AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

SOCIAL ENGINEERING AWARENESS AND ATTACK SIMULATION ANALYSIS

[1]T Tejaswi, [2]A Sagar Goud, [3]A Praveen Kumar, [4]K Ajay
[1]Assistant Professor, [234]Students
Department of Computer Science and Engineering,
Siddhartha Institute of Technology and Sciences, Narapally, Korremula Road,
Ghatkesar, Medchal-Malkajgiri, Hyderabad, Telangana - 500088. INDIA
thadaka.tejaswi@siddhartha.org.in, 23TQ1A6226@siddhartha.co.in,
23TQ1A6203@siddhartha.co.in, 23TQ1A6211@siddhartha.co.in

Abstract

Social engineering is a major cybersecurity concern because it exploits human behavior and decision-making rather than relying only on technical vulnerabilities. Attackers may use deceptive communication, impersonation, urgency, or manipulation to persuade individuals to disclose information or perform unsafe actions. Therefore, improving user awareness is an important part of an organization's overall cybersecurity strategy.

The proposed Social Engineering Awareness and Attack Simulation Analysis system is designed to provide a controlled environment for studying how users respond to simulated social-engineering scenarios. The platform can conduct authorized awareness exercises using safe and non-destructive scenarios and record user interactions without collecting real passwords, confidential information, or sensitive personal data. The primary purpose is education and security improvement rather than actual exploitation.

The system analyzes simulation results to identify common behavioral patterns and awareness gaps. Metrics such as participation, recognition of suspicious indicators, reporting behavior, and completion of awareness activities can be used to evaluate user preparedness. Results can be categorized by department, role, training group, or assessment period while applying appropriate privacy controls.

A centralized dashboard can display simulation statistics, awareness scores, risk trends, and training progress. The system can also provide educational content explaining warning signs such as suspicious requests, unusual links, impersonation attempts, unexpected attachments, and requests for sensitive information. Reports can help security teams identify areas where additional awareness training may be beneficial.

Overall, the system aims to strengthen the human component of cybersecurity by combining controlled simulation, awareness education, behavioral analysis, and reporting. It can be used by organizations, educational institutions, and cybersecurity training programs to measure awareness and improve users' ability to recognize and report potential social-engineering threats in a safe and authorized environment.

I. Introduction

Social engineering refers to techniques that manipulate individuals into taking actions that may compromise security. Unlike attacks that depend entirely on software

vulnerabilities, social-engineering incidents often exploit trust, curiosity, fear, urgency, authority, or familiarity. Examples include impersonation, deceptive messages, fraudulent requests, and other forms of psychological manipulation. Because users interact directly with digital systems, their decisions can significantly influence organizational security.

Organizations commonly deploy technical security controls such as firewalls, antivirus solutions, endpoint protection, identity management, and network monitoring. Although these controls are important, they cannot completely eliminate risks associated with human behavior. A user who unknowingly responds to a suspicious request may bypass otherwise effective technical defenses. Consequently, cybersecurity awareness training has become an important component of security programs.

Traditional awareness programs often rely on presentations, written guidelines, videos, and periodic quizzes. These approaches can communicate security concepts, but they may not accurately measure how users behave when confronted with a realistic but safe simulated situation. Controlled simulations can provide additional insight by allowing organizations to evaluate whether users recognize warning signs, avoid unsafe actions, and report suspicious activity.

The proposed system provides a centralized platform for managing social-engineering awareness exercises and analyzing their outcomes. Authorized administrators can configure safe simulation scenarios, select appropriate training groups, monitor participation, and review aggregated results. The platform can also provide educational feedback after simulations so that participants understand why a scenario was suspicious and how similar situations should be handled.

The main objective of the project is to improve organizational security awareness through measurable and ethical training. By combining simulation analysis with educational content and reporting, the system can help organizations identify awareness gaps and continuously improve their security culture. The platform emphasizes user privacy, authorization, non-destructive testing, and the principle that simulation results should be used for education and risk reduction rather than punishment.

II. Literature Survey

Social engineering has received significant attention in cybersecurity research because human behavior is an important component of information-security risk. Research has examined how attackers exploit psychological principles such as authority, urgency, reciprocity, trust, and fear. These studies indicate that technical security mechanisms alone are insufficient when users are unable to recognize deceptive communication. Consequently, security awareness and user education are considered important defensive measures.

Phishing-awareness research has investigated how users identify suspicious messages and what factors influence their decisions. Studies have shown that users may have difficulty distinguishing legitimate communication from deceptive content when messages appear urgent, personalized, or authoritative. Awareness programs therefore

commonly teach users to inspect senders, verify unexpected requests, avoid suspicious links and attachments, and report questionable communication through established organizational channels.

Security awareness training has evolved from static educational material toward more interactive approaches. Traditional training may include presentations, policy documents, videos, and assessments, whereas modern programs may incorporate quizzes, scenario-based learning, and controlled simulations. Interactive approaches can provide users with practical experience and immediate feedback, potentially making security concepts easier to understand and remember.

Research on security behavior measurement emphasizes the importance of evaluating outcomes rather than simply measuring training completion. Metrics such as reporting behavior, recognition of suspicious indicators, training performance, and repeated behavior can provide better insight into awareness levels. A centralized platform can collect these measurements over time and help organizations identify trends across teams or assessment periods.

Ethical considerations are particularly important when conducting social-engineering simulations. Security exercises should have clear authorization, defined scope, appropriate privacy protections, and safe simulation content. Participants should not be exposed to unnecessary psychological harm, and simulations should avoid collecting actual credentials or sensitive information. Responsible simulation design ensures that the primary purpose remains education and security improvement.

Existing awareness platforms and cybersecurity training systems demonstrate the value of dashboards, simulated exercises, educational modules, and performance reporting. However, organizations may still need to combine different systems for simulation management, training, behavioral analysis, and reporting. The proposed system builds on these concepts by integrating controlled simulation management, awareness education, behavioral metrics, risk analysis, and reporting into a unified defensive platform.

III. System Analysis

System analysis for the proposed platform focuses on identifying the requirements for safe social-engineering awareness assessment. The system should provide authenticated access for authorized administrators and trainers. It should allow administrators to define simulation scope, participant groups, schedules, and safe scenarios. Simulation content should be designed to avoid collecting real passwords or confidential information. The platform should record appropriate interaction and reporting metrics while protecting participant privacy. A training module should provide educational material related to common social-engineering warning signs. The analysis engine should calculate awareness indicators from simulation and training results. Findings should be categorized to identify common behavioral weaknesses and training requirements. A dashboard should display aggregated participation, awareness, reporting, and risk metrics. Historical results should be maintained to evaluate improvement over multiple assessment periods. The system should provide structured reports for security teams and management. Authorization,

privacy, data minimization, and ethical-use controls should be incorporated throughout the system.

Existing System

Existing social-engineering awareness programs commonly depend on classroom training, security-awareness presentations, policy documents, online courses, and periodic quizzes. Some organizations conduct controlled simulations using separate tools to evaluate user responses. Training information and simulation results may therefore be maintained in different systems or spreadsheets. This separation can make it difficult to obtain a complete view of organizational awareness. Basic training programs may measure course completion without evaluating practical behavior. Simulation tools may provide interaction statistics but limited educational analysis. Manual comparison of results across departments or time periods can also require considerable effort. Reporting may involve manually collecting information from multiple sources. Some systems provide limited risk visualization or centralized trend analysis. Privacy and data-retention requirements may also be difficult to manage consistently across disconnected tools. Organizations may therefore struggle to determine whether awareness training is producing measurable behavioral improvement. A unified platform can address these limitations by connecting awareness education, controlled simulation, analysis, and reporting.

Disadvantages of Existing System

- Heavy dependence on traditional awareness training methods.
- Limited practical assessment of user behavior.
- Training and simulation results may be stored separately.
- Difficult to correlate awareness and simulation outcomes.
- Manual analysis can consume significant time.
- Limited centralized visualization of awareness trends.
- Difficult to compare results across assessment periods.
- Report preparation may require manual effort.
- Course completion does not necessarily indicate practical awareness.
- Limited personalized educational feedback.
- Inconsistent data management across different tools.
- Difficult to maintain a unified awareness-risk profile.

Proposed System

The proposed system provides a centralized platform for authorized social-engineering awareness training and controlled attack-simulation analysis. The platform allows security administrators to create safe simulation exercises within a clearly defined organizational scope. Participants can interact with simulated scenarios without being asked to submit real credentials or confidential information. The system records privacy-conscious behavioral metrics such as interaction, recognition, reporting, and training completion. An awareness engine analyzes these results and identifies common security-awareness gaps. Educational modules provide guidance on recognizing suspicious requests, impersonation attempts, unexpected links, attachments, and other warning signs. A risk-analysis component can categorize awareness results according to predefined organizational criteria. The dashboard

provides aggregated statistics, awareness scores, participation metrics, and trend information. Administrators can compare assessment results across departments or different training periods where appropriate. The reporting module generates structured reports for security teams and management. Historical records can be used to measure improvement after additional training. The overall system creates a continuous cycle of simulation, education, measurement, analysis, and awareness improvement.

Advantages of Proposed System

- Provides centralized social-engineering awareness management.
- Supports controlled and authorized simulations.
- Avoids collecting real passwords or sensitive credentials.
- Measures practical user-security behavior.
- Provides centralized awareness and risk analytics.
- Identifies common security-awareness gaps.
- Provides educational feedback after simulations.
- Supports historical performance comparison.
- Provides dashboards and visual reports.
- Supports privacy-conscious and ethical security assessment.

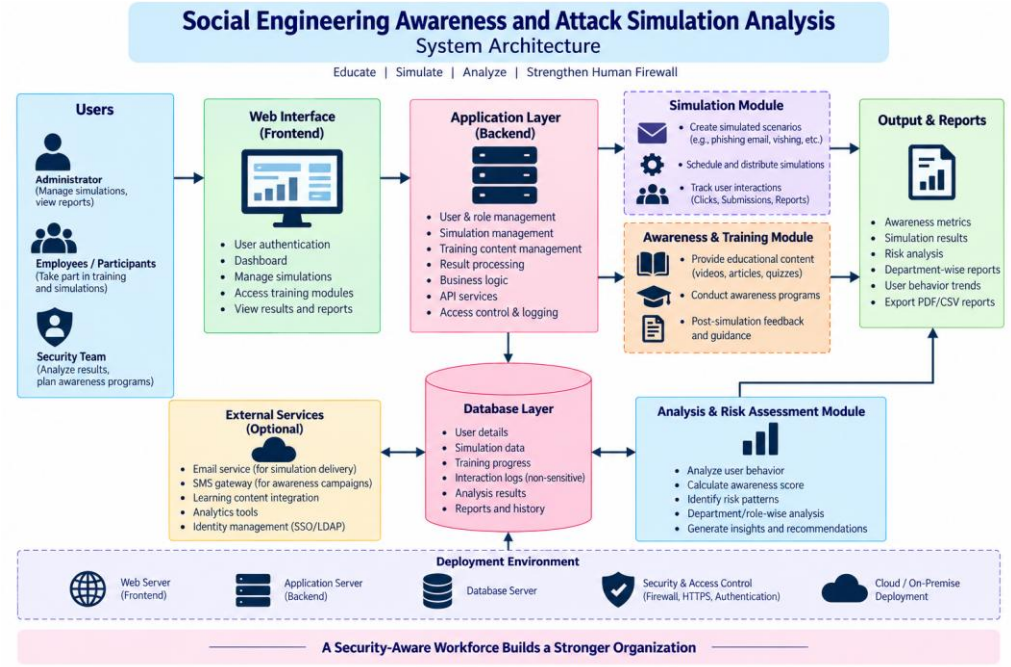
IV. Methodology

The methodology begins by authenticating the administrator and defining the authorized scope of the awareness exercise. The administrator selects an appropriate participant group and configures a safe simulation scenario. The system verifies that the exercise follows predefined authorization, privacy, and safety requirements. Participants receive the controlled simulation through approved communication channels. The platform records only permitted behavioral events required for awareness analysis. No real passwords, authentication secrets, or unnecessary sensitive information are collected. After the exercise, the system provides educational feedback explaining the warning signs within the scenario. Participants can complete awareness modules and knowledge assessments related to social-engineering prevention. The analysis engine calculates aggregated awareness and reporting metrics from the exercise. Results are categorized to identify areas where additional training may be useful. The dashboard presents trends, participation, awareness scores, and training progress. Finally, the system generates reports that support future awareness programs and continuous improvement.

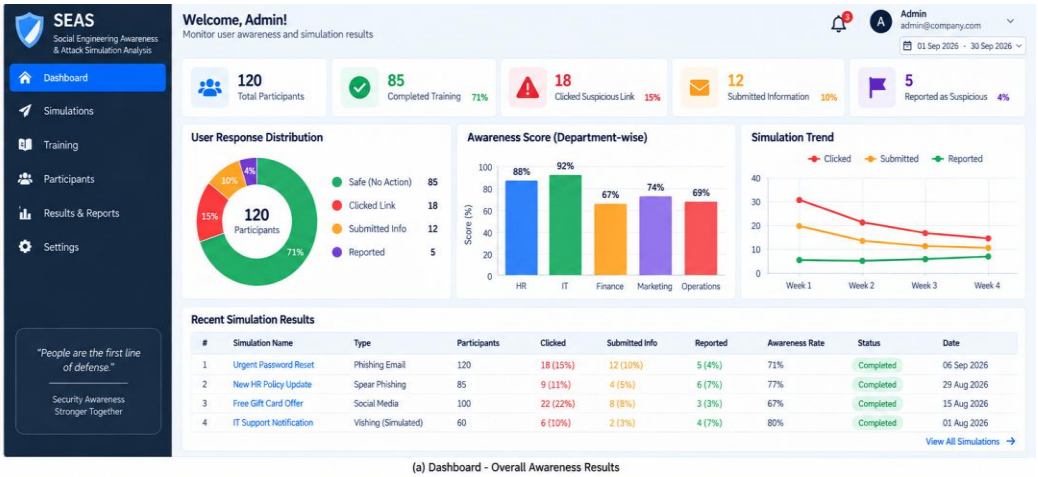
System Architecture

The system architecture consists of multiple interconnected layers that support controlled social-engineering awareness assessment. The User Layer contains authorized administrators, security trainers, and participants who interact with the platform according to their assigned roles. The Web Interface Layer provides dashboards for simulation management, awareness training, results visualization, and reporting. The Application Layer manages authentication, authorization, simulation workflows, participant groups, and system operations. The Simulation Management Layer handles approved and safe awareness scenarios and records permitted interaction events. The Awareness Training Layer provides educational modules,

quizzes, security guidelines, and feedback. The Analysis and Risk Assessment Layer evaluates aggregated behavioral metrics and identifies awareness gaps. The Database Layer securely stores simulation configurations, training records, aggregated results, and assessment history according to defined retention policies. The Analytics and Visualization Layer presents awareness scores, reporting rates, participation statistics, and trends through dashboards. The Reporting Layer generates structured awareness assessment reports for authorized security personnel. Privacy and access-control mechanisms restrict sensitive information according to user roles.



V. Result and Output



(a) Dashboard - Overall Awareness Results

(b) Simulated Phishing Email (Example)

(c) User Reactions - Simulation Results

(d) Output - Generated Awareness Report

VI. Conclusion

The Social Engineering Awareness and Attack Simulation Analysis system provides a structured approach for improving an organization's human-centered cybersecurity defenses. The platform combines controlled simulations, security-awareness training, behavioral analysis, risk assessment, and reporting to help organizations understand how users respond to common social-engineering scenarios.

The proposed system reduces the limitations of traditional awareness programs by providing measurable results rather than relying only on presentations or quizzes. Through dashboards and analytical reports, security teams can identify awareness gaps, evaluate reporting behavior, monitor training progress, and compare results across different assessment periods.

The system also emphasizes ethical, authorized, and privacy-conscious simulation. By avoiding the collection of real credentials and unnecessary sensitive information, the platform can provide practical security education without creating additional security risks. Participants can receive immediate feedback and guidance to improve their ability to recognize suspicious communication.

Overall, the platform can serve as a useful foundation for cybersecurity awareness programs, academic research, organizational training, and defensive security assessment. Future enhancements can include adaptive training, improved behavioral analytics, AI-assisted awareness recommendations, multilingual training content, continuous awareness monitoring, and integration with existing organizational security systems.

References

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.
[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.
[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, “Real-Time Object Detection in Drone Surveillance Using YOLOv5,” in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, “Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks,” in

Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
[7] R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.
[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.
[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.
[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.
[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.