Human Factors in Network Security: Social Engineering Defenses and Security Awareness Training

Prakriti Dhungel
Computer Science and Engineering
University of North Texas
Denton, Texas
prakritidhungel@my.unt.edu

Ashwini Gondhi
Computer Science and Engineering
University of North Texas
Denton, Texas
ashwinigondhi@my.unt.edu

Song Dang
Computer Science and Engineering
University of North Texas
Denton, Texas
songdang@my.unt.edu

Abstract— **The use of human behavior has become a common attacker in social-engineering attacks thus making users an important target to network security. Current literature demonstrates that conventional training usually gives short-term gains and is not realistic and does not respond to organizational and psychological considerations, particularly in the face of developing AI-based phishing attacks. The paper analyses major literature on social-engineering defenses and establishes the major gaps such as a lack of long-term assessment and user interaction. To address this, we have suggested a multi-layered, human-centric design that is a combination of behavioral evaluation, adaptive training, AI-generated phishing simulations, and organizational culture reinforcement. It is aimed at helping to maintain the resilience of users and increasing the organizational protection against a changing social-engineering attacks.**

Keywords— Social engineering, cybersecurity awareness training, human factors, phishing attacks, AI-generated phishing, behavioral assessment, security culture, adaptive training, network security, deep learning–based detection.

I. Introduction

With the current digitalized world where the world is interconnected, organizational security cannot be achieved through technological means alone, due to the changing nature of cyber threats. This is because human behavior has been one of the most abused weaknesses in network security and therefore social-engineering attack especially phishing is the primary cause of security breach. Recent research (Rathod et al., 2025; Khadka et al., 2025) stresses that, in an increasing number of cases, the attackers learn to use psychological manipulation, urgency, and trust to trick people into making the secure systems vulnerable. With the development of artificial intelligence, nowadays, users can have more convincing and adaptive phishing messages (Nature Human Behavior, 2025), which prompts the development of more efficient human-related countermeasures. Security-awareness training (SAT) has become an important defense mechanism that can be used to enhance the capability of the users to identify and resist social-engineering tricks. The systematic reviews and meta-analyses prove that the training programs can help significantly decrease the risk of the user behavior (Prümmer, J., 2024) when they are combined with simulation-based exercises and regular reinforcement. Tailored and context- specific training is shown to result in long-term changes in behavior (Longitudinal studies (Ho et al., 2025)) and the need to evaluate actual outcomes instead of self-reported awareness is evident in scoping reviews (Marshall et al., 2024).

Figure 1: Social Engineering Awareness (Mba, 2025)

Furthermore, interdisciplinary views (Khadka et al., 2025) indicate that organizational culture, motivation, and cognitive biases are some of the major factors in defining training efficacy.

Hence, the current research project investigates the human factor in network security, design and effectiveness of social-engineering protection and security-awareness training. Through the synthesis of emerging research results, the proposed study will help determine strategies, which can improve user resilience, security-conscious behavior, and minimize exposure to contemporary social-engineering threats in networked settings.

II. Literature Review

A. Research Synthesis

One of the most exploitable areas of vulnerability in contemporary cybersecurity has been human behavior. Incorporated in all sectors, social-engineering techniques, including phishing, pretexting, manipulation, and other methods, have become increasingly favored by attackers to circumvent technical controls and contributor to the victims among unsuspecting users. Development of artificial intelligence has augmented the authenticity and steadiness of these assaults further and user-oriented defenses have never been as crucial as they are at present. This literature review is the synthesis of seven scholarly articles that discuss the subject of cybersecurity training approaches, phishing perception, social-engineering strategies, the aspect of human behavior, and new technical solutions like deep-learning-based detection. A combination of these studies reflects the potential and the shortcomings of current strategies and the necessity of better, more integrated strategies to lessen the human risk factor.

B. Training Efficacy

Sometimes, computer technologies are viewed as efficient solutions to prevent cybercrimes. human Cybersecurity Training Approaches (Based on Prummer et al., 2023). Prummer et al. (2023) present a background knowledge on cybersecurity training effectiveness by conducting a large-scale systematic review of the existing relevant literature on training programs that included more than 16,000 initial publications and then reduced the sample to 142. The conclusions made in the review were that cybersecurity training can positively influence user awareness and security behavior in the short term. Other strategies like game-based learning, scenario-based simulations and interactive modules were especially useful in ensuring user engagement. Nevertheless, the authors note that most studies have severe methodological shortcomings such as small sample sizes, use of students rather than employees, and short-term assessment. Consequently, although training has proven to enhance the awareness its long-term behavioral effect is still unclear and this leaves a gap that future research seeks to fill.

C. Phising Specific Training

It is important to highlight that the GetWell Network (2021) industry aims to alleviate the workload of human workers in the medical field to support their work and professional growth. It should be noted that the GetWell Network (2021) industry is focused on helping ease the burden of human labor in the medical sector to help them work and develop as professionals.

*a) Phising Training Performance in Real World: (*Ho et al.,2025) give a practical view by assessing the training of phishing over eight months in a big company. Although embedded phishing simulations and training modules also decreased the failure rates, overall improvements were also insignificant. Notably, the study has established that the important variable is training engagement: active users of training materials performed better, whereas the users who either did not pay attention to the training materials or rushed through it were left quite vulnerable. (European Union Agency for Cybersecurity, 2023). The authors find that the usual training strategies of common corporations, including annual modules, are inadequate. More meaningful behavior change requires more interesting, adaptive, and frequent methods of training.

b) Phising Training Effectiveness Evidence: The scoping review by Marshall et al. (2024) analyzed 42 empirical studies that devoted their attention to email-phishing training interventions. They have found that there are short-term effects on the capacity of users to detect phishing signals, including suspicious URLs, email domains that do not match, and urgent emails. Active learning based and realistic phishing examples based and instant feedback-based training which are used instead of passive awareness-based training proved to be significantly more effective. Nevertheless, the authors are unsuccessful in identifying long-term effectiveness as several participants lose their skills within several months following the uninspired practice. This underscores the need to undertake phishing training as an on-going process and not a one-time process.

D. Landscape and Technique of Social Engineering

Rathod et al. (2025) thoroughly discuss the vectors of attacks based on social engineering: phishing, baiting, pretexting, vishing, and physical impersonation. The survey reveals ten large types of attacks and the psychological stimuli that are often used in each of them, like fear, curiosity, authority and urgency. They have found that technical defenses are not sufficient to mitigate such attacks since attackers do not go after the vulnerability of the software but mostly the human-made decision-making processes. The authors draw attention to the importance of such proactive security measures as constant training, psychological-awareness trainings, and multi-layered security policy. One of the main lessons is that organizational culture is a big problem: the environments that are characterized by weak security culture or low awareness levels have much higher rates of attack success.

E. Human Factor and Behavioral Issues

Human behavior is also addressed in the interdisciplinary review by Khadka and Ullah (2025), who include the perspectives of psychology, organizational behavior, cybersecurity, and education. Their performance proves that training is not sufficient and that cognitive biases, motivational aspects, and work culture have a great impact on security compliance. They claim that there are habitual decision-making, cognitive overload, trust-based vulnerabilities to the users, which attackers can use. The authors suggest a resilience training, adaptive learning, behavioral-reinforcement, and ethical-use approach to AI interdisciplinary framework. With this view, it is acknowledged that the real-life personalized cybersecurity resilience depends on both technical and psychologically informed end-user care methods.

F. The Practicability of Cybersecurity Training

Therefore, this study examines the key elements of the historic development of Latino women and how these factors influence Latino women's civil rights. Thus, this paper analyzes the main aspects of the historic development of the Latino women and their impact on the civil rights of the Latino women.

The concept of awareness not necessarily leading to secure behavior is also supported by the dissertation on cybersecurity training effectiveness. Although training enhances the theoretical knowledge of the users, the research results in inconsistencies of the behavioral consequences. There are users who use what they have been trained in life and others go back to dangerous habits. Some of the factors that are considered by the dissertation as important in predicting behavior change are training relevance, perceived importance, and reinforcement frequency. Such results reveal the importance of organizations not only in training but also in the establishment of a culture of promotion and normalization of the safe practices.

G. Deep Learning and Technical Detection Method

Using the MDPI Systematic Review of Deep Learning techniques, it can be stated that the well-known advantages of this method encompass: (1) scalability; (2) flexibility; (3) free software; (4) no expertise required; and (5) rapid delivery of results.Relying on the MDPI Systematic Review of Deep Learning techniques, one can say that the most popular benefits of this approach include: (1) scalability; (2) flexibility; (3) free software; (4) no expertise needed; and (5) quick delivery of the results.

Along with the human vulnerability, which social engineering attacks, technical defenses are changing as well. The systematic review on deep learning-based phishing detection points to the developments in the application of models like CNNs, RNNs and LSTMs to detect phishing emails on the basis of text, metadata and email structure. These models can also be quite effective in comparison to blacklist methods or the traditional rule-based methods, particularly against novel or unseen phishing patterns. The review however adds that there are also some pitfalls such as bias in the datasets, unfeasibility to explain and susceptible to the adversarial attack that is aimed at deceiving machine-learning. Therefore, technical solutions are generally highly supportive; they cannot be substituted with human-oriented defenses.

III. Literature GAps Findings

An overview of the consulted literature indicates that there are various common limitations that restrict the existing knowledge on cybersecurity training, human vulnerability, and technical protection against social-engineering assaults. Despite the substantial presence of the focus on the role of user-centric protection in the literature, the cumulative evidence base shows that the necessary methodological gaps, scope, and long-term evaluation are evident. These loopholes demonstrate significant potential research opportunities in the future and explain why the current study is needed..

A. Missing Longitudinal Behavioural Assessment

The majority of the research works assess the user awareness or phishing-detection capabilities right after training. But there is little longitudinal evidence, as the behaviour of a person is studied over months or years. Consequently, it is not clear that the advances continue in the absence of reinforcement. The facts of rapid skill degradation following training are explicitly mentioned in several studies (e.g., Prummer et al., 2023; Marshall et al., 2024; Ho et al., 2025), which explains why continuous and measurable behavioural monitoring is necessary.

B. The Lack of real-world organizational research

Much of the literature uses student samples or laboratory conditions instead of using employees who are working within a realistic organizational setting. This restricts ecological validity and does not reflect issues like pressure in the workplace, time-restraints, exhaustion, and organizational norms-factors that are known to affect user-decision making in actual social-engineering efforts.

C. Minimal Interreaction of the User With Training Interventions

In several instances, training modules are either omitted or hurriedly undertaken or, are perceived as a mandatory exercise as opposed to an education process. Lack of engagement makes the work less effective, and the majority of the work reviewed lacks a system of measuring or enforcing active engagement. This introduces a disjunction between the design of theoretical training and user behavior.

D. Broken Promises of Technical and Human-Centric Defenses

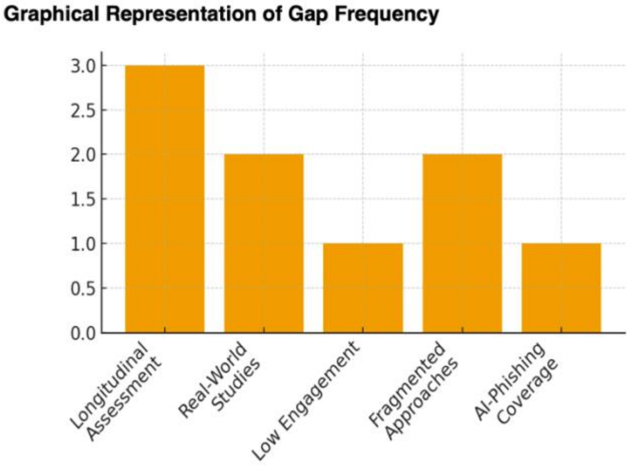
The majority of the researches focus on (a) human-centric (awareness training, psychological factors) or (b) technical (deep-learning detection models) approaches, but not both of them combined in an integrated way. This silo-based approach does not examine the interaction between organizational culture, human behavior, and technical detection systems and the fact that gaps in one area may lead to the lack of others.

E. Slim Representaion of Changing AI-Enchanced Phising Attacks

Although the recent literature has recognized the emergence of AI-generated phishing materials, the existing training models do not typically incorporate highly personalized, adaptive, and AI-based threat situations. This increases the discontinuous gap between the actual attacker capabilities and the training or research experimental scenarios. (Li, Z., & Wang, H.,2024).

Summary of gaps identified in tabular form:

Identified Gaps	Description	Evidence
Absence of longitudinal behavioral evaluation	Short term gains are quantified, although long term behavior is seldom followed up on.	Prümmer et al. (2023); Marshall et al. (2024)
Minimal practical research	High dependency on students and unreal world settings	Prummer et al. (2023); Rathod et al. (2025)
Poor user participation in training	Users forget or skim through the modules, and this diminishes their effectiveness	Ho et al. (2025)
Disjointed human vs. technical treatments	Not many studies are integrating technical detection and human factors	MDPI Review (2024); Khadka and Ullah (2025)
Absence of AI-enacted phishing simulations	Current training does not match sophistication of modern AI-based attacks	Nature Human Behavior (2025); deep-learning review



IV. Methodology

The choice of the methodology of this research is premeditated with the purpose of filling the very critical gaps, which have been detected in the current body of the literature on social-engineering defenses, user behavior, and cybersecurity awareness training. In contrast to the previous research works, which were based on largely short-term measurements, sample of students, or one-domain intervention, the current study is a longitudinal, mixed-method, human-centered study that is based on organizational contexts. The section also identifies the methodological framework, contributions, and strategies that have been established to address the weaknesses found in existing studies.

A. Research Design and Contribution

1) Longitudinal Behavioual Assesment

To address the shortcoming of the previous research which do not conduct any long-term behavioral tracking, this study will utilize a three-phase longitudinal design:

Phase 1: Pre-test of phishing vulnerability and user security practice.

Phase 2: Implementation of multi-format training (interactive, scenario-based, AI-assisted simulations)

Phase 3: 1 month, 3 months and 6 months follow-up assessment.

This model allows the study to include behavioral retention, skill degradation, and training reinforcement requirements that directly fill the gap that is evident in Prummer et al. (2023), Marshall et al. (2024), and Ho et al. (2025).

2) *Real World Organisational Sampling*

Since most studies are based on the students or the laboratory environment, this study applies the subjects that are recruited within an active workplace, which ensures that: time pressure, cognitive load, workflow constraints, and natural organizational norms are automatically factored into the data. (Verizon,2024). This improves the ecological validity and enables the results to be more realistic when it comes to cybersecurity decision-making behaviour

B. Mixed Method Data Collection Strategy

The mixed-methods methodology is followed to deal with the disjointed approach to technical and human factors in earlier literature. This includes:

1) Quantitative Measures
Click-rates of fake phishing emails. Latency of response and accuracy of decision. Interaction logs (engagement, time-spend, skipped modules) Training. Machinery-learning detection performance measures. These measures enable statistical analysis of behavior change and effectiveness of interventions based on human and technical integration.

2) Qualitative Measures
Interviews with participants on motivation, trust, work load and perceived relevance. Cognitive-bias assessments (e.g. authority bias, urgency bias). Organizational culture survey questionnaires. The layer is a qualitative one that solves the problems that Khadka and Ullah (2025) noted about cognitive and cultural factors in cybersecurity practices.

V. PROPOSED FRAMEWORK

A. Framework Overview

To overcome the weaknesses witnessed in the literature, this paper presents a Multi-Layered Human-Centric Security Awareness Framework (MH-SDF) that aims at enhancing security against social-engineering attacks. The framework starts with a longitudinal behavioral assessment stage, during which the phishing vulnerability, decision-making patterns, and cognitive biases of the users are measured across several intervals of time. This will fill the gap in long-term data in the existing literature and create a stable ground on interventions customization. The ideas obtained with the help of this evaluation are used to develop personal learning trajectories, and high-risk and low-engagement users are provided with personalized support depending on their behavioral pattern.

B. Built-In Training and AI-Based Simulation.

As a way of enhancing the efficiency and realism of security awareness programs, the framework uses adaptive training modules, as well as AI-supplied phishing simulations. The learners are presented to interactive and scenario-based learning with micro-learning reinforcement, and immediate feedback as a direct response to the evidence that traditional single training only brings a short-term effect. At the same time, the system sends AI-generated phishing attacks that reflect contemporary, personalized cyber threats, so that trainees can get exposed to the patterns of attacks that are consistent with the capabilities of the adversaries in the real world. Such training insights are subsequently associated with organizational policies and cultural programs, which encourages regular reinforcement and development of a powerful and security conscious work environment. By using this integrated strategy, MH-SDF builds a constant learning cycle, which improves user resilience, minimizes the vulnerability to social-engineering, and changes the behavior towards a sustainable cybersecurity.

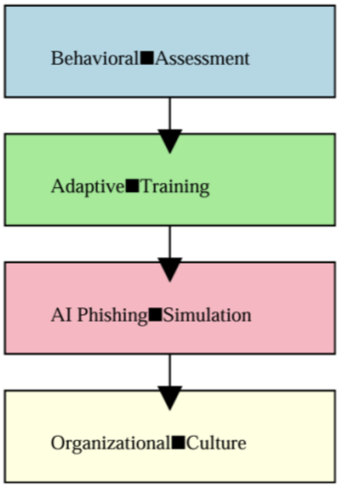


Figure 2Multi Layered Security Awareness Framework

VI. CONCLUSION

. This research paper shows that the training in cybersecurity and technical defenses are crucial when it comes to combating social-engineering attacks, but the existing strategies lack the long-term, adaptive, and realistic mechanisms to deal with the contemporary threats. Limitations are common in the reviewed literature, which includes short-term assessments, lack of user interaction, lack of applicability in the real world, disjointed human-technical strategies, and insufficient coverage of AI-generated phishing. In its turn, the suggested multi-layered framework implies an integrated model that integrates longitudinal behavioral evaluation, individual training, AI-based simulation, and compatibility of organizational culture. Not only does this framework work around the gaps that existed in the earlier research, but it also offers a well-defined roadmap along which organizations could enhance user awareness as well as minimize vulnerability in the long term. Future research can build on this basis by confirming the framework in different industries, incorporating real-time threat intelligence, as well as assessing the effect of new generative AI resources on both defensive and offensive capabilities.

References

[1] (Hoetal.,2025).Understandingtheefficacyofphishingtraininginpractice [Conference paper / journal article]. University / Conference. https://people.cs.uchicago.edu/~grantho/papers/oakland2025_phishing-training.pdf

[2] (Khadkaetal.,2025).Humanfactorsincybersecurity:Aninterdisciplinaryreview. Journal / Publisher. https://link.springer.com/article/10.1007/s10207-025-01032-0

[3] Prümmer,J.,2024).Theeffectivenessofcybersecuritytraining(Master'sthesis/ Dissertation). University of Albany. https://scholarsarchive.library.albany.edu/cgi/viewcontent.cgi?article=1105&contex t=etd

[4] (Marshalletal.,2024).Exploringtheevidenceforemailphishingtraining:Ascoping review. Computers & Security / Journal Name. https://www.sciencedirect.com/science/article/pii/S0167404823006053

[5] (S. Liu,2023) Wi-Fi Energy Detection Testbed (12MTC),, gitHub repository. [Online]. Available: https://github.com/liustone99/Wi-Fi-Energy-Detection-Testbed-12MTC

[6] (Mba, J. F.,2025, July 18). *How to implement social Engineering Awareness Training*. PurpleSec. https://purplesec.us/learn/social-engineering-awareness-training/

[7] (Verizon,2024). 2024 Data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/

[8] (European Union Agency for Cybersecurity, 2023). Phishing: Attack trends and mitigation strategies. https://www.enisa.europa.eu/publications/phishing

[9] (Li, Z., & Wang, H.,2024). AI-driven social engineering attacks: A survey of emerging threats and defenses. IEEE Access, 12, 12245–12262. https://ieeexplore.ieee.org/document/10411210