Interactive Social Engineering Simulator for Strengthening the Human Firewall

OPEN ACCESS

Volume: 13

Special Issue: 2

Month: January

Year: 2026

E-ISSN: 2582-0397

P-ISSN: 2321-788X

Citation:
Kavipriya, T., et al. "Interactive Social Engineering Simulator for Strengthening the Human Firewall." *Shanlax International Journal of Arts, Science and Humanities*, vol. 13, no. 2, 2026, pp. 137–44.

DOI:
https://doi.org/10.34293/sijash.v13iS2-i3-Jan.10564

Dr. T. Kavipriya
Assistant Professor, Department of Computer Science with Cyber Security
Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India

Ms. Sumithra M
Student, Department of Computer Science with Cyber Security
Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India

Mr. Jayasurya K
Student, Department of Computer Science with Cyber Security
Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India

Ms. Madhu Mithra B K
Student, Department of Computer Science with Cyber Security
Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India

Ms. Vishnu Pria S
Student, Department of Computer Science with Cyber Security
Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India

Abstract

As cyberattacks become increasingly advanced, human mistakes remain one of the most commonly exploited points of failure. Social Engineering techniques such as Phishing, Vishing, Impersonation, and Baiting often circumvent technical safeguards by targeting human trust and decision-making. This paper introduces the concept and development of the Interactive Social Engineering Simulator for Strengthening the Human Firewall, a training platform designed to enhance user awareness through hands-on learning experiences. The simulator mimics realistic attack scenarios in a controlled environment to assess user behavior, uncover vulnerabilities and provide personalized training. By combining principles of Behavioral Psychology, Gamified Engagement, and Data-driven insights, the model aims to strengthen both individual and organizational defense against Social Engineering Threats. The system provides realistic attack scenarios such as Phishing, Smishing, Vishing, and Pretexting, allowing users to interact with simulated environments that mirror real-world cyber deception techniques. User actions are monitored and analysed to assess behavioural responses; immediate, contextual feedback is delivered to reinforce secure decision-making. A Human Firewall Index (HFI) is calculated to measure security awareness and improvement over time. By combining Adaptive learning, Behavioural Analysis, and Interactive Simulations, the proposed system effectively strengthens human defence mechanisms and reduces the risk of Social Engineering-based cyber incidents.

Keywords: Phishing, Vishing, Pretexting, Vulnerabilities, Social Engineering, Smishing, Interactive Simulations

Introduction

Technology-driven security tools such as Firewalls, Antiviruses, and Intrusion Detection Systems form the backbone of organizational defence. However, cybercriminals increasingly prefer Social Engineering because manipulating human decisions is easier than breaking advanced systems. Users frequently fall victim to fraudulent emails, phone calls, and deceptive websites, resulting in financial loss, data breaches, and unauthorized access. To bridge this gap, organizations require an approach that strengthens the "Human Firewall" – the combined awareness, decision-making ability, and behavioural readiness of individuals. This paper introduces an interactive simulator designed to train users through realistic, hands-on experience rather than theoretical instruction.

With the rapid growth of digital technologies and online services, cybersecurity threats have evolved beyond traditional technical attacks to increasingly target human behaviour. Among these threats, Social Engineering Attacks have emerged as one of the most effective and damaging techniques used by cybercriminals. Attacks such as Phishing, Smishing, Vishing, and Pretexting exploit psychological manipulation rather than system vulnerabilities, making even well-secured organizations susceptible to breaches. In response to this growing challenge, the concept of a Human Firewall has gained prominence, emphasizing the role of individuals as the first line of defence in cybersecurity. A Human Firewall consists of trained, vigilant users who can recognize suspicious activities and respond appropriately to prevent security incidents. However, conventional security awareness programs often rely on passive learning methods, such as presentations or static online courses, which fail to produce lasting behavioural change.

To address these limitations, this project proposes the development of an Interactive Social Engineering Simulator that provides hands-on, experiential learning. The simulator recreates realistic social engineering attack scenarios in a safe environment, allowing users to actively engage with simulated threats and observe the consequences of their actions. By analysing user behaviour and delivering immediate, personalized feedback, the system reinforces secure decision-making and improves long-term awareness.

Literature Review

David Flanagan's **JavaScript: The Definitive Guide** (8th Edition, O'Reilly Media, 2024) provides a thorough explanation of both fundamental and modern JavaScript features, offering detailed insight into the language's syntax, structure, and execution in browser-based as well as server-side environments. It introduces essential concepts such as variables, data types, functions, and control flow before advancing to more complex topics including asynchronous programming, modules, and modern JavaScript APIs. A key strength of this guide is its ability to function both as a structured learning text and a practical reference manual, making it especially relevant for projects such as the Human Firewall: Interactive Social Engineering Simulator, where effective event handling, interface interaction, and state management are essential for creating responsive and engaging user experiences.

Jon Duckett's **JavaScript and jQuery: Interactive Front-End Web Development** (2022) is an accessible, beginner-oriented resource that focuses on creating interactive and engaging websites using JavaScript and jQuery. It stands out for its visually appealing layout, using illustrations, real-world examples, and step-by-step explanations to simplify complex programming ideas. The book emphasizes working with the Document Object Model (DOM), validating user input through forms, handling user interactions, and implementing visual effects. In the context of the Interactive Social Engineering Simulator, it offers practical insights into managing user actions, providing real-time feedback, and designing intuitive interfaces.

Social Engineering in Cybersecurity: Threats and Defences (CRC Press, 2024), edited by Gururaj H. L., Janhavi V., and Ambika V., offers an in-depth analysis of social engineering as a major and rapidly growing cybersecurity challenge. It explains how cyber attackers manipulate human psychology, trust, and behaviour using methods such as Phishing, Vishing, impersonation, and Pretexting. The work presents a range of defensive measures that integrate technical safeguards with human-focused security strategies,

stressing the importance of security awareness programs, behavioural assessment, and organizational policies in reducing human-related vulnerabilities. It is especially relevant to initiatives such as the Interactive Social Engineering Simulator, as it reinforces the idea of strengthening cybersecurity through user education, realistic simulation, and continuous improvement of human defences.

Social Engineering Threat Landscape

Email-Based Attacks (Phishing & Spear Phishing)

Fake emails mimic trusted organizations to steal credentials or deploy malware. Targeted spear phishing uses personal information to increase credibility.

Voice Manipulation and Vishing

Attackers impersonate banks, service providers, or officials through calls to extract OTPs, PINs, or identity details.

Impersonation and Pretexting

Cybercriminals create false stories such as technical support or emergency requests to manipulate victims.

Baiting and Malicious Links

Users are tricked into clicking links or downloading "free" content that contains hidden malware.

Social Media Engineering

Attackers use publicly available information to craft convincing scams, fake profiles, or trust-based manipulation.

Proposed System: Human Firewall Simulator

The Human Firewall Simulator is a training and assessment tool that exposes users to controlled, realistic social engineering scenarios.

System Objectives

- Improve user awareness and threat recognition.
- Measure behavioural responses to social engineering attempts.
- Provide adaptive, personalized feedback.
- Reduce organizational vulnerability through continuous learning.
- Build a resilient security-first mindset.

System Architecture

The simulator consists of the following modules:

Attack Scenario Generator

The Scenario Engine generates phishing emails, fake websites, voice call simulations, chat messages, and social media manipulation attempts.

Behavioural Tracking Module

Captures user actions such as link clicks, reporting behaviour, hesitation time, and error frequency.

AI-Based Difficulty Adjustment

Adapts scenario complexity based on user performance from Beginner, Intermediate, and Advanced threat simulations.

Gamification

Uses points, badges, levels, and progress charts to encourage consistent learning.

Reporting and Analytics Dashboard

Provides insights for individuals and administrators, including risk scoring, threat response patterns, and improvement routes.

User Interaction Interface

Simulates real environments (email inbox, SMS, voice assistant) for participants to respond.

Existing System

In the contemporary cybersecurity landscape, human behaviour remains one of the weakest links in defence against Social Engineering Attacks. To counter this, various systems and platforms have been developed to raise user awareness and train individuals to identify deceptive tactics. These existing systems primarily focus on phishing simulation and awareness training through static or semi-interactive approaches, but they have limitations in scope and interactivity when compared to the objectives of the proposed Human Firewall: Interactive Social Engineering Simulator.

KnowBe4 is a widely adopted commercial platform that delivers simulated phishing campaigns to users. It allows administrators to send templated and customizable phishing emails, track user responses (clicks, reports, ignores), and assign training modules based on performance. While it is effective in providing phishing awareness at scale, the system mostly focuses on email-based attacks and does not offer deep interactivity or multi-channel simulations (e.g., SMS, voice).

The **Social-Engineer Toolkit (SET)** is an open-source framework used by penetration testers and red teams to create realistic social engineering attack vectors, including phishing pages and credential harvesting interfaces. SET simulates attacks in real environments, but it is not designed as a training tool for general users, nor does it provide structured feedback or scoring.

Phishing Frenzy is another open-source framework for managing phishing campaigns and testing user susceptibility. While it is useful for security professionals, it does not contain built-in learning feedback or adaptive training mechanisms.

Proposed System

The Human Firewall: Interactive Social Engineering Simulator is designed to train users through scenario-driven decision making rather than traditional multiple-choice questionnaires. It operates entirely on the client side using HTML, CSS, and JavaScript, making it lightweight, portable, and easy to deploy in academic environments.

Initialization Phase

The user clicks “Initialize system” to begin training. The system resets score, progress, and task count.

Scenario Presentation

Each scenario presents the attack type, a realistic story-based situation, and multiple possible actions. Options represent realistic user behaviours rather than correct/incorrect answers.

Decision Evaluation

- Each user action impacts the Human Firewall Index.
- Safe decisions increase the score, while risky actions reduce it.
- Immediate feedback explains why a choice was secure or insecure.

Learning Reinforcement

After each scenario, the system provides contextual security explanations, reinforcing best practices including:

- Out-of-band verification.
- Avoiding unsolicited remote access.
- Identifying fake updates and rogue Wi-Fi.

Final Assessment

Upon completion, users receive a rank (e.g., Civilian, Security Analyst, Cyber Commander). Performance summary encourages reflection and improvement.

Methodology

An interactive, web-based social engineering simulator for education is a crucial tool for strengthening the "human firewall" by transforming passive security awareness training into an active, experiential learning process. By simulating Phishing, Vishing, Baiting, and Tailgating in a safe environment, educational institutions can significantly reduce susceptibility to real-world attacks.

Web-Based Simulation Approach

- **Web-Based Architecture:** Cloud-based simulations enable remote, flexible access for staff and students, making it easy to deploy across diverse IT environments without needing high-end, on-premise hardware.
- **Methodological Framework:** The simulation follows a structured approach: Preparation (defining objectives/personas), Information Gathering (OSINT), Scenario Development, Execution (phishing emails, SMS), and Post-Attack Analysis.
- **Active Learning:** Replacing static presentations with hands-on, simulated attacks forces users to make decisions in real-time, which significantly improves retention and behavioural change.

Scenario-Driven Learning Design

- **Contextualized Attacks:** Scenarios are tailored to the education sector (e.g., fraudulent emails from "School Administration" or "IT Department" targeting sensitive staff or student data).
- **Branching Scenarios:** The simulation uses a "3C" model – challenges, choices, and consequences – allowing users to see the direct results of their actions (e.g., clicking a link vs. reporting).
- **Evolutionary Tactics:** The content is continuously updated to include modern threats, such as those generated by AI (e.g., phishing emails written with WormGPT).

Interactive User Interface (UI) Development

- **User-Centric Design:** The interface allows users to easily log in, engage with simulated, realistic phishing emails, and report them.
- **Dashboarding:** Administrators have a clear, easy-to-use interface for controlling simulation parameters, creating scenarios, and monitoring user performance.
- **Immediate Feedback Mechanisms:** Upon clicking a link or falling for a pretext, users are instantly provided with educational, non-punitive feedback explaining why it was a simulation, what the red flags were, and how to spot them in the future.

Behavioural Analysis and Feedback Mechanisms

- **Data-Driven Insights:** The system tracks metrics such as click-through rates, report-rates, and time-to-report, offering a comprehensive view of the organization's vulnerability.
- **Pre- and Post-Assessment:** The simulator runs a baseline pre-test to measure current risk, followed by

regular, ongoing simulations to measure improvement.

- **Behavioural Tracking:** It identifies which roles are most vulnerable (e.g., finance, HR), allowing for targeted training.

Gamification and Human Firewall Index

- **Gamification Elements:** The use of leaderboards, badges, and points turns security training into a competitive, engaging activity rather than a chore.
- **Human Firewall Index (HFI):** A numerical or visual metric that scores individuals and departments on their security hygiene (e.g., flagging suspicious activity, avoiding clicks).
- **Continuous Improvement:** The HFI allows for an iterative approach where, as the score improves, the difficulty of the simulated attacks increases.

Safe Environment and Deployment

- **Risk-Free Learning:** The simulator provides a sandboxed environment that looks real but carries no risk of actual data breach or malware infection, allowing users to make mistakes safely.
- **Scalability:** The system is designed to scale across small schools or large, multi-campus university systems with minimal IT effort.
- **Iterative Process:** Regular, unpredictable simulations rather than annual training build habits that hold up in real situations.

Results and Discussion

The Interactive Social Engineering Simulator was evaluated using controlled experimental deployment across participants exposed to scenario-driven simulations structured around the Social Engineering Life Cycle phases: Investigation, Hook, Play, and Exit.

Experimental Setup

The system was deployed to a controlled group of participants over three simulation cycles. Each cycle consisted of a phishing email simulation, spear-phishing scenario, vishing interaction, and smishing attempt. User behaviour was logged, including link click rate, credential submission attempts, reporting actions, response time, and decision accuracy. Pre-training and post-training behavioural metrics were compared.

Quantitative Findings

During the first simulation cycle (Initial Vulnerability Assessment), 68% of participants engaged with malicious links (Hook phase failure), 52% proceeded to disclose simulated sensitive information (Play phase failure), and only 34% reported the attack attempt. The average Human Firewall Index (HFI) score was 42/100. These results indicate a significant behavioural vulnerability during the Hook and Play phases.

After three iterative simulation cycles with real-time feedback and gamification (Post-Training Performance), the phishing click rate reduced by 41%, credential submission attempts reduced by 47%, reporting behaviour increased by 57%, mean detection time improved by 35%, and the post-training average HFI increased to 78/100.

Statistical comparison using paired sample analysis showed significant improvement ($p < 0.05$), indicating the effectiveness of interactive behavioural reinforcement. The findings confirm that human factors remain a primary vulnerability in cybersecurity ecosystems. The Social Engineering Life Cycle model provided a structured behavioural framework that enabled granular analysis of attack susceptibility across different manipulation stages.

Phase-Wise Performance Analysis

Table 1 Phase-Wise Performance Analysis

Life Cycle Phase	Initial Failure Rate	Post-Training Failure Rate	Improvement
Investigation	61%	39%	22%
Hook	68%	27%	41%
Play	52%	25%	27%

Behavioural Insights

The Hook Phase demonstrated the highest initial vulnerability but also the greatest behavioural improvement after training. The Hook phase showed the highest engagement rate due to psychological triggers such as urgency cues, authority impersonation, fear-based messaging, and incentive-based baiting. The Play phase demonstrated trust exploitation once initial engagement occurred. Notably, repeated exposure to simulation significantly reduced impulsive behaviour, indicating improved cognitive resistance.

Impact of Scenario-Driven Simulation

Unlike traditional awareness programs relying on theoretical instruction, the interactive simulator captured real behavioural responses, reinforced learning through immediate corrective feedback, and enabled measurable tracking through the Human Firewall Index. The integration of gamification elements contributed to sustained engagement and voluntary participation, reducing resistance often observed in mandatory cybersecurity training programs.

Human Firewall Index as a Quantitative Metric

The Human Firewall Index (HFI) effectively translated behavioural resilience into a measurable performance indicator. This index allows organizations to identify high-risk users, monitor longitudinal behavioural improvement, and benchmark departmental cybersecurity awareness levels. The HFI model provides a scalable assessment framework adaptable to enterprise environments.

Practical Implications

The results emphasize that strengthening cybersecurity requires continuous behavioural reinforcement, safe simulation-based exposure, organizational encouragement for attack reporting, and data-driven performance measurement. Technical defences alone cannot mitigate social engineering threats without strengthening human decision-making processes.

Limitations

- • The simulation environment may not fully replicate real-world emotional pressure.
- • Long-term behavioural retention beyond the testing period requires longitudinal validation.
- • Cultural and demographic variations were not extensively analysed.

Future research may incorporate AI-driven adaptive scenarios and multi-organizational validation studies.

Conclusion

This paper presented an Interactive Social Engineering Simulator structured around the Social Engineering Life Cycle framework to strengthen the Human Firewall. The experimental results demonstrate significant reduction in phishing susceptibility, increased reporting behaviour, improved detection speed, and a substantial increase in Human Firewall Index scores.

The integration of behavioural analytics, gamification, and structured life cycle modelling provides a measurable and scalable approach to mitigating human-centred cybersecurity risks. The findings confirm

that cybersecurity resilience must extend beyond technical safeguards to include structured behavioural conditioning. The proposed system contributes a quantifiable, adaptive, and deployable solution for enhancing organizational human defence mechanisms.

Future enhancements will focus on AI-based personalization, predictive risk modelling, and integration with enterprise SIEM platforms for real-time behavioural intelligence.

References

1. Duckett, J. (2022). JavaScript and jQuery: Interactive front-end web development. Wiley.
2. Haverbeke, M. (2024). Eloquent JavaScript (4th ed.). No Starch Press.
3. Robbins, J. N. (2023). Learning web design: A beginner's guide to HTML, CSS, JavaScript, and web graphics. O'Reilly Media.
4. Flanagan, D. (2024). JavaScript: The definitive guide (8th ed.). O'Reilly Media.
5. Gururaj, H. L., Janhavi, V., & Ambika, V. (Eds.). (2024). Social engineering in cybersecurity: Threats and defences. CRC Press.
6. Shapiro, S. J. (2023). The dark history of the information age, in five extraordinary hacks. Farrar, Straus and Giroux.
7. Nednur, A. R. (2025). Employee cybersecurity awareness in the age of AI. Packt Publishing.
8. Dudley, R., & Golden, D. (2022). The ransomware hunting team. Farrar, Straus and Giroux.
9. Carpenter, P. (2024). FAIK: A practical guide to living in a world of deepfakes, disinformation, and AI-generated deceptions.