Phish & Shield – AI-Based Cybersecurity Board Game

Submitted By

Urwah Siddiqui
22K-4676

Shiza Faisal
22K-4750

For Course

Artificial Intelligence

Department of Cyber Security
National University of Computer & Emerging Sciences

1. Motivation

> *In today's digital landscape, social engineering attacks like phishing are some of the most successful and overlooked threats. This game was built to make cybersecurity concepts more interactive, fun, and memorable. By gamifying realistic phishing attacks, it helps players build instinctive defense strategies.*

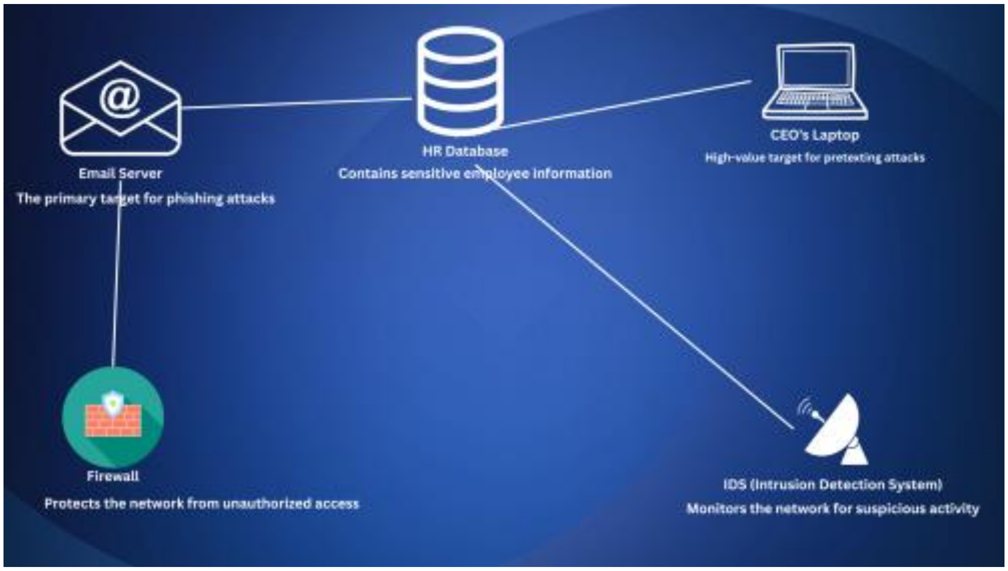
2. Overview

2.1 Significance of the Project

Phish & Shield transforms cybersecurity education into an engaging game. It raises awareness about phishing and ransomware threats, helping users build decision-making skills while defending digital assets. It is both practical and educational.

2.2 Description of the Project

Phish & Shield is a board-style Python game where an AI attacker targets network nodes with phishing/ransomware. The player analyzes alerts and selects defense strategies. Each node has unique behavior and risk. The goal is to survive attacks and prevent critical compromises using smart defense choices.


Email Server
The primary target for phishing attacks
HR Database
Contains sensitive employee information
CEO's Laptop
High-value target for pretexting attacks
Firewall
Protects the network from unauthorized access
IDS (Intrusion Detection System)
Monitors the network for suspicious activity

2.3 Background of the Project

The game is inspired by real-world phishing simulation tools and cybersecurity training models. It uses Python + Pygame, and incorporates basic AI strategy logic. Background research includes cybersecurity threat modeling and social engineering detection.

2.4 Project Category

Product-based Educational Game

3. Features / Scope / Modules

- AI launches phishing/ransomware attacks based on node state
- Real-time email simulation and popup
- Visual defense cards with strategic consequences
- Node-specific traits: e.g., CEO Laptop gives double points if breached
- Win/loss overlays, restart option, help screen
- Emotional feedback with alerts and urgency messages

4. Project Feasibility

- Technical: Feasible using Python + Pygame on standard systems.
- Economic: Zero-cost development, uses open-source libraries only.
- Schedule: Completed within 3 weeks including planning, coding, testing, and polish.

5. Hardware and Software Requirements

- Python 3.10 or higher
- Pygame library (cross-platform)
- Minimum: 4GB RAM, Recommended: 8GB+

6. Technologies Used

- Python
- Pygame
- Custom AI attack logic
- Real-time decision feedback
- GitHub for version control

7. References

[1] https://www.pygame.org/

[2] https://cisa.gov/stopransomware

[3] https://owasp.org/www-community/social_engineering_attacks