, cyber threats have also

increased, particularly phishing attacks. Phishing is a type of online scam where attackers trick individuals into providing sensitive information such as passwords, bank details, or personal data by pretending to be legitimate organizations. These attacks often exploit human emotions like trust, fear, and urgency, making them highly effective.

The main problem is that many users still struggle to correctly identify phishing emails. Traditional methods of prevention, such as lectures, seminars, and informational materials, are often passive and lack engagement. While these methods provide knowledge, they do not give users enough practical experience in recognizing phishing attempts in real-life situations. Because of this, there is a gap between what users know and how they apply that knowledge when faced with actual threats.

The purpose of an AI-driven game-based learning system for phishing detection training is to improve users' ability to recognize and respond to phishing attacks. The proposed system, Phishing Quest, uses interactive and scenario-based learning where users analyze simulated emails and decide whether they are legitimate or malicious. The system evaluates key indicators such as suspicious links, unusual sender addresses, urgent language, and unexpected attachments to help users develop critical analysis skills.

The system will also use artificial intelligence to adapt to each user's performance. It will track user responses, identify strengths and weaknesses, and adjust the difficulty of training scenarios accordingly. Each user will receive personalized challenges, allowing beginners to start with simple cases while more advanced users handle complex phishing attempts. Through this adaptive learning approach, the system can provide a more effective and engaging training experience.

RELATED LITERATURE

In today's digital era, email remains a primary mode of communication for individuals and organizations. However, its widespread use has made it a major target for cyber threats, particularly phishing attacks. Phishing is a form of social engineering that manipulates users into disclosing sensitive information by impersonating legitimate entities. According to the Anti-Phishing Working Group (APWG, 2023), phishing attacks account for a significant percentage of global cyber incidents, continuously evolving in sophistication through the use of deceptive links, spoofed email addresses, and psychological manipulation techniques such as urgency and fear.

Traditional cybersecurity training approaches, such as lectures, seminars, and static tutorials, are often limited in effectiveness. While they provide foundational knowledge, they fail to simulate real-world scenarios where users must make quick decisions. Research shows that users who undergo traditional training often struggle to apply theoretical knowledge when confronted with actual phishing emails (Sheng et al., 2021). This gap between knowledge and application emphasizes the importance of experiential learning.

Game-based learning has emerged as a powerful educational approach that enhances engagement and retention. By incorporating elements such as scoring, challenges, and interactive scenarios, learners become more actively involved in the learning process. Hamari et al. (2016) found that gamification significantly improves motivation and knowledge retention in digital learning environments. Similarly, Kumar et al. (2020) demonstrated that gamified phishing simulations allow users to practice identifying threats in a controlled yet realistic setting, improving their decision-making skills.

Traditional approaches to cybersecurity awareness, including lectures, informational materials, and static tutorials, have proven inadequate for preparing users to identify phishing attempts in real-world scenarios. Studies show that while users may understand phishing concepts theoretically, they often fail to detect actual phishing emails due to factors such as cognitive overload, stress, and deceptive design of emails (Sheng et al., 2021). This gap between knowledge and application underscores the importance of practical, hands-on, and interactive training methods. Game-based learning has emerged as a highly effective solution, providing learners with immersive and engaging experiences. Kumar et al. (2020) demonstrated that incorporating realistic phishing scenarios into gamified environments increases learner engagement and allows users to apply theoretical knowledge in practice, thereby enhancing skill retention and decision-making under pressure.

Local studies in the Philippines also support the effectiveness of AI and gamified learning for cybersecurity awareness. DICT (2022) reported that users who participated in interactive online cybersecurity programs showed improved phishing detection performance and greater awareness of online threats. A case study conducted at a Manila-based university (Reyes, 2021) implemented AI-driven phishing simulations in a classroom setting, demonstrating that students' ability to identify phishing emails improved by over 30% after completing adaptive, gamified exercises. These findings highlight the applicability and effectiveness of AI-based adaptive learning in improving practical cybersecurity skills locally.

Furthermore, international research emphasizes the scalability and adaptability of AI-driven systems. Studies in the U.S. and Europe have implemented neural networks and machine learning algorithms to simulate realistic phishing scenarios, evaluate learner performance, and adapt exercises dynamically (Zhang et al., 2021; Al-Bahadili, 2021). These systems have proven effective in enhancing learner engagement, providing real-time feedback, and reinforcing practical decision-making skills. Collectively, these studies illustrate that AI, gamification, and adaptive learning approaches are effective tools for cybersecurity awareness programs, offering a model for the proposed Phishing Quest system.

METHODOLOGY

This chapter explains how Phishing Quest: An AI-Driven Game-Based Learning System for Adaptive Email Threat Detection Training is planned and developed. It presents the methodology used in the system's development, the overall system architecture, the identified system requirements, and the tools and techniques utilized to implement and demonstrate the system's functionality. It also describes how the game-based learning environment and AI-driven adaptability are structured to simulate phishing scenarios and enhance user learning.

The components discussed in this chapter provide a clear understanding of how the system is designed to deliver interactive training and support users in improving their ability to recognize phishing threats.

Research Design

This study employs a developmental research design to design, develop, and evaluate Phishing Quest: An AI-Driven Game-Based Learning System for Adaptive Email Threat Detection Training. This approach is appropriate because the study focuses on creating an interactive system that enhances users' ability to detect phishing threats through simulation and adaptive learning.

The Waterfall model ensures that each stage of development is carefully documented and reviewed, minimizing errors and providing a clear structure for the development process. This approach is particularly effective for educational systems where content, structure, and functionality must be well-organized before implementation.

Requirements & Analysis

In this phase, the researchers conducted a thorough analysis to determine the functional and non-functional

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VI June 2026

requirements of the system. The primary objective was to develop an interactive game-based platform that enhances users' ability to detect phishing emails using adaptive AI techniques. Requirements were gathered through the review of related literature on phishing attacks, cybersecurity awareness, and game-based learning methodologies.

System Design

The system design phase focused on creating the overall architecture and structure of Phishing Quest. This includes designing the user interface, database schema, system workflows, and integration of AI components for adaptive learning. Game mechanics were carefully planned to simulate real-world phishing scenarios, while ensuring an engaging and educational user experience.

Implementation

During the implementation phase, the system was developed based on the approved design specifications. The researchers utilized appropriate programming languages, development frameworks, and tools to build the platform. Core functionalities such as user registration, gameplay modules, phishing scenario simulations, scoring systems, and AI-driven adaptability were coded and integrated.

Testing

The testing phase involved systematic evaluation of the system to ensure that it meets the specified requirements and performs as intended. Various testing methods, including functional testing, usability testing, and performance testing, were conducted. The researchers verified the accuracy of the AI adaptation, the correctness of phishing scenarios, and the responsiveness of the system.

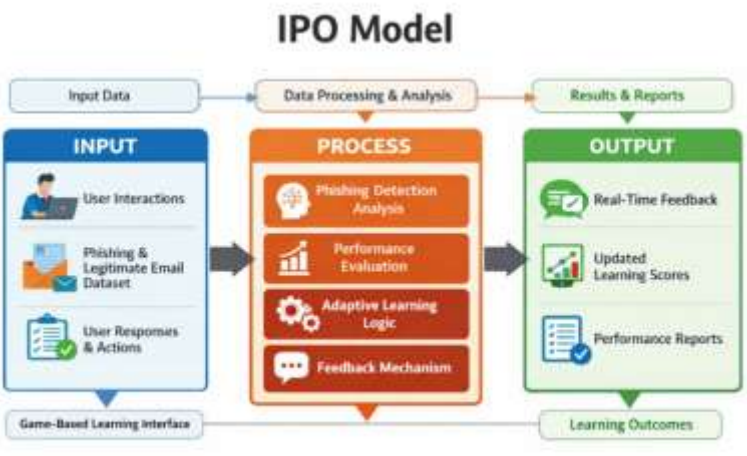
Deployment

After successful testing, the system was deployed for actual use. Phishing Quest was made accessible to its intended users, allowing them to engage with the game-based learning environment. Necessary configurations were completed to ensure smooth system operation in the deployment environment.

Maintenance

The maintenance phase involves continuous monitoring and improvement of the system after deployment. Updates are performed to fix bugs, enhance system performance, and incorporate new phishing scenarios that reflect evolving cyber threats. Additionally, improvements to the AI model may be implemented to increase accuracy and adaptability.

System Architecture



The system architecture follows the Input–Process–Output (IPO) model to clearly define the flow of data from user interaction with phishing simulation scenarios to the generation of learning outcomes and performance results. This approach ensures that each component of the system is well-structured, easy to maintain, and capable of delivering accurate, interactive, and adaptive phishing detection training for users.

The system receives input from users through a game-based learning interface, where learners interact with simulated email scenarios. These inputs include user responses to emails (such as identifying, ignoring, reporting, or opening messages), decision choices made during gameplay, and performance data gathered throughout the learning process. The system also utilizes a dataset of phishing and legitimate emails to support scenario generation and simulation activities.

Once the input data is received, it undergoes a series of processing stages. The AI-driven detection module analyzes user responses to determine whether the selected actions correctly identify phishing attempts. The system then computes performance scores based on accuracy, response time, and decision patterns. Using adaptive learning logic, the difficulty level of succeeding email scenarios is adjusted depending on user performance.

The final outputs include real-time feedback on user actions, updated learning scores, and adaptive progression to more advanced phishing scenarios. The system also generates performance reports that show the user's improvement in identifying phishing emails over time, as well as summaries of common mistakes and learning progress. These outputs are accessible through the user interface and serve as a guide for continuous improvement in phishing detection skills.

REFERENCE

1. Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005
2. Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304–312. https://doi.org/10.1016/j.chb.2014.05.046
3. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behavior? arXiv Preprint arXiv:1901.02672. https://arxiv.org/abs/1901.02672
4. Bishop, C. M. (2021). Pattern Recognition and Machine Learning. Springer.
5. Canova, G., Volkamer, M., Bergmann, C., & Reinheimer, B. (2015). NoPhish app evaluation: Lab and retention study. NDSS Workshop on Usable Security. https://doi.org/10.14722/usec.2015.23012
6. Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. Computers & Education, 59(2), 661–686. https://doi.org/10.1016/j.compedu.2012.03.004
7. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 581–590). Association for Computing Machinery. https://doi.org/10.1145/1124772.1124861
8. Furnell, S. (2019). Cybersecurity education and awareness: Looking back and looking forward. Computer Fraud & Security, 2019(10), 13–15. https://doi.org/10.1016/S1361-3723(19)30100-0
9. Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does gamification work? A literature review of empirical studies on gamification. In 2014 47th Hawaii International Conference on System Sciences (pp. 3025–3034). IEEE. https://doi.org/10.1109/HICSS.2014.377
10. Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650
11. Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, 62(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

12. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
13. Prensky, M. (2001). Digital Game-Based Learning. McGraw-Hill.
14. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 373–382). Association for Computing Machinery. https://doi.org/10.1145/1753326.1753383
15. Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483