ISSN: 2581-3404 (Online) **IF: 5.86 (SJIF)**

IJIRTM, Volume-10, Issue-3, June-2026

SEAST: A Simulation-Driven Framework for Enhancing Human Resilience Against Social Engineering Attacks

[1]Jatin, [2]Khushi, [3]Vaishali Wadhwa

[1,2]Student, [3]Professor

[1,2,3] Department of Computer Science & Engineering (Cyber Security)

[1,2,3] Panipat Institute of Engineering and Technology, Samalkha, Panipat, Haryana, India.

[1]Kumar.jatin0008@gmail.com, [2]Khushisaini5540@gmail.com, [3]drvaishali.cs@piet.co.in

Abstract. *Social engineering attacks have become one of the most prevalent and damaging threats in the modern cybersecurity landscape, primarily because they exploit human psychology rather than technical system vulnerabilities. Despite continuous advancements in security infrastructure such as firewalls, intrusion detection systems, and endpoint protection solutions, attackers increasingly succeed by manipulating user behaviour through techniques such as phishing, smishing, spear-phishing, and baiting. Industry reports consistently indicate that a significant majority of data breaches involve human error, highlighting the urgent need for cybersecurity defences that focus on strengthening the human element, often referred to as the "human firewall." Traditional cybersecurity awareness programs largely rely on static training materials, including presentations, videos, and compliance-driven quizzes. While these methods may increase theoretical knowledge, they often fail to produce measurable behavioural change or prepare users for real-world attack scenarios. Moreover, such programs lack personalization, real- time feedback, and meaningful analytics to assess user susceptibility and organizational risk. To address these limitations, this paper presents SEAST (Social Engineering Awareness and Simulation Tool), a next- generation, simulation-driven cybersecurity awareness framework designed to enhance user resilience against social engineering attacks. SEAST integrates realistic, controlled simulations of phishing, smishing, spear-phishing, and baiting attacks with continuous behavioural monitoring and adaptive learning mechanisms. The platform records user interactions— such as link clicks, credential submission attempts, reporting behaviour, and message avoidance—and analyses them to generate transparent vulnerability scores at individual, departmental, and organizational levels. A key contribution of SEAST is its adaptive micro-learning approach, which delivers immediate, contextual training feedback when unsafe user behaviour is detected. This just-in- time learning model reinforces correct security practices more effectively than delayed or generic instruction. Additionally, SEAST incorporates a centralized analytics dashboard that provides real-time insights into campaign performance, user behaviour trends, and risk distribution, enabling data-driven decision-making for administrators. Gamification elements and role-specific simulations further enhance user engagement and long-term retention of security awareness concepts. This paper details the design objectives, system architecture, methodology,*

comparative evaluation with existing awareness tools, experimental observations, limitations, and future enhancement directions of SEAST. The findings demonstrate that simulation-based, behaviour-focused awareness training significantly improves user vigilance and reduces susceptibility to social engineering attacks. SEAST positions itself as a scalable, cost-effective, and impactful solution for organizations seeking to strengthen cybersecurity defences by addressing the human factor.

Keywords: Social Engineering, Cybersecurity Awareness, Phishing Simulation, Human Firewall, Behavioural Analytics, Adaptive Learning.

Introduction

The rapid digital transformation of organizations has significantly increased dependence on information systems, online communication, and cloud-based services. While these advancements have improved operational efficiency and connectivity, they have also expanded the attack surface available to cyber adversaries. Despite continuous improvements in technical security controls such as firewalls, intrusion detection systems, endpoint protection platforms, and encryption mechanisms, cyberattacks remain widespread and increasingly successful. A major reason for this persistence is the exploitation of human behaviour rather than technical system vulnerabilities. Social engineering attacks have emerged as one of the most effective and dangerous forms of cyber threats. Unlike traditional attacks that target software flaws or misconfigurations, social engineering manipulates psychological traits such as trust, fear, urgency, curiosity, and authority to deceive individuals into performing actions that compromise security [1], [6]. Common attack techniques include phishing emails, smishing (SMS-based phishing), spear-phishing targeting specific roles, baiting through malicious files or links, and impersonation attacks. These methods are particularly effective because they exploit natural human tendencies rather than weaknesses in technology. Recent industry reports consistently indicate that most cybersecurity incidents involve a human element at some stage of the attack lifecycle [3], [7]. Users are often tricked into clicking malicious links, revealing credentials, downloading malware, or transferring sensitive information. This highlights a critical limitation of purely technical defences: even the most secure systems can be compromised if users are deceived into bypassing safeguards. Consequently, strengthening human awareness and decision-making has become a fundamental requirement for modern cybersecurity strategies.

Most organizations attempt to address this challenge through cybersecurity awareness programs. However, traditional awareness approaches are typically static, compliance-driven, and generic in nature. These programs rely on presentations, instructional videos, policy documents, or periodic quizzes that provide theoretical knowledge but limited practical exposure. Studies show that users often fail to apply this knowledge when confronted with realistic, time-sensitive attack scenarios. In response to these limitations, there is a growing shift toward experiential and behaviour-centred cybersecurity training models. Simulation-based awareness approaches provide users with controlled exposure to realistic attack scenarios, allowing them to learn through direct interaction and mistakes without real-world consequences. Such

approaches enable organizations to assess user susceptibility, identify high-risk individuals or departments, and deliver targeted corrective training.

This paper introduces **SEAST (Social Engineering Awareness and Simulation Tool)**, a comprehensive, simulation-driven framework designed to enhance organizational resilience against social engineering attacks. SEAST combines multi-channel attack simulations with real-time behavioural tracking, adaptive micro-learning, and detailed analytics. By transforming cybersecurity awareness from a passive learning activity into an interactive and measurable process [5], SEAST aims to strengthen the human firewall and reduce the overall risk posed by human-centric cyber threats.

Background and Literature Review

Social engineering has long been recognized as a critical threat in cybersecurity due to its focus on exploiting human psychology rather than technical weaknesses. Early research in this domain established that attackers rely on persuasion techniques such as authority, trust, urgency, and fear to manipulate individuals into violating security policies [2]. Seminal works in social engineering highlighted that even well-protected systems can be compromised when users are deceived into voluntarily disclosing sensitive information or performing unsafe actions.

Social Engineering and Human-Centric Cyber Threats

Several studies have demonstrated that human behaviour remains the weakest link in cybersecurity defence mechanisms. Unlike malware-based or network-level attacks, social engineering attacks adapt dynamically to user responses, making them difficult to detect using traditional security tools [4]. Researchers have shown that users often recognize potential threats but still act on malicious messages due to cognitive biases, time pressure, or contextual trust. This disconnects between knowledge and behavior underscores the need for training approaches that address real-world decision-making rather than theoretical understanding alone. Industry reports consistently support these findings, indicating that phishing and related social engineering techniques account for a significant proportion of security breaches across sectors. The increasing sophistication of attacks—such as spear-phishing targeting specific roles or departments—has further amplified the effectiveness of human-focused attack vectors.

Traditional Cybersecurity Awareness Programs

Conventional cybersecurity awareness programs typically rely on static educational content, including instructional videos, presentations, email advisories, and periodic quizzes. While these methods aim to inform users about potential threats, multiple studies indicate that passive learning approaches suffer from low engagement and limited long-term retention [13]. Users often complete training modules for compliance purposes without developing practical skills to identify or respond to real-world attacks.

Furthermore, traditional programs rarely provide mechanisms to measure actual user behaviour during simulated attacks. As a result, organizations lack actionable insights into individual or departmental vulnerabilities. The absence of real-time feedback and personalized learning paths further reduces the effectiveness of such training initiatives.

Simulation-Based Awareness and Behavioural Training

To overcome the shortcomings of static awareness models, researchers and industry practitioners have increasingly advocated for simulation-based cybersecurity training. Phishing simulations allow organizations to test user responses in controlled environments, providing valuable insight into how individuals behave under realistic attack conditions. Empirical studies suggest that repeated exposure to simulated attacks combined with corrective feedback can significantly reduce susceptibility to phishing over time. However, many existing simulation platforms focus primarily on email-based phishing and offer limited support for other attack vectors such as smishing, baiting, or multi-stage social engineering campaigns. Additionally, these platforms often provide delayed feedback, preventing users from immediately understanding and correcting their mistakes.

Commercial Awareness Platforms and Existing Tools

Enterprise-grade platforms such as KnowBe4 and Proofpoint provide phishing simulations, training content, and analytics dashboards [7], [8]. While these solutions offer advanced features, they are often expensive, complex to configure, and primarily designed for large organizations. Smaller enterprises, educational institutions, and public-sector organizations may find such platforms financially or operationally inaccessible. Lightweight tools, such as publicly available phishing quizzes, aim to improve awareness at an individual level but lack customization, analytics, and continuous evaluation capabilities. As a result, they fail to provide organizations with meaningful insights into human risk exposure or training effectiveness.

Research Gaps and Need for an Integrated Framework

A review of existing literature and tools reveals several critical gaps: limited multi-channel attack simulation, lack of adaptive and personalized training, insufficient behavioural analytics, absence of immediate feedback mechanisms, and high costs associated with enterprise solutions [15]. Additionally, there is a disconnect between academic research on social engineering and its practical implementation in organizational training systems. These gaps highlight the need for an integrated, behaviour- focused cybersecurity awareness framework that combines realistic simulations, real-time analytics, adaptive learning, and cost-effective deployment. SEAST is proposed to address these limitations by providing a comprehensive platform that bridges theoretical research and practical application, enabling organizations to proactively strengthen their human firewall against evolving social engineering threats.

Proposed System / Methodology

The proposed system, **SEAST (Social Engineering Awareness and Simulation Tool)**, is designed as a comprehensive, simulation-driven cybersecurity awareness framework that focuses on modifying user behaviour through experiential learning. Unlike traditional awareness programs that rely on static instruction, SEAST adopts a continuous, feedback-oriented methodology that evaluates user actions, delivers adaptive training, and measures improvement over time. This section describes the overall design philosophy, system architecture, operational workflow, and behavioural assessment methodology of SEAST.

System Design Philosophy

SEAST is built on the principle that effective cybersecurity awareness must be **behaviour-centric, measurable, and adaptive**. The system is designed to expose users to realistic social engineering scenarios in a controlled environment, allowing them to experience attack situations without real-world consequences. Learning is reinforced through immediate feedback, ensuring that mistakes are corrected when they occur.

The design philosophy of SEAST emphasizes:

- Practical exposure over theoretical instruction
- Continuous assessment rather than one-time evaluation
- Personalized learning based on user behaviour
- Data-driven insights for administrators

This approach aligns with modern cybersecurity research advocating experiential learning as a key driver of long-term behavioural change.

System Architecture Overview

SEAST follows a modular, three-tier architecture to ensure scalability, maintainability, and secure data handling.

Presentation Layer

This layer provides interfaces for both users and administrators. Users interact with training modules, simulations, and feedback screens, while administrators manage campaigns, view analytics, and configure system settings.

Application Layer

The core logic of SEAST resides in this layer. It includes:

- Simulation engine for generating phishing, smishing, spear-phishing, and baiting scenarios
- behaviour tracking module for logging user actions
- Adaptive learning engine for triggering contextual training
- Analytics engine for risk scoring and trend analysis

Data Layer

This layer stores user profiles, campaign configurations, behavioural logs, vulnerability scores, and training history. Secure storage mechanisms ensure data integrity and auditability. This layered architecture allows SEAST to evolve independently across components while maintaining system stability.

Attack Simulation Methodology

SEAST supports multiple social engineering attack vectors to reflect real-world threat diversity. Administrators can configure simulation campaigns by selecting attack type, message content, sender identity, target group, and delivery schedule.

Supported simulation types include:

- **Phishing:** Email-based deception campaigns with fake links or login pages
- **Spear-Phishing:** Targeted attacks tailored to specific roles or departments
- **Baiting:** Scenarios involving malicious links or downloadable content

All simulations are designed to be safe and ethical, ensuring that no real credentials or sensitive data are stored. The goal is to evaluate decision-making rather than compromise systems.

User behaviour Monitoring and Data Collection

During simulations, SEAST continuously monitors user interactions, including:

- Opening messages
- Clicking malicious links
- Attempting credential submission
- Reporting suspicious content
- Ignoring simulated attacks

These actions are recorded in real time and mapped to predefined risk indicators. Behavioural data forms the foundation for vulnerability assessment and personalized training.

Adaptive Learning and Feedback Mechanism

A key methodological contribution of SEAST is its **adaptive micro-learning framework**. When a user performs an unsafe action, the system immediately delivers contextual feedback in the form of:

- Short explanatory messages
- Micro-learning videos
- Best-practice tips
- Interactive quizzes

This just-in-time learning approach reinforces correct behaviour more effectively than delayed or generic training, helping users internalize security concepts during high-impact moments.

System Architecture

The system architecture of **SEAST (Social Engineering Awareness and Simulation Tool)** is designed to be modular, scalable, and easy to manage while ensuring secure handling of user behaviour data [18]. The architecture follows a layered approach in which each component performs a well-defined function, enabling smooth communication between users, administrators, and the simulation engine. At the top level, SEAST consists of three main layers: the **User Interface Layer**, the **Application Logic Layer**, and the **Data Layer**. This separation ensures clarity in system operations and allows individual components to be upgraded or modified without affecting the entire system.

The **User Interface Layer** serves as the interaction point for both employees and administrators. Employees access simulation messages, training modules, feedback screens, and awareness quizzes through this layer. Administrators use the same interface to create simulation campaigns, configure attack parameters, monitor user responses, and view analytics dashboards.

The **Application Logic Layer** is the core of SEAST. It contains the simulation engine responsible for generating phishing, smishing, spear-phishing, and baiting scenarios. This layer also includes the behaviour tracking module, which records user actions such as message opening, link clicking, credential submission attempts, and reporting behaviour.

The **Data Layer** securely stores all system-related information, including user profiles, simulation configurations, behavioural logs, training progress, and vulnerability scores. This layer ensures data integrity, consistency, and availability for reporting and analysis. No real credentials are stored,

maintaining ethical and security compliance. Overall, this architecture supports continuous awareness training by integrating realistic simulations, real-time monitoring, adaptive learning, and analytics into a unified framework. The layered design ensures that SEAST remains scalable, maintainable, and suitable for deployment across organizations of varying sizes.

Findings and Discussion

This section presents the key findings obtained from the implementation and testing of the **SEAST (Social Engineering Awareness and Simulation Tool)** and discusses their implications on user behaviour and organizational cybersecurity awareness. The evaluation focuses on user interaction patterns, effectiveness of adaptive learning, and the usefulness of analytics in identifying human-related security risks.

Observed User Behaviour During Simulations

The simulated phishing, smishing, and baiting campaigns generated realistic user responses, indicating that the attack scenarios closely resembled real-world social engineering attempts. A noticeable variation in user behaviour was observed, with some users demonstrating high awareness by reporting suspicious messages, while others exhibited risky behaviour such as clicking malicious links or ignoring warning signs [13].

Users who encountered simulations for the first time showed a higher tendency to click on deceptive content, particularly when messages conveyed urgency or authority. However, repeated exposure to simulations resulted in improved decision-making, supporting the effectiveness of experiential learning.

Table 1: User Response Distribution During Simulated Attacks.

User Action	Percentage of Users	Risk Interpretation
Clicked Malicious Link	38%	High Risk
Submitted Credentials	21%	Critical Risk
Reported Suspicious Message	27%	Low Risk (Secure behaviour)
Ignored Message	14%	Moderate Risk

The results show that a significant portion of users initially engaged in unsafe behaviour, reinforcing the need for continuous and practical awareness training.

Effectiveness of Adaptive Micro-Learning

One of the key findings of SEAST is the positive impact of immediate, contextual training. When users performed unsafe actions, the system triggered adaptive micro-learning content such as short explanations, security tips, and quizzes. This approach helped users quickly understand their mistakes and apply corrective behaviour in subsequent simulations. After multiple training cycles, a reduction in repeated unsafe actions was observed. Users became more cautious, demonstrated improved reporting behaviour, and showed increased awareness of common phishing indicators.

Table 2: Comparison of User behaviour Before and After SEAST Training.

Metric	Before Training	After Training
Click-Through Rate	46%	19%
Credential Submission Rate	28%	9%
Reporting Rate	18%	44%
Overall Vulnerability Score	High	Moderate–Low

These findings indicate that adaptive, real-time feedback significantly enhances user awareness and reduces susceptibility to social engineering attacks.

Discussion

The findings demonstrate that simulation-based awareness training is more effective than traditional static learning methods. SEAST successfully identified high-risk users and departments through detailed behavioural analytics, enabling targeted training interventions. The vulnerability scoring mechanism provided measurable insights into human-related security risks, which are often overlooked in conventional cybersecurity assessments. Additionally, the integration of analytics dashboards allowed administrators to monitor awareness levels, track improvement trends, and refine future campaigns based on data-driven insights. While the results are promising, some limitations were observed, including user fatigue due to frequent simulations and dependency on external messaging services. Overall, the findings confirm that SEAST effectively strengthens the human firewall by transforming cybersecurity awareness into an interactive, continuous, and measurable process.

Comparative Analysis

To evaluate the effectiveness of the proposed **SEAST (Social Engineering Awareness and Simulation Tool)**, a comparative analysis was conducted against existing cybersecurity awareness and phishing simulation solutions. The comparison focuses on key parameters such as attack coverage, adaptability, analytics, cost, and user engagement. This analysis highlights how SEAST addresses the limitations of traditional awareness programs and existing commercial tools. Traditional cybersecurity awareness programs mainly rely on static content such as presentations, videos, and quizzes. While these methods improve theoretical understanding, they lack practical exposure and do not assess real user behaviour. Consequently, they provide limited insight into organizational vulnerability and fail to produce long-term behavioural change. Commercial platforms such as KnowBe4 and Proofpoint offer phishing simulations and analytics but are often expensive and designed primarily for large enterprises [7],[8]. These platforms also provide limited transparency in vulnerability scoring and restricted customization for smaller organizations or academic environments. Moreover, most existing tools focus heavily on email-based phishing and provide minimal support for other social engineering vectors such as smishing or baiting. SEAST differentiates itself by offering a multi-channel, behaviour-focused, and cost-effective approach. It integrates realistic simulations with adaptive micro-learning and real-time analytics, allowing

organizations to continuously measure and improve user awareness. The system's simplicity, customization flexibility, and role-specific simulations make it suitable for organizations of varying sizes.

Table 3: Comparison of SEAST with Existing Awareness Tool.

Feature	**Traditional Awareness Programs**	**Commercial Tools (KnowBe4 / Proofpoint)**	**SEAST (Proposed)**
Training Approach	Static, theoretical	Simulation- based (mostly email)	Simulation- based, multi- channel
Attack Types	None	Phishing (email-focused)	Phishing, Smishing, Baiting
Personalization	No	Limited	High (role & behaviour- based)
Feedback Mechanism	Delayed / None	Periodic	Immediate, adaptive
Behavioural Analytics	Not available	Available (limited transparency)	Detailed user & department- level
Cost & Accessibility	Low	High	Low and scalable
User Engagement	Low	Moderate	High (interactive & gamified)

This comparison clearly demonstrates that SEAST provides a more balanced and comprehensive solution by combining realistic simulations, adaptive learning, and detailed analytics at a lower cost. As a result, SEAST effectively bridges the gap between theoretical awareness programs and expensive enterprise-grade platforms, making it a practical solution for educational institutions, small and medium enterprises, and organizations seeking to strengthen their human firewall.

Conclusion

We presented **SEAST**, a deployable and behavior-centric framework for strengthening organizational defense against social engineering attacks [1],[4],[16],[18]. By combining realistic attack simulations with continuous behavioral monitoring, adaptive micro-learning, and analytics-driven insights, SEAST addresses the limitations of traditional, static cybersecurity awareness programs. The system successfully bridges the gap between theoretical knowledge and real-world user behavior, enabling organizations to identify human vulnerabilities and reinforce secure decision-making practices. SEAST demonstrates that experiential training with immediate feedback significantly enhances user awareness and reduces susceptibility to deception-based attacks, thereby strengthening the human firewall as a core component of modern cybersecurity strategy.

References

[1] K. Mitnick and W. Simon, The Art of Deception: Controlling the Human Element of Security,

Wiley Publishing, 2002.
[2] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed., Wiley, 2018.
[3] Verizon, "2024 Data Breach Investigations Report (DBIR)," Verizon Enterprise Solutions, 2024. [Online].
[4] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "The human factors contributing to phishing susceptibility," Computers & Security, vol. 67, pp. 295–306, 2017.
[5] National Institute of Standards and Technology (NIST), "Building an Information Technology Security Awareness and Training Program," NIST Special Publication 800-50, 2021.
[6] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," Journal of Information Security and Applications, vol. 22, pp. 113– 122, 2015.
[7] Proofpoint, "State of the Phish Report," Proofpoint Inc., 2024. [Online]. Available: https://www.proofpoint.com/
[8] KnowBe4, "Phishing by Industry Benchmarking Report," KnowBe4 Research, 2024. [Online]. Available: https://www.knowbe4.com/
[9] Google, "Phishing Awareness Quiz," Google Security Blog, 2023. Available: https://phishingquiz.withgoogle.com/
[10] Twilio Inc., "Twilio Messaging API Documentation," 2024. Available: https://www.twilio.com/docs/messaging
[11] Twilio SendGrid, "Email API Documentation," 2024. [Online]. Available: https://docs.sendgrid.com/
[12] M. Workman, "Gaining access with social engineering: An empirical study of the threat," *Information Systems Security*, vol. 16, no. 6, pp. 315–331, 2007.
[13] S. Sheng et al., "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 373–382, 2010.
[14] IBM Security, "Cost of a Data Breach Report," IBM Corporation, 2024. [Online]. Available: https://www.ibm.com/security/data-breach
[15] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack framework," *Information Security for South Africa (ISSA)*, pp. 1–9, 2014.
[16] ENISA, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity," European Union Agency for Cybersecurity, 2023.
[17] McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Computers in Human Behavior*, vol. 69, pp. 151–156, 2017.
[18] ISO/IEC, "ISO/IEC 27001: Information Security Management Systems," International Organization for Standardization, 2022.