JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A GAMIFIED WEB-BASED SOCIAL ENGINEERING AWARENESS TRAINING PLATFORM

[1]Darren Chetty, [2] Ms. Sehar Khan
[1]MSc Computer Science (Specialization in Cybersecurity), [2]Asst. Professor
[1]Department of Advance computing,
[1]Nagindas Khandwala College, Mumbai, India

Abstract: Social engineering attacks have become one of the most effective cyber threats, as attackers exploit human psychology rather than technical vulnerabilities [1], [12]. Despite the use of advanced cybersecurity tools such as firewalls, intrusion detection systems, and antivirus software, human error remains the leading cause of security breaches [3], [8]. Traditional security awareness programs rely on static training methods such as videos and presentations, which show limited long-term effectiveness [4], [5]. This paper proposes a gamified web-based social engineering awareness training platform that educates users through interactive simulations of phishing, baiting, vishing, tailgating, and pretexting attacks [1], [2]. The system incorporates scenario-based learning, scoring mechanisms, real-time feedback, and behavioural analytics to improve cybersecurity awareness and decision-making [9], [10]. Experimental observations from prior studies indicate that gamified learning significantly improves engagement, retention, and resistance to social engineering attacks when compared to conventional training approaches [6], [11].

Index Terms — Social Engineering, Cybersecurity Awareness, Gamification, Phishing, Human-Centric Security, Web Application

I.INTRODUCTION

Social engineering has become one of the most prevalent and dangerous attack methods in contemporary cybersecurity, primarily because it targets human psychology rather than technical weaknesses in systems or networks [12], [14]. Instead of exploiting software vulnerabilities, attackers manipulate individuals through deception, trust, and persuasion. Common social engineering techniques include phishing emails, baiting through attractive offers or removable media, voice-based fraud (vishing), unauthorized physical access such as tailgating, and impersonation of trusted authorities to extract confidential information from victims [1], [13]. These attacks are particularly effective because they bypass even advanced technical security controls by directly influencing human decision-making.

Numerous studies indicate that organizations with strong technical defenses are still frequently compromised due to insufficient user awareness and poor judgement during suspicious interactions [3], [8]. Employees and users often fail to recognize subtle warning signs in malicious communications, making them vulnerable despite the presence of firewalls, intrusion detection systems, and email filtering mechanisms. This highlights the critical role of the human factor in overall cybersecurity resilience.

Conventional cybersecurity awareness programs typically rely on classroom-based training sessions, informational emails, and video tutorials to educate users about potential threats [4], [5]. While these approaches provide basic theoretical knowledge, they are largely passive and fail to actively engage participants. As a result, users often lose interest quickly and struggle to retain security concepts over time. Furthermore, such methods do not accurately replicate real-world attack situations, leaving users unprepared to respond effectively when faced with actual social engineering attempts [6], [7].

Research in cybersecurity education suggests that interactive and experiential learning techniques are significantly more effective in shaping user behaviour and improving security awareness [9], [11]. By allowing users to actively participate in simulated attack scenarios, these methods promote deeper understanding and practical skill development. Gamification, in particular, has gained recognition as a powerful educational strategy that combines engagement, motivation, and learning reinforcement through elements such as scoring, challenges, feedback, and progression [1], [10].

As a result, gamified training approaches are increasingly viewed as a promising solution for strengthening human-centric cybersecurity defenses. By transforming awareness training into an immersive and interactive experience, gamification helps bridge the gap between theoretical knowledge and real-world application, ultimately reducing user susceptibility to social engineering attacks and improving overall organizational security posture [1], [10].

II.SYSTEM ARCHITECTURE

The proposed system architecture is designed using a modular client–server model to ensure scalability, flexibility, and efficient management of system components. In this architecture, the frontend layer is responsible for delivering an interactive and user-friendly interface that allows users to engage with simulated social engineering scenarios in a seamless manner [2], [10]. This interface facilitates user interaction, scenario selection, and real-time feedback, ensuring an engaging learning experience. The backend layer handles the core system logic, including scenario execution, scoring mechanisms, user session management, and analytical processing of user actions [2], [10].

All user interactions, including decisions made during gameplay, response times, and performance scores, are securely stored in a centralized database [3], [8]. This centralized storage enables systematic analysis of user behaviour and supports the generation of detailed performance reports. By maintaining structured records of user activity, the system allows for long-term tracking of learning progress, identification of recurring mistakes, and assessment of overall awareness improvement [3], [8].

The modular nature of the system architecture allows individual components to be developed, modified, or extended independently without affecting the entire platform [9], [11]. This design approach simplifies the process of adding new social engineering scenarios, introducing additional attack types, or integrating the platform with existing organizational training or learning management systems. As a result, the platform can be easily adapted to meet evolving cybersecurity training requirements and organizational needs [9], [11].

In addition to user-facing components, the architecture includes administrative modules that provide monitoring and management capabilities [6], [14]. Administrative dashboards offer visual insights into user behaviour patterns, performance metrics, and awareness levels across different individuals or groups. These dashboards enable security teams and administrators to identify high-risk users, evaluate training effectiveness, and make informed decisions regarding future awareness initiatives [6], [14]. Overall, the modular client–server architecture enhances system maintainability, extensibility, and effectiveness in delivering human-centric cybersecurity training [2], [10]. The architecture is shown in the Fig 2.1: System Architecture.

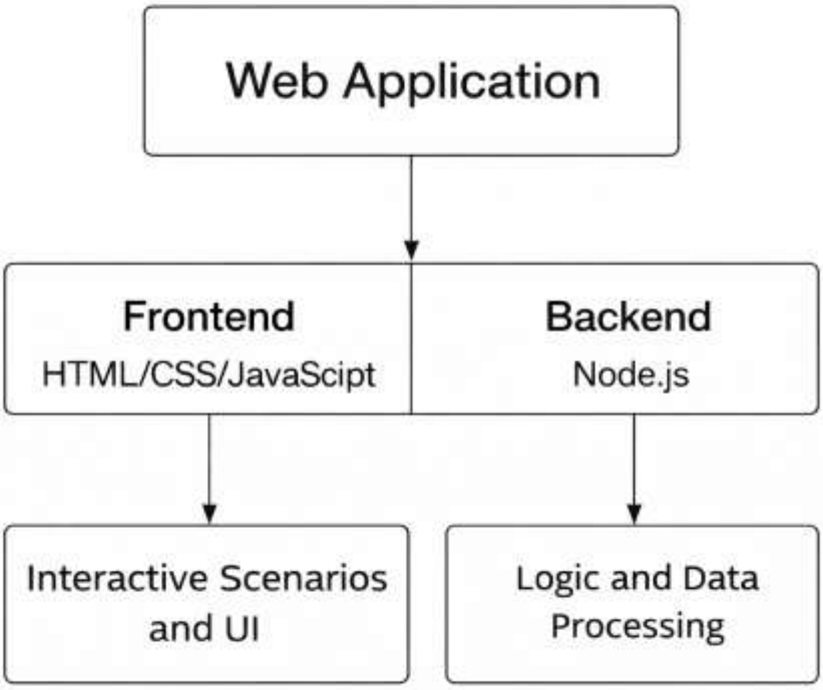

Fig 2.1: System Architecture

III. IMPLEMENTATION DETAILS

The proposed platform is developed as a web-based application that can be accessed through standard web browsers, ensuring platform independence and simplifying deployment across different operating systems and devices [2], [10]. By eliminating the need for specialized software installations, the system allows users to engage with the training environment using commonly available devices such as desktops, laptops, and mobile systems. This design choice enhances accessibility and supports wide-scale adoption within educational institutions and organizational settings.

Users are required to authenticate into the system before accessing the training modules, ensuring controlled participation and secure tracking of individual performance [1], [9]. Once authenticated, users engage in scenario-based gameplay sessions that simulate realistic social engineering attacks. These scenarios are designed to replicate common threat situations, enabling users to experience practical decision-making challenges rather than passive learning. Through repeated interaction with varied attack scenarios, users develop improved awareness and understanding of social engineering techniques [1], [9].

Each action performed by a user during gameplay is processed and evaluated in real time by the system [6], [7]. Immediate feedback is provided after every decision, clearly explaining whether the chosen action was safe or risky and outlining the potential security consequences. This instant feedback mechanism plays a critical role in reinforcing correct behaviour and discouraging unsafe practices, enabling users to learn from mistakes without real-world repercussions [6], [7].

The system incorporates a scoring engine that assigns rewards for secure decisions while penalizing unsafe actions [11], [12]. This scoring mechanism motivates users to actively participate and encourages repeated engagement with the platform. By linking performance outcomes with decision quality, the system reinforces learning through experience and repetition, which has been shown to be effective in behavioural change and skill development [11], [12].

User performance data, including decision history, response patterns, and score progression, is continuously recorded and stored within the system [3], [8]. This data is used to generate detailed analytics reports that allow administrators and security teams to monitor individual and group-level improvements over time. Additionally, the analytics component helps identify high-risk users who may require further training or targeted intervention. Overall, the platform combines accessibility, real-time feedback, gamification, and behavioural analytics to deliver an effective and scalable solution for social engineering awareness training [3], [8].

IV. RESULTS AND DISCUSSIONS

Prior research on gamified cybersecurity awareness platforms has consistently shown that such approaches lead to a measurable reduction in users' susceptibility to phishing attacks and other risky online behaviours [1], [6]. Studies indicate that individuals who undergo training through interactive simulations develop a stronger ability to identify deceptive tactics commonly used by attackers, such as spoofed emails, impersonation attempts, and psychological manipulation techniques [13], [14]. In addition to improved threat recognition, trained users are more likely to report suspicious activities rather than ignore or engage with them, contributing to a more proactive security posture [13], [14].

Gamification has also been widely recognized for its ability to enhance user engagement and motivation when compared to traditional awareness methods such as lectures, presentations, or video-based training modules [9], [11]. By incorporating elements such as scoring, feedback, challenges, and progression, gamified platforms encourage sustained participation and repeated interaction, which are essential for effective learning and behavioural change [9], [11]. This increased engagement directly contributes to higher knowledge retention and improved application of security principles in real-world situations.

Behavioural studies further suggest that repeated exposure to realistic attack scenarios significantly enhances decision-making accuracy and strengthens long-term retention of cybersecurity concepts [7], [12]. As users encounter similar threat patterns multiple times in a controlled environment, they develop cognitive familiarity and confidence in responding appropriately. These findings collectively support the effectiveness of the proposed gamified approach, demonstrating its potential to strengthen human-centric cybersecurity defenses by addressing the psychological and behavioural dimensions of security awareness [1], [10].

V. FUTURE ENHANCEMENTS

Future improvements to the proposed platform may focus on the incorporation of artificial intelligence techniques to enable the dynamic generation of adaptive training scenarios based on individual user behaviour, performance trends, and assessed risk profiles [10], [12]. By leveraging AI-driven models, the system can tailor scenario difficulty and content to address specific user weaknesses, thereby enhancing the effectiveness of personalized cybersecurity training. Such adaptability would allow the platform to respond to evolving threat patterns and user learning needs in real time.

Expanding the platform to include mobile application support represents another significant enhancement. A dedicated mobile version would increase accessibility and encourage more frequent user participation by allowing training to be conducted on smartphones and tablets [11], [14]. This mobility would be particularly beneficial for organizations with remote or hybrid work environments, where consistent access to training resources is essential.

Additionally, the integration of advanced analytics tools could provide deeper insights into user behaviour, training effectiveness, and organizational risk levels [3], [8]. By combining detailed behavioural metrics with visualization dashboards, administrators could make informed decisions regarding targeted interventions and policy improvements. Integration with existing Learning Management Systems would further improve scalability and streamline deployment across large institutions, enabling seamless incorporation of the platform into established training frameworks [3], [8]. Collectively, these enhancements would strengthen the platform's adaptability, reach, and long-term impact on cybersecurity awareness.

VI. CONCLUSION

The findings of this research clearly indicate that a gamified, web-based approach to social engineering awareness training delivers significantly better outcomes when compared to conventional training techniques [1], [6]. Unlike traditional methods that rely on passive instruction, the proposed approach actively engages users by placing them in realistic threat scenarios that closely mirror real-world attack situations. This experiential learning model enables users to better understand attacker strategies and respond more effectively to potential threats.

By integrating interactive simulations, immediate feedback mechanisms, and behavioural analytics, the proposed system enhances user awareness and strengthens decision-making capabilities in security-critical situations [9], [11]. Real-time feedback allows users to instantly recognize mistakes and understand the consequences of unsafe actions, while behavioural analytics help track progress and identify recurring weaknesses. This combination promotes continuous learning and reinforces correct cybersecurity practices over time.

Furthermore, the platform is designed to be scalable and adaptable, making it suitable for deployment across a wide range of environments, including educational institutions, corporate organizations, and training programs [12], [14]. Its web-based nature ensures ease of access and simplifies integration into existing infrastructures without requiring specialized hardware or complex installation processes. Overall, the proposed system provides a practical and effective solution for addressing human-centric security challenges, emphasizing the importance of strengthening the human element in cybersecurity defense strategies [12], [14].

REFERENCES

[1] L. Kassner and A. Schönbohm, "A Serious Game to Improve Phishing Awareness," in *Proceedings of the International Conference on Human Aspects of Information Security*, Springer,2024.https://www.researchgate.net/publication/365647425_A_Serious_Game_to_Improve_Phishing_Awareness

[2] T. Li et al., "Security Awareness Adventure: A Serious Social Engineering Game," *Computer Law & Security Review*,Elsevier,2025. https://www.sciencedirect.com

[3] G. Ho, A. Mirian, E. Luo et al., "Understanding the Efficacy of Phishing Training in practice," in *IEEE Symposium on Security and Privacy*,IEEE,2025. https://www.researchgate.net/publication/392739544

[4] D. Hillman, "Evaluating Organizational Phishing Awareness Training," *Computers & Security*,Elsevier,2023.https://www.sciencedirect.com

[5] "Assessing the Efficacy of Security Awareness Training in Mitigating Phishing Attacks: A Review,"ResearchGate,2025. https://www.researchgate.net/publication/392495542

[6] A. Yasin, "What Goes Wrong During Phishing Education?," *Computers & Security*, Elsevier,2024. https://www.sciencedirect.com

[7] E. N. M. Le-Nye, "Evaluating Phishing Awareness Strategies: A Comparative Study," *Procedia Computer Science*,Elsevier,2024. https://www.sciencedirect.com/science/article/pii/S1877050924034008

[8] J. Prümmer, "A Systematic Review of Current Cybersecurity Training Methods," *Computers & Security*,Elsevier,2024. https://www.sciencedirect.com/science/article/pii/S0167404823004959

[9] D. C. Tatum, "Gamification of Cyber Security Awareness Training Programs," Doctoral Dissertation, Middle Georgia State University,2023. https://comp.mga.edu/static/media/doctoralpapers/2023_Tatum_0516152056.pdf

[10] "Gamified Tailored Roleplay Story-Based Phishing Awareness Training," ResearchGate, 2025.https://www.researchgate.net/publication/383104568

[11] J. Nijland, "Gamification of Cyber Security Awareness Training for Students," Bachelor's Thesis, University of Twente,2022. https://essay.utwente.nl/89424/

[12] M. Alomair et al., "Key Factors Influencing Employees' Awareness of Social Engineering Attacks,"*Heliyon*,Elsevier,2025. https://www.sciencedirect.com

[13] L. Burita, I. Klaban, and T. Racil, "Education and Training Against the Threat of Phishing Emails,"ResearchGate,2025. https://www.researchgate.net/publication/359032741

[14] Z. Morić et al., "Exploring End-User Defensive Approaches Against Phishing Attacks," *Future Internet*,MDPI,2025. https://www.mdpi.com/2624-800X/5/3/38

[15] L. Hafner et al., “TASEP: A Collaborative Social Engineering Tabletop Game,” *arXiv preprint*,2023.https://arxiv.org/abs/2308.15161