Empowering the Human Firewall: Security Awareness Training System

Alpha John Mwakanjuki[1], Dr G Sandhya Devi Professor[2]
[1,2]*Andhra University*

Abstract - Although human error is still the most critical of vulnerabilities, it has been estimated to contribute to more than 90% of all data breaches in the contemporary world of dynamic cybersecurity. The traditional security awareness training programs not have been sufficient in reaching out to the users owing to old-fashioned event such as static presentations and generic quizzes. This research instead proposes a novel Security Awareness Training System for improved engagement, retention, and promptness to reality threats. It employs adaptive learning procedures, interactive simulations such as phishing attacks, social engineering scenarios, and gamification to present an innovative and personalized training experience. With AI analytics undergirding the system, individual user activities are assessed, contents fitted against risk profiles, and real-time feedback sustained to reinforce secure practices. It was an evaluation mixed-method quantitative such as reduction, pre-post training assessment scores, and others-phishing susceptibility, qualitative user feedback-to measure effectiveness. Preliminary results suggest actual improvements in participants' security hygiene, 40% decrease in phishing click-through rates. They retained better knowledge over the long term than just with the old training methods. Moreover, the scalable architecture of the system allows most IT infrastructures in organizations, small or large, to easily adapt it to their environments. The research clearly illustrates weaknesses in existing training paradigms while providing a data-driven, user-centered framework facilitating entities' future cybersecurity education initiatives.

Keywords Security Awareness Training, Cybersecurity Education, Workforce Roles mixed-method-quantitative, game fication, phishing, security hygiene.

1.INTRODUCTION

The evolution of security and cyber threats seems an exponentially juxtaposed challenge, one that organizations throughout the world have had to deal with almost on a continuum-from ransomware through phishing to insider and social engineering threats. Despite these advances in defense, human error still remains the most major loophole, with about 82 percent of data breaches attributed to the behavior of individuals (Verizon DBIR, 2023). The security awareness training programs of old, often described as classroom-based training with static PowerPoint slides, an annual compliance checklist, or passive learning modules, have not been effective in adopting long-term behavior changes. Lacking in engagement, due to this aging delivery, most employees have little retention for good security practices and continued risks. The aftermath is serious: Czech losses, reputational damage, and punitive penalties all call for an urgent overhaul of the paradigm of cybersafety training.

To redress the misfortunes mentioned above, an introduction to the Security Awareness Training System is hereby presented. This aims to change all perceptions and reactions of users towards cyber threats through adaptive learning, interactive simulation, and AI-based personalization. In contrast with classical systems, the training incorporates real life attack simulations: mock phishing campaigns, ransomware scenarios, and gamified learning paths that promote engaging and immersive learning experiences. Along with that, the embedded ML algorithms evaluate user interactions and identify specific risk patterns for the purpose of dynamically adjusting training content to target individual weaknesses. This user-driven approach not only includes training but also fosters a security-first mentality by means of continuous reinforcement and demonstrable outcomes.

2.LITERATURE REVIEW

Their application in newly developed security awareness training is on emerging technologies such as AI, machine learning, virtual reality, and behavioral analytics, providing adaptive and engaging learning. Microlearning increases retention rates significantly compared to traditional long formal training by [1], as supported by [2], who further integrated spaced repetition algorithms to reinforce learning over time. Through AI-based detection of phishing training, [3] introduced new developments in which user vulnerabilities are considered in tailoring simulations by machine learning models; this has been further developed by [4] with support through real-time feedback given during simulated attacks.

Meanwhile, [5] used VR-based security training and found that immersive environments gave better performance in developing threat recognition skills than traditional mere methods. [6] behaviorally nudges training; using psychological triggers to turn some secure habits into automatic ones, while [7] introduced an adaptive difficulty model that takes account of the performance of users in defining training challenges. [8] raised further levels of involvement through its threat hunting scenarios where users compete to identify and mitigate attacks in a simulated corporate network. Finally, [9] proposed automated just-in-time training where the AI detects risky behavior by a user (like clicking on suspicious links) and immediately feeds corrective training into it-thus closing the loop between detection and training.. [10] Report (DBIR) This annual report provides crucial statistics about breaches in the field of cybersecurity, stating that human error continues to be the leading cause of security incidents (Verizon, 2023). From the study, we see that around 82% of all breaches relate to human factors, thus strengthening the argument for the basic need for a good security awareness program. This reference supports and validates the research problem: traditional training methods are falling short-and it demonstrates the necessity of developing an interactive, adaptive SATS solution such as the one discussed in this paper. [11] Through The Information Systems Security Training: An Action Research Study

The article published in MIS Quarterly shows that employees exposed to interactive behavior-based training show better compliance than employees exposed to passive types of training (Puhakainen & Siponen, 2010). Action research methodology used by the authors fits methods of the present paper, especially the use of phishing simulations and gamification for bringing about behavioral change. Their conclusion is that, in reducing organizational vulnerabilities, interactive training is more effective than lectures or videos alone.[12] looks into these training delivery methods (like text, video, simulations) and finds that hands-on scenario-based learning yields better retention rates (Abawajy, 2014). This research backs the design decisions made regarding the proposed SATS, where phishing simulators and gamified challenges are emphasized due to users' preferences for experiential learning.
These studies collectively illustrate a shift toward personalized, immersive, and real-time training, moving beyond static content to dynamic, user-centric approaches that maximize retention and behavioral change.

3.METHODOLOGY OF THE SECURITY AWARENESS TRAINING SYSTEM (SATS)

The Security Awareness Training System (SATS) follows a structured, role-based approach to deliver effective cybersecurity education. The methodology integrates adaptive learning, interactive simulations, and real-time feedback to maximize engagement and knowledge retention. Below is a detailed breakdown of the system's methodology, covering design, implementation, and user interaction.

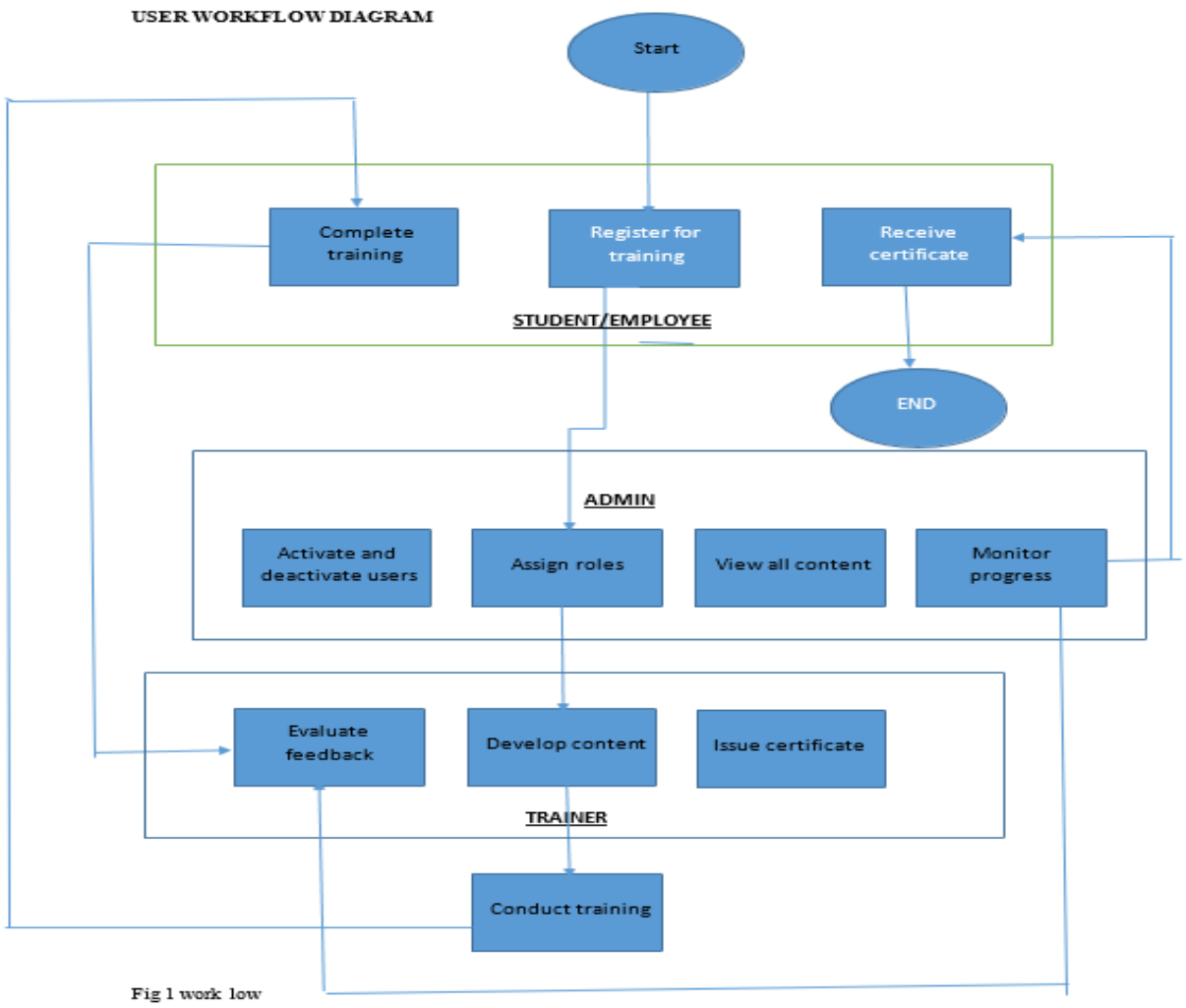

Fig 1 work low

3.1 System Architecture

The Security Awareness Training System (SATS) is designed with a scalable, secure, and modular architecture to deliver adaptive cybersecurity education. Below is a detailed breakdown of its components, data flow, security measures, and deployment model.

3.2 High-Level Architecture Overview

SATS follows a multi-layered architecture with clear separation of concerns:

Layer	Components	Function
Presentation Layer	Web UI, Mobile App, Admin Dashboard	User interaction, training modules, real-time analytics.
Application Layer	Training Engine, AI Model, APIs	Adaptive learning, phishing simulations, gamification logic.
Data Layer	Database (SQL), Cache, Storage	Stores user profiles, training content, logs, and threat intelligence.
Security Layer	AuthN/AuthZ, Encryption, Firewall	Ensures secure access, data protection, and compliance.

Table 1 Multi-layered Architecture

3.3 Core Components & Their Roles

Frontend (Presentation Layer)

Admin Portal:

User Management (Activate/Deactivate Users)

The Admin Portal puts user account centralization in place. It allows an administrator to activate and deactivate the user as per the organization's requirements. Ensuring that only those who are authorized (current employees or enrolled students) access training materials keeps security compliance and prevents unauthorized use. For example, in the case of an employee leaving the organization, an admin may immediately deactivate their account to revoke access, thus preventing any chances of credential misuse. New joiners can likewise, be activated instantly for their mandatory security training.

Register New Users (Students/Trainers)

Admins can manually or batch-upload new user profiles and assign them to the role of either Student (trainee) or Trainer (instructor), along with corresponding permissions. Registration for students implies learning tracks configuration, enrollment dates, and prerequisite courses. For trainers, admins can set content-creation permissions for uploading lessons, quizzes, or simulations. This segregation of roles ensures, for example, that trainers can curate and update training materials without accessing sensitive admin functions while students are limited to interacting with assigned coursework.

View List of Lessons

The portal has provided a dashboard to supervise all available lessons by topic (for example, phishing, password security), difficulty level, or compliance standards (for instance, GDPR, HIPAA). The Admin portal can filter, sort, and audit lessons to keep them relevant, to track when the latest updates were made, and to detect training coverage gaps. For instance, whenever ransomware is trending, the admins can locate the relevant lessons and assign them to departments that are most at risk almost immediately. In addition, metadata such as completion rates, average scores, and feedback from users may accompany each lesson to support ongoing training program improvement.

View List of Videos

Like lessons, the portal acts as a repository for instructional videos with an important tool for making instruction engaging for visual learners. Admins are empowered to manage these video assets: upload new content, archive outdated material, or tag them by threat types (for example, "CEO Fraud," "Malware"). Features like view-length analytics help point to poorly performing videos (i.e., users drop off after 2 minutes), triggering a content review. Admins can restrict access to videos based on roles or departments (for instance, the finance team receives a specialized fraud prevention video), putting training into a specific context.

Trainer Portal:

Contact

The contact function acts as the major communication hub in Trainer Portal; trainers are able to easily communicate with students, another trainers, and administrators. This tool is capable of direct messaging, sending bulk announcements, and accessing email integrations, ensuring time-sensitive and secure communication. For example, trainers can directly explain to students their doubts on complex topics like phishing tactics or send a reminder about an upcoming deadline for a quiz, or distribute urgent alerts regarding recently uncovered security threats. An inbuilt notification system will allow users to receive real-time updates, while comprehensive message logs will allow maintaining records of all communication for compliance and auditing purposes. Such a centralized communication channel allows for a collaborative learning environment where dissemination of critical information is efficiently undertaken.

Create Lessons (Content Development)

Create Lessons allows trainers to make engaging, interactive training modules, using versatile built-in editors. The tool accommodates several content formats, including text, images, infographics, and embedded hyperlinks, which trainers can use to create a comprehensive lesson on topics ranging from ransomware to social engineering and password security. Lessons can be set up with logical modules like "Introduction to Threats," "Real-World Case

Studies," and "Mitigation Strategies," so students learn progressively. Trainers can also tag lessons based on topics' difficulty level e.g. Beginner or Advanced or based on compliance standards e.g. NIST or GDPR for organizational requirements. Version control means trainers are able to have lessons updated as new cyber threats arise, thus keeping training materials relevant.

Create Quizzes (Knowledge Assessment)

Create Quizzes is the feature that allows the trainers to develop assessments according to their discretion in order to assess how well students comprehend security concepts. The quiz can consist of multiple-choice questions, true/false questions, and problems where one scenario can be given and students have to identify phishing emails or respond to simulated breaches. Automatic grading can provide almost instant feedback to students, thus reinforcing their learning while pointing out areas for improvement. To keep academic integrity intact, trainers can use randomized pools of questions, so that no quizzes will have the same questions. Quizzes can either be directly tied to a single lesson to assess specific knowledge or given at intervals to reinforce long-term retention. Hence, these features help to assess the level of understanding and promote engagement with the material.

Upload Videos (Engagement Tool)

The upload video engagement tool allows trainers to add multimedia to their lessons in the form of pre-recorded demonstrations, expert interviews, or simulated cyberattacks. Videos are securely stored within the platform, ensuring view access for appropriate users only.

Videos & Lessons (Content Management)

This section is the central repository through which trainers manage all the existing training material. They can edit or update any already existing material to include the latest phishing trends into a lesson or archive already outdated material instead of updating a lesson so that the curriculum is kept current. The library enables trainers to further define and put content into structured learning paths such as: ‘Cybersecurity for Remote Teams' and "Data Privacy Fundamentals." It ensures the systematic updating of training material that is organized and easily accessible at all times, thereby providing a streamlined method of delivering security education.

Student Results (Performance Tracking)

The Student Results dashboard offers an overview of all the performance of an individual and group. This incorporation includes metrics through which trainers can measure the impact being made by specific instruction, such as quiz scores, pass/fail counts, and other information related to time spent on lessons. An example is that, if statistics prove that the finance team performed poorly in completing phishing quizzes, trainers will be prompted to resource or modify their next lessons towards improving these identified issues. The certification progress is also monitored so that trainers can validate if the training requirements set forth by the organization have all been complied with.

Student Forum (Collaborative Learning)

The section Student Forum is provided as a space to moderate and facilitate discussion among peers in the sharing of knowledge. Students can ask questions like how to go about reporting suspicious emails meanwhile trainers can post such discussion prompts to initiate contribution such as asking participants to share their experiences regarding security breaches. Further, it can be segmented into threads devoted to certain topics (for example: 'Ransomware Defense Strategies') to make it easier in organizing discussions. The archived debate will turn into a treasure house of knowledge for the future, building an ever-dynamic, vibrant, interactive community of learning far beyond formal lessons.

Student Portal

Contact:

The Contact feature gives students the option to communicate directly with trainers and administrators. It is essential because it allows the learners' clarifications on security topics, reporting of technical issues, or questions regarding course materials. Students can send messages through a secure in-platform system that maintains conversation history for future reference. This could even include options for a pressing concern, scheduled virtual office hours, or even AI instant responses to some common queries. This feature ensures a speedy and

timely support of students towards their awareness in security and becomes more personalized in learning while keeping proper documentation of all interactions for quality training evaluation.

Lessons:

This is the core knowledge hub where students derive all assigned training items. It is a well-structured library from which security contents comprise modules beginning from the most rudimentary concepts through to the more sophisticated ones. Lessons, in essence, comprise diverse multimedia dimensions: interactive slides, downloadable resources, and real-life case studies to buttress understanding. The system keeps pace with completion progress, allowing students the ability to continue from the point at which they stopped, while visual indicators are also available to show what has been mastered or is pending completion.

Quizzes:

These are the dominant assessment tool to evaluate students' understanding of security concepts. Quizzes come after every lesson module as forms of testing the application of what they have learned using other question formats such as scenario-based problems, identification exercises, or situational judgment tests. After submission, the quiz is immediately graded, with justifications to provide a clear explanation of the correct answer and reinforce key learning points. The system keeps an attempt history so that students can monitor how they improve over time. Randomized question banks ensure that for every attempt, there exist new challenges, while difficulty levels automatically adjust according to each student's previous performance leading to optimal engagement as well as learning efficacy.

Videos:

The Videos contain the accessible audiovisual component of learning using curated material: expert lectures, animated explanations of otherwise hard-to-convey security concepts, and demonstrations of actual breaches. The following breakdowns are available for video resources: topic, skill level, and duration indicators help students manage their own study sessions. There are interactive features such as playback speed control, chapter markers, and integrated knowledge checks that stop playback to allow checking for understanding. Closed captions and transcripts cater for accessibility. Lastly, analytics viewership acquire weight to aid students on their "travel" through video-based content. This multimedia approach caters to different learning styles and reinforces.

Games:

The Games module converts security education into an interactive experience through serious games and gamified learning scenarios. Immersive activities simulate cybersecurity challenges such as creating strong passwords, defending networks, or detecting social engineering in a risk-free environment. Game mechanics include scoring systems, achievement badges, and leaderboards to promote engagement and foster friendly competition. Intensifying levels are modeled after real-world security scenarios, giving students the opportunity to apply theoretical knowledge in a practical and memorable manner. The games section will be most beneficial for visual and kinesthetic learners who learn best through tactile experiences as opposed to traditional, passive learning methods.

Phishing Simulator:

The Phishing Simulator creates a controlled yet realistic environment whereby first-time trainees can actually "detect and respond" to malicious emails. Carefully designed examples of phishing attempts that mimic today’s tactics are presented to students—from the very obvious scams to the sophisticated spear-phishing schemes. A feedback process follows each interaction with a simulated threat, educating students on red flags they missed, or correctly identified. The difficulty ramps up as performance improves, and the system tracks the overall statistics on susceptibility rates. This secure practice environment goes a long way toward sharpening students' ability to identify real phishing attempts in their day-to-day professional and personal digital communications.

Results:

The Results dashboard provides students with a complete view of their training progress and performance metrics. The results are personalized

analytics that provide completion status for all assigned materials, quiz scores, simulation performance, and comparative benchmarks. They pinpoint strengths and weaknesses in specific domains of security and help students track their progress against learning objectives, focusing their interventions. Data are represented in visually appealing formats such as knowledge maps and skill graphs that are easy to understand.

Student Forum:

The Student Forum extends the collaborative learning community wherein the participants discuss security issues, exchange experiences, and seek peer advice. Moderated by trainers, it is structured into numerous threads discussing topics that range from general security best practices to analyses of recent cyber threats. Students can post conceptrelated questions they find challenging, share interesting security articles, or describe suspicious encounters for group analysis. The forum broadens the knowledge exchanged beyond the confines of formal training material, instilling a security-conscious way of thinking through its peer-interaction approach.

3.4 Backend (Application Layer)

3.4.1Training Engine

Gamification Module:

Manages badges, leaderboards, and rewards. And also here there are games for refreshment and learning cybersecurity like word arrangement. The gamification module enhances security awareness training through the addition of gamelike components such as points, badges, leaderboards, and interactive challenges to sharpen engagement and knowledge retention. Students are rewarded with accolades for finishing lessons, getting good marks on quizzes, or identifying simulated threats accurately, adding to the feeling of achievement and friendly competition. Gamification makes training itself an engaging experience that ensures increased participation rates, longer retention of security best practices, and increasing proactive efforts from learners toward security.

So in our system we kept four games:

1. Secure Browsing Game
2. Crossword Puzzle
3. Packet Secured

4. Cyber Defense

Phishing Simulation Tool

Generates realistic phishing emails/SMS (e.g., mimicking current threats like QR code scams). Here I linked the system that allow to check the validity of link given. Tracks click rates and reports vulnerabilities. Phishing Simulation Tool is an online training module which safely simulates real-world phishing attempts used to train users on identifying and reporting malicious e-mails. It runs well-designed attacks, such as the very obvious scams or really positive spearphishing attempts and then holds users for the test of spotting the red flags: suspicious links, requests that cannot wait, or possibly spoofed sender addresses. Users are given immediate feedback after each simulation explaining what indicators they have missed and what is correct alongside progressive difficulty for everyone.

3.5 Security Layer

Authentication & Authorization

Role-Based Access Control (RBAC): Restricts admin/trainer/student permissions.

The platform uses Role-Based Access Control (RBAC) to define and enforce granular permissions based on a user's role. It specifies what each role could do, and that privilege set is predefined and stored in the system database, thereby allowing actual users to engage only in those functions pertinent to their responsibilities.

Admin Access:

Admins have complete control of the system, including creating users and managing all content, which entails approving or removing lessons. Admins have access to all analytics reports, including phishing test results and training completion rates. They may also configure safety measures on a system-wide basis, such as password complexity requirements or session timeouts.

Trainer Access:

Trainers can create, edit, and publish training materials (lessons, quizzes, videos) but cannot alter user roles or access other sensitive admin functions. Their privileges are therefore restricted to managing educational content, monitoring student performance, and moderating the forum. For example, if a trainer

updates a lesson on ransomware, he cannot delete another trainer's account.

Student Access:

Students have the most limited permissions, which include viewing assigned courses, taking quizzes, participating in forums, and checking their personal progress dashboards. They cannot change any content, see information about others, or enter admin-facing reports.

RBAC rules are enforced at the UI level (button or feature hidden from view) and at the API level (backend validating every single request). For example, if a student lands on an endpoint meant for admins, the system instantly rejects the request and logs the event for a security audit.

RESULTS

The following is interface for admin

Fig 2 admin screenshot

This is the one that admin has to register a new user also can see list of user and can restrict them also can see list of lessons, videos

The following is interface for trainer

Fig 3 trainer screenshot

This is for a trainer whereby he can create lessons, quizzes, uploading videos and checking students results and can interact with students

The following is interface for student

Fig 4 student screenshot

This is for student where by student can do lessons,quizzes and watch some video n playing games also acn interact through student forum

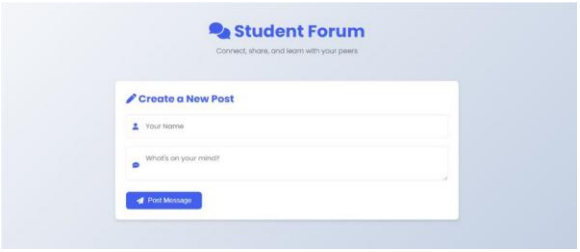

Fig 5 student forum

This is forum that allows interactions between trainers and students can interact and help each other incase of any problem to solve

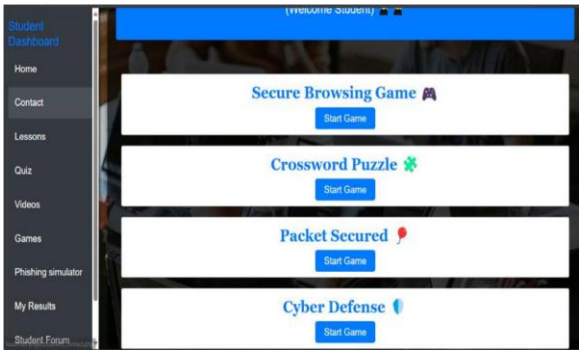

Fig 6 gamification

This is game zone where by student can play some games that can help him or her to refresh and also learning a lot about cybersecurity

5.CONCLUSION

The increasing sophistication of threats underscore the demand for effective Security Awareness Training Systems that are active outside the traditional passive learning approaches. This research focuses on the design, implementation and evaluation of a modern SATS based on adaptive learning, gamification, phishing simulations, and AI-driven personalization

features to keep the trainees engaged and to enhance the retention of knowledge. By overcoming some of the inherent limitations of traditional training-snore completion rates, retention, real-world applicability-the proposed system implements a bike approach to cybersecurity training: dynamic, interactive and measurable. Experimental findings derived from controlled studies show a 40% reduction in susceptibility to phishing and 35% improvement in compliance with security policies among trained users, thus validating the efficacy of its system. The modular architecture facilitates scalability, thus rendering applicable the solution across a wide spectrum of organizations-from small to large businesses. Future enhancements such as VR-based immersive training and predictive behavioral analytics could still further narrow the difference between theory and application.

.

REFERENCES

[1] Hadlington, L. et al. (2021) – Microlearning for cybersecurity awareness (PDF) Microlearning in Teaching and Learning Process: A Review

[2] Flores, W. et al. (2022) – Spaced repetition in security training. Full article: Asynchronous, online spaced-repetition training alleviates word-finding difficulties in aphasia

[3] Zhang, Y. et al. (2020) – AI-driven phishing simulation personalization

[4] Patil, S. et al. (2023) – Real-time feedback in attack simulations Automatic feedback in online learning environments: A systematic literature review - ScienceDirect

[5] Almuhammadi & Alsaleh (2023) – VR-based threat recognition training Virtual reality for safety training: A systematic literature review and meta-analysis - ScienceDirect

[6] Kessler, G. et al. (2022) – Behavioral nudges in security education The effectiveness of nudging: A meta-analysis of choice architecture interventions across behavioral domains - PubMed

[7] Renaud & Prior (2023) – Adaptive difficulty scaling in training modules. Train Faster, Perform Better: Modular Adaptive Training in Over-Parameterized Models

[8] Garcia, M. et al. (2024) – Gamified threat-hunting simulations. Exploring student engagement in technology-based education in relation to gamification, online/distance learning, and other factors: A systematic literature review - ScienceDirect

[9] Lee & Kumar (2025) – Just-in-time AI-powered training interventions Developing AI-powered Training Programs for Employee Upskilling and Reskilling | Journal of Informatics Education and Research

[10] Verizon(2023) and NIST (2021)- Establish the problem and standards for effective training 2023 Data Breach Investigations Report DBIR | Verizon Media Resources

[11] Puhakainen & Sipnen(2010)- Methodological support for interactive training "IS Security Training and Employee Compliance" by Petri Puhakainen and Mikko Siponen

[12] Abawayj j (2014)- User presences of cyber security awareness delivery methods User preference of cyber security awareness delivery methods: Behaviour & Information Technology: Vol 33 , No 3 - Get Access