ISSN 2278-3091

Volume 14, No.3, May - June 2025

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse081432025.pdf

https://doi.org/10.30534/ijatcse/2025/081432025

Assessing the Efficacy of Security Awareness Training in Mitigating Phishing Attacks: A Review

Khulud Alluqmani[1], Abdelrahman Elsharif Karrar[2], Mashael Alhaidari[3], Rawan Alharbi[4], Shahad Alharbi[5]

[1,2,3,4,5] College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia

[1] tu4570538@taibahu.edu.sa, [2] akarrar@taibahu.edu.sa, [3] tu4570396@taibahu.edu.sa, [4]tu4570401@taibahu.edu.sa, [5]tu4570418@taibahu.edu.sa

Received Date: April 25, 2025   Accepted Date: May 29, 2025   Published Date: June 06, 2025

ABSTRACT

Phishing remains one of the most common and advanced forms of cybercrime with serious consequences for individuals, organizations, and national infrastructures. This article offers a comprehensive literature review of recent research (2021–2024) into phishing attack vectors and the impact of security awareness training (SAT) in mitigating such threats. Grounded in empirical studies, simulation-based experiments, personality-based vulnerability analysis, and AI-driven detection models, the research synthesizes evidence from 30+ peer-reviewed articles to assess the effectiveness, limitations, and best practices of awareness interventions. Key findings indicate that simulation-based SAT significantly reduces user susceptibility, particularly when training is adaptive, behavior-aware, and reinforced over time. Studies confirm that demographic variables such as age and gender, as well as personality traits like neuroticism and agreeableness, influence phishing vulnerability and training success. The most prominent topics analyzed include the lifecycle and anatomy of phishing attacks, psychological and behavioral drivers of risk, demographic influences, and the integration of technical and policy-based countermeasures. The research highlights gaps in training design, fatigue-related limitations, and the need for context-sensitive delivery. It concludes by proposing a multi-dimensional solution involving personalized simulation, leadership-driven security culture, and integration with emerging technologies. This paper offers practical insights for cybersecurity practitioners, educators, and policy-makers working to reinforce the human firewall.

Key words: Phishing, Security Awareness Training, Simulation-Based Learning, AI Detection.

1. INTRODUCTION

Phishing remains the most ubiquitous and dynamic cyber threat globally, leveraging the human element to acquire sensitive information such as login details, financial details, or individual identifiers. With the increasing advancement of phishing attacks—such as spear phishing, business email compromise (BEC), and artificially generated impersonation—organizations increasingly find it challenging to defend themselves against them through technical means alone [1],[2]. The Digital Transformation, remote work, and online education explosion, in particular, during the COVID-19 pandemic, has increased phishing attacks and attack surfaces [3],[4]. Current studies point out that phishing is not merely a technical problem anymore but rather a psychological and behavioral problem. The cognitive biases of urgency, authority, and trust are taken advantage of by phishers to turn phishing campaigns more effective [5],[6].

Against all these dangers, Security Awareness Training (SAT) has emerged as a prominent people-oriented anti-phishing protection. SAT training models strive to give users the kind of knowledge and skill sets essential to recognize and react to phish threats properly. The program effects are positively variable and governed by aspects including training design, frequency, population demographics of users, and supportive organizational climate [7],[8]. Research confirms that age, sex, personality traits, and prior work experience significantly influence phishing susceptibility and response patterns [9], [10]. For example, younger individuals have been observed to have higher detection abilities, while agreeableness or neuroticism traits are linked with greater susceptibility [11]. In addition, training through simulations, personalized content presentation, and culture-sensitive modules have been found to be more efficient in raising awareness and reducing click-through rates [12],[13].

Despite widespread application, issues in standardizing the assessment of SAT outcomes, addressing user-side fatigue, and training alignment with evolving phishing trends [14] exist. The pandemic also revealed vulnerabilities in cybersecurity preparedness, with pandemic-themed pandemic phishing campaigns taking advantage of fear, misinformation, and digital unreadiness [4],[15].

This review aims to assess the current efficacy of SAT in mitigating phishing attacks by analyzing recent empirical and theoretical research. It addresses the following research questions:

1. How effective are current SAT programs in reducing phishing susceptibility?

2. What factors enhance or hinder the long-term impact of such training?

3. How can SAT programs adapt to emerging threats and behavioral patterns?

The remainder of this paper is structured as follows: Section 2 reviews the related literature and foundational studies on phishing and awareness training. Section 3 explores the evolution and diversification of phishing attack vectors. Section 4 outlines key concepts and behavioral models underlying SAT programs. Section 5 evaluates the effectiveness of SAT implementations based on recent empirical studies. Section 6 discusses the major challenges and gaps in current training practices. Section 7 proposes best practices and strategic recommendations. Finally, Section 8 concludes the paper and outlines future directions for feature-driven, adaptive awareness training.

2. RELATED WORKS

A substantial body of recent literature explores the complexity of phishing attacks, their psychological underpinnings, and the effectiveness of Security Awareness Training (SAT) as a defense mechanism. Researchers have categorized phishing as a socially engineered cybercrime that exploits human trust and behavioral triggers, often bypassing traditional security defenses [1],[2]. Jain and Gupta [1] presented a comprehensive taxonomy of phishing attacks, including their lifecycle and distribution methods, emphasizing the limitations of current countermeasures. Alkhalil et al. [2] expanded on this by proposing a new anatomy of phishing, covering attack phases, targets, mediums, and vulnerabilities, providing a framework for end-to-end understanding. These foundational studies underscore the dynamic and multifaceted nature of phishing.

Sadiq et al. [3] addressed phishing risks within Industry 4.0, particularly in IoT-integrated environments. They noted that smart systems present an expanded attack surface, requiring robust human-centered and automated responses. Azeez et al. [10] introduced an automated whitelist detection method to improve phishing site identification, achieving a true positive rate of 95%. Similarly, Basit et al. [9] reviewed AI-based detection techniques such as machine learning and deep learning, though they emphasized that technological solutions alone are insufficient. A growing consensus identifies human behavior as the weakest link in cybersecurity [4], [5], [6]. Das et al. [4] found that user susceptibility to phishing is often triggered by urgency, familiarity, and visual cues in email content. Eftimie et al. [5] established that personality traits—specifically agreeableness and neuroticism—increase the likelihood of falling victim to spear-phishing. Daengsi et al. [6] observed significant correlations between phishing awareness and user demographics, notably age and gender.

The importance of contextually tailored SAT is reinforced in recent studies. Okokpujie et al. [4] evaluated phishing simulations among students, revealing a 70.6% vulnerability rate due to lack of awareness. Al-Qahtani and Cresci [7] analyzed 54 COVID-19-era phishing studies, identifying pandemic-induced fear as a dominant phishing vector. Work experience also emerged as a predictor of cyber risk awareness. Pósa and Grossklags [14] found that students with prior work experience demonstrated significantly greater awareness of phishing and cyber hygiene practices. Rizzoni et al. [17] conducted phishing simulation campaigns in a large hospital and found that tailored phishing emails were more likely to deceive employees, emphasizing the importance of message personalization. In a similar vein, Greco et al. [18] proposed an LLM-based adaptive SAT framework that generates personalized content aligned with user profiles.

Cybersecurity awareness for underrepresented groups has also gained attention. Awang et al. [15] explored awareness levels among special needs students, highlighting the moderating role of parental control. Kutschera et al. [26] surveyed incidental data sharing on social media, demonstrating gaps in user privacy awareness that intersect with phishing susceptibility. From a systemic perspective, Hedberg et al. [16] investigated cybersecurity readiness in the automotive repair industry, identifying a lack of integration of cybersecurity into work culture. Similarly, Felgueiras and Pinto [19] assessed DNS and HTTP security in Portuguese universities, revealing wide disparities in adoption of security protocols. Emerging technologies like blockchain have been suggested for phishing mitigation. Khalifa et al. [11] developed a blockchain-based email verification system that enhances authenticity through smart contracts. Furthermore, Yan et al. [24] surveyed abnormal behavior detection in blockchain environments, offering insights for broader awareness frameworks.

Table 1 presents a summary of the related studies that were addressed in this paper.

Table 1: Summary of Related Studies on Phishing and Security Awareness Training

Author(s)	**Focus Area**	**Methodology**	**Key Findings and Context**
A. K. Jain & B. B. Gupta (2022)	Phishing techniques and defenses	Survey and literature review	Analyzed phishing lifecycle, distribution methods, attack techniques, and defences; emphasized need for improved solutions.
Z. Alkhalil et al. (2021)	New phishing anatomy model	Conceptual framework and literature review	Introduced a detailed anatomy of phishing to enhance understanding and guide defence development.
A. Sadiq et al. (2021)	IoT and phishing in Industry 4.0	Review	Identified threats to smart business applications and discussed countermeasures.
Okokpujie et al. (2023)	Student phishing awareness	Field experiments and surveys	70.6% of students susceptible to phishing; need for improved cybersecurity training in academic settings.
S. Eftimie et al. (2022)	Personality traits and spear-phishing	Phishing simulations and psychological testing	Personality traits influence phishing susceptibility; training reduces vulnerability.
T. Daengsi et al. (2022)	Phishing awareness in Thailand	Large-scale phishing simulation	Significant improvement in awareness post-training; gender influenced susceptibility.
Al-Qahtani & Cresci (2022)	Phishing during COVID-19	Survey of 54 studies	Reviewed phishing trends during the pandemic; proposed countermeasures and highlighted future directions.
A. Basit et al. (2021)	AI in phishing detection	Comprehensive survey	Compared ML, DL, and hybrid techniques for phishing detection; discussed challenges and opportunities.
N. A. Azeez et al. (2021)	Whitelist-based phishing detection	Experimental research	Proposed a whitelist technique with 96.17% accuracy, outperforming other methods.
O. Khalifa et al. (2024)	Blockchain for phishing mitigation	Proposed framework	Blockchain email verification improves authenticity and mitigates phishing threats.
Akpachiogu & Williams (2023)	Effectiveness of phishing awareness	Evaluation study	Assessed training effectiveness; emphasized need for ongoing training against social engineering.
Okeke & Amaechi (2024)	Higher education phishing awareness	Literature review and analysis	Reviewed attack types and defenses; advocated for integrated technical and educational strategies.
Pósa & Grossklags(2022)	Work experience & cybersecurity awareness	Survey study	Work experience increases security awareness; recommended tailored security practices.
H. Awang et al. (2024)	Cybersecurity among special needs students	Online survey	Moderate awareness; highlighted importance of parental control and customized training.
D. Hedberg et al. (2024)	Car cybersecurity awareness	Interviews and thematic analysis	Gap in cybersecurity between branded and independent auto workshops; calls for industry collaboration.
F. Rizzoni et al. (2022)	Phishing simulation in hospitals	Phishing simulations	Customized emails had higher engagement; highlighted complexity of ethical simulations.
F. Greco et al. (2024)	LLM-based phishing education design	Proposed method	Suggested LLMs to customize training content and improve awareness efficacy.
Felgueiras & Pinto (2022)	Web security in Portuguese HEIs	Security audits using scripts	Assessed DNS/HTTP security implementation; found low adoption of advanced security protocols.
Teichmann et al. (2023)	Geopolitical impact on ransomware	Desk research	Analyzed ransomware evolution during geopolitical conflicts; connected to cybersecurity policies.
Papathanasiou et al. (2023)	BEC threats in Greece	Review of regulatory frameworks	Reviewed BEC attack techniques; highlighted national policies for cybersecurity.
Naqvi & Smolander (2024)	Usable security challenges	Workshop and practitioner interviews	Highlighted disconnect between research and practice in aligning usability with security.
M. Canham et al. (2021)	Employee phishing behavior clusters	Longitudinal phishing campaign analysis	Identified repeat clickers/reporters and categorized employees into phishing response profiles.
Kutschera et al. (2024)	Incidental data on social media	Student survey	Found a significant portion of students unknowingly post privacy-compromising data; recommended awareness training.

3. NATURE AND EVOLUTION OF PHISHING ATTACKS

Phishing attacks have evolved into a sophisticated, multi-layered cyber threat that exploits both technological vulnerabilities and human psychology. What began as simple mass-email fraud has morphed into a complex arsenal of targeted, AI-driven campaigns involving spear phishing, business email compromise (BEC), Vishing, Smishing, and even Quishing [1],[2]. Jain and Gupta [1] traced the development of phishing techniques, highlighting a progression from static attacks to dynamic, context-aware deceptions. Alkhalil et al. [2] expanded this view by proposing a new anatomy of phishing, which categorizes attack phases, mediums, and types of perpetrators. This evolution reflects the increasing adaptability of attackers, who employ machine learning and behavioral profiling to evade detection and manipulate users. The COVID-19 pandemic accelerated phishing trends significantly. Al-Qahtani and Cresci [7] coined the term “scamdemic” to describe the parallel rise of phishing attacks during global lockdowns. Their review of 54 studies revealed that most pandemic-era attacks relied on fear and urgency, exploiting crisis-related themes to elicit impulsive user responses. Similarly, Friel [8] emphasized the use of psychological manipulation, including authority bias, fear appeals, and urgency tactics, to increase the effectiveness of phishing emails.

In the modern digital ecosystem, phishing threats are no longer limited to emails. Sadiq et al. [3] noted a sharp increase in phishing vectors targeting IoT devices and smart business applications. These environments are particularly vulnerable due to increased attack surfaces and lack of user training. Azeez et al. [10] addressed this by proposing an automated whitelist-based solution to improve phishing detection across platforms, particularly where rapid identification of spoofed URLs is essential. New forms of attack—like BEC and AI-driven impersonation—have also emerged. Papathanasiou et al. [21] examined the rise of BEC, showing how attackers now exploit social engineering in combination with malware to bypass technical safeguards and compromise enterprise systems. Teichmann et al. [20] further linked cybercrime trends to geopolitical conflicts, particularly highlighting how ransomware and phishing converge in times of international instability.

The human element remains a central focus. Studies by Das et al. [4] and Eftimie et al. [5] confirmed that email structure, sender familiarity, and user personality traits significantly affect phishing response. Daengsi et al. [6] found that demographic factors—such as age and gender—also play a role in awareness and susceptibility. Work experience has been shown to enhance awareness: Pósa and Grossklags [14] found that students with job experience exhibit greater cybersecurity risk awareness, especially in remote environments.

Phishing has also invaded non-traditional domains. Hedberg et al. [16] identified a cybersecurity readiness gap in modern auto workshops, where vehicle systems can now be compromised via phishing tactics targeting diagnostic tools. Similarly, Rizzoni et al. [17] demonstrated in a large hospital setting that customized phishing simulations were more successful at tricking staff than generic ones—an insight that underscores the importance of personalization in phishing evolution. Recent advances in technology have facilitated adaptive phishing. Basit et al. [9] and Yan et al. [24] surveyed AI-enhanced phishing techniques and anomaly detection using blockchain, respectively. These technologies underscore how attackers now have the ability to emulate authentic communication with the precision of almost perfection, forcing more advanced and adaptive countermeasures.

4. CONCEPTS AND MODELS OF SECURITY AWARENESS TRAINING

Security Awareness Training (SAT) is among the most effective non-technical countermeasures to phishing attacks, engineered to increase user resistance through response, cognition, and behavior to social engineering attacks. As with greater adaptability and psychological manipulation involved in phishing, SAT also needs to be a dynamic, behavior science-based, context-aware system for integration [1],[4],[5]. Most SAT models draw on theories of behavior change such as Protection Motivation Theory (PMT), which asserts that users will be more inclined to adopt safer behavior when threatened as being preventable and severe [4]. Friel [8] identified how the phishing attacks ride on psychological impulses like fear, urgency, deference to authority, and curiosity, and so SAT programs should teach users protection against emotional trickery and thinking biases. The latter include confirmation bias, bias towards authority, and over-confidence—factors that increase risk despite technical proficiency.

SAT programs are typically either static or dynamic in nature. Static education—presentations, posters, and reading material—creates general awareness but is low on recall and interactivity. Dynamic frameworks, in contrast, employ gamification, simulation, and adaptive delivery of content to foster engagement and real-world usability [12], [13]. Akpachiogu and Williams [12], for example, demonstrated that interactive phishing simulations significantly enhanced user detection of malicious cues compared to traditional lectures. Latest trends are in the direction of adaptive learning. Greco et al. [18] suggested an LLM-based system that has the capability to tailor phishing training based on individual behavioral profiles and learning feedback. The model utilizes AI for the detection of user weaknesses and generating tailored content, which enhances the efficiency of learning as well as relevance. Similarly, Daengsi et al. [6] and Eftimie et al. [5] also pointed out that personality, gender, and age influence awareness of phishing and that these ought to guide the design of training modules.

Social engineering underlies phishing. Ferreira et al. [8] and Meta Compliance [16] explained how the phishing emails tend to impersonate authority figures or regular patterns of communication to psychologically manipulate users emotionally. SAT training courses that define and replicate such psychological strategies—e.g., urgency markers or appeals to emotion—can generate more precise detection. Social context is another essential one. Al-Qahtani and Cresci [7] illustrated how phishing evolved during the COVID-19 pandemic by utilizing emotionally charged material and mimicking health organizations to take advantage of user fear. Training programs thus need to address up-to-date socio-technical trends in order to remain effective. Medlin and Shaw [15] also found that cultural variables affect training impacts significantly. Respect for authority hierarchy in some locales may leave users vulnerable to impersonation attacks, while cynicism elsewhere can cut exposure. SAT content must be localized and culture-aware to maximize impact. Even organizational culture enters the picture: Alruwaili [16] found that training can only be successful after leadership endorsement and incorporation into normal workflows. Game learning and prompt response are becoming more central in the development of SAT. Das et al. [4] and Rizzoni et al. [17] found that quick, situation-dependent feedback after simulation helped reinforce good behavior and limit potential faults. Incorporating leaderboards, tests, and role-playing tasks will also assist engagement as well as long-term memorization.

5. EFFECTIVENESS OF TRAINING PROGRAMS

Security Awareness Training (SAT) programs have been a central step to mitigate phishing attacks. However, the efficacy of such efforts is dependent upon several variables, including user engagement, content development, organizational infusion, and new threat responsiveness [1], [4], [12]. Experimental findings and latest advancements in the evaluation of SAT effectiveness in both organizational and educational contexts are analyzed in this section.

Simulation training has been shown to be more effective in phishing detection. Akpachiogu and Williams [12] demonstrated that the users who were trained through role-specific phishing simulation had significantly lower click-through rates compared to the users who received generic training. Similarly, Rizzoni et al. [17] conducted a large-scale real-world phishing simulation in an Italian hospital and found that phishing emails personalized to the individual were more effective in deceiving users compared to generic phishing emails, reflecting the necessity of personalized simulation scenarios. Okokpujie et al. [4] conducted a two-phase experiment in a Nigerian university and reported that 70.6% of the students were susceptible to phishing emails prior to training. However, awareness actually gained momentum after simulated exposure and post-exposure contemplation. The study highlights the role of concrete simulation with feedback in solidifying security behavior among students.

The use of immediate, targeted feedback improves SAT performance. Das et al. [4] suggested that phishing exercise feedback helps users recognize misleading indicators they had missed, thereby improving cognitive protection. Eftimie et al. [5] also added that subjects given feedback matching their personality profiles were less vulnerable to spear-phishing attacks during repeated testing, confirming the significance of behavioral compliance in feedback channels. It is also worth noting the repetition. Alruwaili [16] highlighted that SAT should not be considered as one intervention. Continuous reinforcement through longitudinal training improves retention of memory and avoids complacency. This was further evidenced by findings from Daengsi et al. [6], where employees under phased SAT interventions showed a 71.5% improvement in detecting email phishing.

Personalization enhances the effectiveness of SAT. Daengsi et al. [6] confirmed that age and gender played a major role in levels of awareness, where female personnel exhibited greater phishing recognition rates than males. Greco et al. [18] suggested a framework involving Large Language Models (LLMs) to design adaptive training paths based on user profiles and behavioral history. This customization can address variation in learning style of users, leading to longer-lasting results. Furthermore, Friel [8] observed that users' cognitive biases, which include overconfidence and authority bias, can undermine SAT effectiveness unless specifically addressed. Therefore, effective programs must do more than provide content and make a concerted effort to restructure cognitive patterns.

Organizational culture impacts the effectiveness of training. Alruwaili [16] and Medlin and Shaw [15] stated that SAT programs embedded into the security culture in a firm and supported by leadership are optimal. Leadership buy-in improves user morale and indicates the importance of cybersecurity at every level. The cultural adaptation was also highly significant in the COVID-19 pandemic. Al-Qahtani and Cresci [7] investigated 54 studies and found that pandemic-related thematic phishing emails were particularly effective at capitalizing on the fears of the users. SAT programs which responded to the situational factors experienced higher learning performance and engagement.

Despite demonstrating encouraging outcomes, SAT programs also remain to present measurement problems. Aleroud and Zhou [18] criticized the reliance on crude indicators such as click-through rates or quiz scores. They may not even capture behavioral change or risk avoidance over time adequately. To counteract this, Greco et al. [18] proposed that SAT systems be complemented with real-time analysis and feedback loops to measure participation and adapt intervention accordingly. Furthermore, training fatigue continues to exist. Friel [8] and Hedberg et al. [16] described that if content is duplicative or seen as irrelevant, then users might lose interest and the effectiveness of the program is lost. The inclusion of gamification, real-world applications, and periodic updates helps to retain interest and effectiveness.

6. CHALLENGES AND IMPLEMENTATION GAPS

Despite widespread usage, Security Awareness Training (SAT) initiatives are beset with a number of challenges that make them ineffective in combating phishing attacks. These challenges vary from measurement limitations, user participation, context disparity, and the escalating complexity of phishing attacks.

One of the largest challenges to effective SAT implementation is a lack of standard measurement tools for assessing training impact. Aleroud and Zhou [18] commented that organizations too often rely on superficial measures such as click-through and quiz results that do not reflect deeper behavioral or cognitive shifts. Without robust measures, it is difficult to measure long-term effectiveness or drive lasting change. Greco et al. [18] suggested employing AI-driven analytics and large language models (LLMs) to measure user engagement dynamically and adjust training materials accordingly. Yet, integration of such technology into current training systems remains in its early stages due to the constraints of resources and available technical expertise.

Training fatigue is another critical issue. If SAT content is redundant, too basic, or irrelevant to users' daily behavior, users' engagement level falls significantly [16]. Friel [8] pointed out that users become resistant to phishing simulations if they are overly predictable or not immediately relevant. Such immunity reduces the effectiveness of the program and can even lead to a false sense of security. Further, cultural and psychological factors control users' responses to training. Cognitive biases such as authority bias and overconfidence lead the users to underestimate their own susceptibility to phishing even after they have gone through awareness training [22].

Generic, one-size-fits-all training modules do not suffice to cater to the diverse needs of users. Daengsi et al. [6] found extreme variations in phishing susceptibility across gender and age groups, necessitating the creation of specially created training modules. Eftimie et al. [5] noted that personality traits—agreeableness and neuroticism—also influence phishing susceptibility, which reflects the need for SAT programs to incorporate psychological profiling. Special populations are also harder. For instance, Awang et al. [15] showed that special needs students have moderate awareness of cybersecurity and require parental as well as educative support in order to facilitate learning. Pósa and Grossklags [14] also discovered that university students with work experience had much better awareness than those with no work experience, emphasizing the importance of context-aware training.

Organizational buy-in is often lacking. Alruwaili [16] noted that when senior management fails to support or participate in training initiatives, employees are less likely to engage seriously. Moreover, training programs often exist in silos and are not integrated with broader cybersecurity policies or incident response frameworks. The study by Hedberg et al. [16] illustrated this issue in the automotive industry, where cybersecurity was not embedded in the work culture of many auto workshops. A similar disconnect between training and real-world application is found in healthcare, where Rizzoni et al. [17] reported organizational resistance to phishing simulations due to ethical concerns and logistical challenges.

SAT programs often struggle to keep pace with the dynamic nature of phishing attacks. Al-Qahtani and Cresci [7] observed that the COVID-19 pandemic led to a dramatic increase in phishing attacks exploiting health-related fears, yet many SAT programs were slow to adapt their content. The growing use of AI, deepfake technologies, and novel attack vectors like business email compromise (BEC) and QR-code phishing ("quishing") necessitates continuous content updates, which many organizations fail to provide [1], [3]. Emerging threats in blockchain environments and smart infrastructure also require advanced awareness strategies. Studies by Yan et al. [24] and Khalifa et al. [11] stressed the need to include new platforms and decentralized systems in SAT content as phishing expands into these domains.

7. BEST PRACTICES AND RECOMMENDATIONS

Effective implementation of Security Awareness Training (SAT) programs is essential for building human defenses against phishing attacks. To optimize impact, organizations must adopt evidence-based best practices that address behavioral, contextual, and technological dimensions of phishing resilience.

Simulation training remains to be one of the most effective methods of phishing learning. As Akpachiogu and Williams [12] have demonstrated, phish tests through simulated phishing emails—especially tailored according to user types—exhibit great recognition improvements with the decline in click rates. The same was affirmed by Rizzoni et al. [17], with results of increased user activities through adapted phishing emails within the hospital context compared to generic emails, indicating the necessity of context realism in simulations. Greco et al. [18] recommended using large language models (LLMs) in order to dynamically adjust training material to the user's own individual profile, optimizing relevance and level of engagement of training. It allows for adaptation in real time to the performance of learners, offering a tailored experience that constantly evolves with every session. The incorporation of psychological and demographic profiling in training design is increasingly being accepted as a necessity. Eftimie et al. [5] demonstrated that personality traits, including neuroticism and agreeableness, influence vulnerability to phishing. Likewise, Daengsi et al. [6] mentioned the influence of age and gender in training effectiveness and advocated gender-sensitive and age-appropriate strategies. Parental involvement and personalized interventions, as suggested by Awang et al. [15], also need to be taken into consideration in awareness programs for special populations, like special needs students. Behavioral models such as those by Canham et al. [23] can be used to segment users into "repeat clickers," "protective stewards," or "spectators" to which training strategies for each group can be tailored.

Leadership support is crucial for fostering a security-conscious culture. Alruwaili [16] and Medlin and Shaw [15] both emphasized that training initiatives gain more traction when visibly endorsed and practiced by organizational leaders. Executives who undergo the same training as employees help demonstrate the importance of cybersecurity and model expected behaviors. Friel [8] also noted that visible security policies and consistent messaging from leadership foster trust and engagement, helping users internalize the importance of security practices in their daily roles. Repetition strengthens retention. Okokpujie et al. [4] and Daengsi et al. [6] found that repeated phishing simulations significantly reduce user error over time. Monthly microlearning sessions, periodic quizzes, and scenario-based refreshers help counter knowledge fading and keep users alert to evolving tactics. SAT programs should also incorporate real-life examples and consequences of phishing, particularly those relevant to the organization's sector. For example, referencing local BEC scams—as reviewed by Papathanasiou et al. [21]—can increase emotional engagement and perceived risk.

Training content must be continuously updated to cover the latest threat vectors. Jain and Gupta [1] and Alkhalil et al. [2] emphasized the importance of educating users about new phishing forms, including spear phishing, vishing, smishing, and AI-generated messages. Al-Qahtani and Cresci [7] illustrated how pandemic-specific phishing surged during COVID-19, while Khalifa et al. [11] and Yan et al. [24] advocated for integrating blockchain and smart contract security into awareness programs. As phishing attackers increasingly use sophisticated deception and automation tools, organizations must also train users on how these attacks differ from traditional methods. This includes understanding emotional triggers (e.g., urgency and authority bias), as outlined by Friel [8], and social media-related risks, such as incidental data leaks analyzed by Kutschera et al.[26] .

SAT programs should not function in isolation. They must be integrated with technical defenses such as DNS/HTTP safeguards [35], email authentication protocols, and anomaly-based detection tools. Azeez et al. [10] and Bhardwaj et al. [11] presented technical solutions that can complement user training by reinforcing behavioral defenses with automated intervention layers. Yan et al. [24] and Putrenko and Pashynska [25] also stressed the situational awareness—both civilian and military—role as an adjunct to technical countermeasures, especially in conflict-situational or high-risk environments.

8. CONCLUSION AND FUTURE WORK

Phishing continues to be an active and pervasive threat, leveraging technical vulnerabilities and psychological biases alike. As this review has suggested, Security Awareness Training (SAT) is a crucial measure in restraining phishing susceptibility, but one that heavily depends on adaptive, user-centered design, leadership inclusion, contextual realism, and frequent revision. Recent research attests that phishing attacks are becoming more sophisticated through the use of AI, emotional manipulation, and cross-platform delivery channels [1], [2], [21]. These trends underpin the limitations of static training programs and the necessity for dynamic, personalized, and simulation-based learning experiences [12], [19], [24]. SAT programs must also consider different user groups and psychological profiles as these have an important impact on training effectiveness [5],[6],[23]. Substantive challenges remain despite this progress. Institutions struggle to quantify training outcomes in more than superficial ways like click-through rates [18], and some are confronted with resistance due to training exhaustion or cultural incompatibility [15], [22]. There is evidence that there are knowledge deficits among training vulnerable populations like students, special needs users, and front-line healthcare workers [13], [19], [23]. SAT technologies are also rarely integrated with real-time threat information or technical defense, so resulting security strategy remains disjointed [10].

Future research should focus on the integration of SAT platforms with real-time behavioral analytics and adaptive AI models. Moreover, cross-sectoral comparative studies and longitudinal analyses are needed to assess retention and behavior change over time. Development of universal SAT metrics and feature-rich dashboards that align with evolving phishing trends will also enhance program scalability and effectiveness.

REFERENCES

[1]. A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," Enterprise Information Systems, vol. 16, no. 4, pp. 527–565, 2022.

[2]. Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," Frontiers in Computer Science, vol. 3, p. 563060, 2021.

[3]. A. Sadiq et al., "A review of phishing attacks and countermeasures for Internet of Things-based smart business applications in Industry 4.0," Human Behavior and Emerging Technologies, vol. 3, no. 5, pp. 854–864, 2021.

[4]. K. Okokpujie, G. C. Kennedy, K. Nnodu, and E. Noma-Osaghae, "Cybersecurity awareness: Investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment," Int. J. Sustain. Dev. Plan., vol. 18, no. 1, pp. 255–263, 2023.

[5]. S. Eftimie, R. Moinescu, and C. Răcuciu, "Spear-phishing susceptibility stemming from personality traits," IEEE Access, vol. 10, pp. 73548–73561, 2022.

[6]. T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks," Education and Information Technologies, vol. 27, no. 4, pp. 4729–4752, 2022.

[7]. A. F. Al-Qahtani and S. Cresci, "The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures," IET Information Security, vol. 16, no. 5, pp. 324–345, Jul. 2022.

[8]. D. Friel, "Unraveling the psychology behind phishing scams," MetaCompliance Cyber Security Awareness Blog, Oct. 13, 2023. [Online]. Available: https://www.metacompliance.com/blog/cyber-security-awareness/unraveling-the-psychology-behind-phishing-scams

[9]. A. Basit et al., "A comprehensive survey of AI-enabled phishing attacks detection techniques," Telecommunication Systems, vol. 76, no. 1, pp. 139–154, 2021.

[10].N. A. Azeez, S. Misra, I. A. Margaret, and L. Fernandez-Sanz, "Adopting automated whitelist approach for detecting phishing attacks," Computers & Security, vol. 108, p. 102328, 2021.

[11]. O. Khalifa, T. Effendy, M. Z. Ahmed, E. El-Khazmi, and A. Esgiar, "Blockchain based email security to mitigate phishing attack," Asian Journal of Electrical and Electronic Engineering, vol. 4, pp. 77–86, Dec. 2024.

[12].C. D. Akpachiogu and A. B. Williams, “Evaluating the effectiveness of phishing awareness training in mitigating social engineering attacks,” 2023.

[13]O. C. Okeke and C. E. Amaechi, “Awareness of phishing attacks in institutions of higher learning: A review of types and technical approaches,” Int. J. Res. Innov. Appl. Sci., vol. 9, no. 10, pp. 309–333, 2024.

[14]T. Pósa and J. Grossklags, “Work experience as a factor in cyber-security risk awareness: A survey study with university students,” Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 490–515, Jun. 2022.

[15]H. Awang et al., “Cybersecurity awareness among special needs students: The role of parental control,” Mesopotamian Journal of CyberSecurity, vol. 4, no. 2, pp. 63–73, Jun. 2024.

[16]D. Hedberg, M. Lundgren, and M. Nohlberg, “Cybersecurity in modern cars: Awareness and readiness of auto workshops,” Information and Computer Security, vol. 32, no. 4, pp. 407–419, Sep. 2024.

[17]F. Rizzoni et al., “Phishing simulation exercise in a large hospital: A case study,” Digital Health, vol. 8, pp. 1–13, Mar. 2022.

[18]F. Greco, G. Desolda, and L. Vigano, Supporting the Design of Phishing Education, Training and Awareness Interventions: An LLM-Based Approach, Springer, 2024.

[19]N. Felgueiras and P. Pinto, “An overview of the status of DNS and HTTP security services in higher education institutions in Portugal,” Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 442, pp. 457–469, 2022.

[20]F. Teichmann, S. Boticiu, and B. Sergi, “The evolution of ransomware attacks in light of recent cyber threats,” International Cybersecurity Law Review, vol. 4, pp. 1–22, Jul. 2023.

[21]A. Papathanasiou, G. Liontos, V. Liagkou, and E. Glavas, “Business email compromise attacks: Threats, vulnerabilities and countermeasures—A perspective on the Greek landscape,” Journal of Cybersecurity and Privacy, vol. 3, pp. 610–637, 2023.

[22]B. Naqvi and K. Smolander, “Practitioners’ perspectives on and prospects for usable security,” IEEE Computer, vol. 57, no. 10, pp. 66–74, Oct. 2024.

[23]M. Canham et al., “Phishing for long tails: Examining organizational repeat clickers and protective stewards,” SAGE Open, vol. 11, no. 1, Jan. 2021.

[24]C. Yan, C. Zhang, Z. Lu, Z. Wang, Y. Liu, and B. Liu, “Blockchain abnormal behavior awareness methods: a survey,” Cybersecurity, vol. 5, no. 1, Mar. 2022.

[25]V. Putrenko and N. Pashynska, “Military situation awareness: Ukrainian experience,” Applied Cybersecurity & Internet Governance, Jul. 2024.

[26] S. Kutschera et al., “Incidental data: A survey towards awareness on privacy-compromising data incidentally shared on social media,” Journal of Cybersecurity and Privacy, vol. 4, no. 1, pp. 105–125, Feb. 2024.