An In-Depth Study of Phishing Attacks and User Awareness in Modern Web Applications

Hensei Patel[1], Ankita Kothari[2]

[1]KPGU University, Krishna School of Technology,
Vernama, Vadodara, Gujarat, India
hensei13122000[at]gmail.com

[2]KPGU University, Krishna School of Emerging Technology & Applied Research,
Vernama, Vadodara, Gujarat, India
ankitakothari.cse.kset[at]kpgu.ac.in

Abstract: ***Phishing attacks have evolved into one of the most prevalent threats affecting modern web applications, exploiting both technological weaknesses and human decision-making. This review provides an in-depth examination of contemporary phishing techniques, the expanding attack surface within web-based systems, and the behavioural factors contributing to user vulnerability. It synthesizes recent research on detection approaches, including machine learning, deep learning, multimodal analysis, and browser-integrated defensive mechanisms, while also analysing empirical studies on user awareness, decision processes, and susceptibility. The review highlights how emerging vectors such as mobile-first phishing, QR code phishing, OAuth consent manipulation, and artificially generated phishing content challenge traditional defences. Furthermore, it identifies critical weaknesses in current solutions, including limited real-time detection, reliance on outdated datasets, and inadequate integration between automated detection and user education. The study concludes by outlining the need for comprehensive, user-centric, and application-aware strategies that combine technical defences with behavioural insights to enhance resilience against phishing within modern web application.***

Keywords: Phishing attacks, cybersecurity, machine learning, user awareness, web applications

1.Introduction

The dramatic expansion of the internet, cloud platforms, and digital services has made cybersecurity one of the most important domains in modern information systems. As organizations migrate toward highly distributed architectures and web-based service ecosystems, the threats have expanded, allowing adversaries to exploit human and technological vulnerabilities in far more sophisticated ways. Recent studies indicate that social engineering threats now account for more than 80% of first intrusion vectors, with phishing consistently ranking as the most prevalent and damaging category of global cyberattacks [1], [4]. Digital communication-encompassing email, messaging applications, social platforms, and browser-based services-has gradually evolved into environments where trust is easily compromised, allowing attackers to deceive users at scale. In this context, phishing has already emerged not only as a technical problem but also as a significant socio-behavioural challenge affecting individuals, enterprises, and critical infrastructures worldwide.

Phishing, in general, is a phishing technique where the attackers masquerade as trustworthy entities to elicit confidential information such as credentials, financial information, or personal identifiers from unsuspecting users [2], [7]. Today's well-known phishing vectors include email-based phishing, spear-phishing, clone phishing, smishing, business email compromise, and webpage-based credential harvesting attacks. Studies conducted in 2023–2025 indicate that the current phishing attacks use AI-generated content, real-time impersonation of websites, and adaptive manipulation methods to evade traditional detection systems [5], [11], [16]. The impact, therefore, has been devastating globally because of the billions of dollars that phishing attacks have caused in financial losses, massive data breaches, and identity theft incidents that led to ransomware infections on individuals and enterprises alike [8], [13]. As the attackers continue perfecting their craft with generative AI and automation, the efficiency, personalization, and believability of these phishing attempts have increased significantly, thus weakening the effectiveness of static security controls and reactionist defence mechanisms.

Modern web applications have increased the scope and severity of phishing attacks due to their dynamic, interactive and authentication-driven architectures. The shift toward single-page applications, OAuth-based logins, cross-platform access, and API-centric designs introduces new attack vectors that enable session hijacking, token theft, and client-side deception [6], [14]. Studies show that phishing kits increasingly mimic legitimate web interfaces using real-time DOM manipulation, advanced obfuscation, and script-based credential exfiltration techniques that are difficult for users to detect [9], [17], [22]. Furthermore, the rise of cloud-based services and federated identity systems has made impersonation more scalable, allowing attackers to deploy phishing sites within minutes using vendor-approved infrastructure [18], [25]. These technological advances combined with low user awareness have resulted in a dangerous landscape where phishing attacks are evolving in complexity and effectiveness [3], [10], [21].

User awareness plays a crucial role in reducing phishing risk, but empirical research consistently shows that users remain highly vulnerable to deception despite increased training efforts [12], [15], [19]. Behavioural studies show that cognitive biases, interface familiarity, visual persuasion, and trust inferences strongly influence decision-making in online environments, making users vulnerable to well-designed phishing pages that closely mimic legitimate applications [20], [26]. Furthermore, research conducted between 2023 and 2025 shows that traditional awareness programs-such as periodic training and static alerts-are insufficient to address sophisticated phishing tactics that exploit real-time emotional triggers and context-dependent decision-making patterns [23], [29]. As a result, improving user awareness in the modern web application ecosystem requires a more adaptive and user-centred approach that integrates behaviour modelling, continuous feedback, and intelligent detection systems [24], [30]. Understanding the interplay between evolving phishing techniques and user behaviour is critical to developing a more robust security framework in the modern online environment.

Despite significant advances in cybersecurity technologies, the modern online ecosystem remains highly vulnerable to increasingly sophisticated phishing attacks. The shift toward dynamic, client-centric architectures-such as single page applications (SPAs), progressive web applications (PWAs), and real-time DOM-driven interfaces-has created complex environments where users interact with rapidly changing content and visually similar page elements. These dynamic interfaces reduce the ability to verify user authenticity and allow adversaries to design phishing pages that adapt content in real-time to mimic legitimate web applications [1], [4]. As a result, it becomes increasingly difficult to distinguish between genuine interactions and deceptive interactions, even for trained users.

Furthermore, modern browser-based authentication mechanisms introduce new attack surfaces that traditional phishing protection does not adequately address. Technologies such as token-based authentication, session delegation, and passwordless login flows rely heavily on client-side security. OAuth 2.0 and OpenID Connect, which support sign-in systems on thousands of platforms, are particularly vulnerable to authorization code interception, consent phishing, and token misdirection attacks when deployed without strict verification controls [3], [7]. Research shows that phishing kits now replicate OAuth consent screens, browser-based login widgets, and federated identity flows with high accuracy, bypassing signature-based and URL-filtering protections [6], [8]. This reflects a fundamental mismatch between evolving web authentication models and outdated anti-phishing mechanisms.

The security landscape has become even more complex with the rise of API-driven architectures. Modern web applications rely on REST and GraphQL APIs for data retrieval, user state synchronization, and third-party service integration. Attackers exploit these API interactions through session hijacking, CSRF-based credential forwarding, and malicious API endpoint impersonation, techniques that traditional email and domain reputation systems cannot detect [5], [9]. Because APIs operate behind authentication layers and often lack visible user-facing indicators, phishing attacks targeting API tokens remain invisible to users and security filters.

The social development behind these technical vulnerabilities remains a serious challenge. Recent studies from 2023–2025 show that adversaries increasingly rely on psychological manipulation to exploit cognitive biases in digital environments-such as authorization signals, urgency determinations, and context-specific triggers [2], [10]. Mobile-first usage patterns worsen this problem: mobile interfaces provide limited visual space, hide full URLs, and limit access to browser security indicators. As more users access financial and business applications on smartphones, the reduced ability to verify authenticity dramatically increases susceptibility to phishing [11], [12].

Traditional phishing defenses-including blacklists, static rule-based detectors, and periodic awareness training-are insufficient to meet these new challenges. Blacklists fail to detect short-lived phishing domains created and distributed within minutes; Signature-based detectors cannot identify AI-generated phishing content that lacks previously known patterns; And traditional awareness programs do not prepare users for dynamic, context-specific attacks delivered through modern interfaces [13], [14]. Additionally, businesses continue to rely on training materials that do not reflect the latest attack vectors related to OAuth flows, browser extensions, or mobile phishing sites. This misalignment leaves a significant gap between real phishing techniques and current defensive strategies.

These interconnected technical and behavioral issues highlight an important research problem: existing phishing mitigation frameworks are not designed for dynamic web architectures, modern authentication systems, API-driven ecosystems, or mobile-first user behavior. Addressing this gap requires a comprehensive study that integrates insights from phishing evolution, human factors, web application security, and adaptive user awareness strategies. This review therefore tries to synthesize contemporary research to find challenges, evaluate existing countermeasures, and highlight directions for more effective phishing resilience in the modern online environment.

Although phishing has been widely studied, significant gaps stay in the understanding of how attacks work within the modern online ecosystem. Existing research focuses primarily on static phishing websites and e-mail frauds and offers limited insight into attacks targeting dynamic web interfaces such as SPAs and DOM-manipulated content used by modern applications [1], [4]. Similarly, phishing strategies that leverage OAuth, OpenID Connect, and API-based authentication workflows are rarely detected, even when attackers spoof consent screens, steal tokens, and impersonate API endpoints to bypass traditional security controls [2], [5], [9]. Another major gap exists in mobile-first phishing studies: most awareness and usability studies rely on desktop environments, ignoring the low visibility, hidden URL bars, and gesture-based navigation that significantly increase user sensitivity on smartphones [7], [10].

The behavioral aspects of phishing also require closer scrutiny. The current literature provides limited understanding of how modern interface design-micro-animations, interactive components, visual familiarity, and layout dynamics-shapes user decisions when interacting with confusing elements [6], [10]. Furthermore, existing protections are still outdated: blacklists, signature-based scanners, and static machine learning models cannot keep up with AI-generated phishing content, rapid domain rotation, and cloud-hosted phishing kits evolving in real-time [3], [5], [8]. Finally, this area lacks a unified framework that integrates technical vulnerabilities, authentication flows, API behavior, and human factors. Research is still fragmented across different domains, resulting in an incomplete picture of how phishing attacks work in complex, modern online environments [1], [11]. Traditional awareness programs also fail due to their reliance on static training methods rather than an adaptive, behavior-driven approach that aligns with modern user patterns and cognitive models [8], [12]. These gaps highlight the need for a comprehensive review that synthesizes new evidence and addresses phishing challenges specific to dynamic, authentication-intensive, and mobile-centric web applications.

The purpose of this review is to systematically examine how phishing attacks have evolved within the modern web application ecosystem and to identify the most important technical and behavioral factors that influence user vulnerability in these environments. This study aims to synthesize recent findings on dynamic web interfaces, SPA architectures, OAuth and API-based authentication mechanisms, and mobile-first user interactions to provide an integrated understanding of modern phishing threats [1], [3], [6]. It attempts to evaluate the limitations of existing anti-phishing protections-such as blacklists, static machine learning models, and traditional awareness programs-which have shown declining effectiveness against AI-generated phishing content, rapid domain rotation, and cloud-hosted phishing kits [4], [7]. By integrating insights from security engineering and human-centered cybersecurity research, the review aims to highlight unsolved challenges and outline future research directions that can support adaptive, user-centered, and technically aligned phishing mitigation strategies for modern web applications [2], [5], [8].

2.Taxonomy of Phishing Attacks

Phishing has evolved from simple email scams into diverse, multi-channel attacks that target both system weaknesses and human behavior. Today's phishing campaigns use AI-generated content, dynamic webpages, mobile-first deception, and cloud-hosted infrastructures to bypass traditional defenses [1], [5], [16]. Understanding this broader taxonomy is crucial to recognizing how attackers exploit user trust and modern web application environments.

A. Email-Based Phishing

Email remains the most prevalent phishing vector due to its universality, low cost, and ability to impersonate organizational communication channels. Classic email phishing involves sending deceptive messages that mimic legitimate brands, financial institutions, or service providers to lure users into clicking malicious links or divulging sensitive information [2], [7]. Recent studies indicate that attackers now use AI-generated emails, stylometric manipulation, and linguistic mimicry to create more convincing phishing content capable of bypassing traditional email filters [29], [30]. Spear-phishing-targeted phishing aimed at specific individuals or departments-has also grown significantly in sophistication. Attackers often tailor messages using personal or organizational data gathered from social networks, breached databases, or open-source intelligence, making them highly believable and difficult for users to identify [13], [21].

B. Webpage-Based Credential Harvesting

Webpage-based phishing involves the creation of fraudulent websites designed to mimic the appearance and behavior of legitimate online services. These webpages often use cloned HTML/CSS templates, real-time DOM manipulation, JavaScript-based input captures, or session token exfiltration techniques [6], [17], [22]. Research shows that modern phishing kits can replicate entire login flows of financial institutions, e-commerce sites, and enterprise SaaS platforms, including error messages, interactive components, and multi-factor authentication prompts [9], [18]. Due to the increasing adoption of dynamic frameworks such as React, Angular, and Vue, attackers can now embed malicious scripts that adapt page layouts and deliver customized content to users, making detection significantly more challenging [3], [10]. Furthermore, cloud-hosted phishing infrastructures enable adversaries to deploy large-scale phishing sites with minimal effort and rapidly rotate domains to evade blacklists and reputation systems [11], [25].

C. Mobile-Based Phishing (Smishing, App-Based Deception, Mobile Web Phishing)

The widespread use of smartphones has led to rapid growth in mobile phishing, where attackers exploit the unique constraints of mobile interfaces. Smishing-SMS-based phishing-involves sending deceptive text messages having malicious URLs or social engineering prompts [12], [19]. Mobile browsers often hide full URLs, reduce access to certificate information, and display limited security indicators, enabling attackers to craft deceptive webpages that appear legitimate on small screens [20], [26]. Mobile applications pose additional risks, as malicious apps can mimic login screens, overlay fake UI components, or access device permissions to intercept authentication tokens. Studies show that users on mobile devices are significantly more susceptible to phishing due to reduced visual cues, faster decision-making, and habitual behavior patterns [18], [24].

D. QR Code Phishing (QRishing)

QRishing has emerged as a significant attack vector due to the seamless integration of QR code scanning in modern mobile workflows. In QRishing attacks, users are tricked into scanning malicious QR codes placed on posters, menus, payment terminals, emails, or public signage [28]. These codes redirect users to fraudulent websites, initiate unauthorized app actions, or trigger credential-harvesting workflows. Research highlights that individuals often trust QR codes because they appear visually neutral and machine-generated, reducing suspicion and increasing compliance rates [23], [28]. The lack of URL visibility and the automatic execution of encoded actions further increase the risk, particularly when users scan QR codes in public spaces or during financial transactions.

E. OAuth and API-Based Phishing

As modern web applications increasingly rely on OAuth 2.0, OpenID Connect, and API-driven authentication flows, attackers have developed phishing techniques that target authorization workflows rather than traditional login credentials. OAuth phishing-or "consent phishing"-tricks users into granting malicious applications access to their accounts via legitimate OAuth consent screens [3], [7]. Instead of stealing passwords, attackers acquire tokens that allow them to impersonate users or access sensitive resources. Studies show that fraudulent OAuth flows are highly effective because users often trust branded authorization dialogs and fail to inspect requested permissions [6], [8]. Additionally, API-based phishing attacks exploit insecure endpoints, token misdirection, session hijacking, or API impersonation to steal authentication credentials or access data behind authentication layers [5], [9]. These attacks bypass many client-facing security indicators and often go undetected by traditional phishing defenses**.**

F. Voice-Based Phishing (Vishing) and Hybrid Attacks

Vishing (voice phishing) involves attackers using phone calls, VoIP systems, or AI-generated voice synthesis to manipulate victims into sharing sensitive information. With advancements in real-time voice cloning, attackers can impersonate trusted individuals or corporate representatives, significantly increasing user susceptibility. Hybrid phishing attacks combine multiple vectors-such as email + phone follow-ups, SMS + OAuth consent requests, or QR code + webpage impersonation-to reinforce credibility and bypass user suspicion. Recent research highlights a dramatic increase in multi-stage phishing campaigns, particularly those targeting financial institutions and enterprise systems [1], [14], [20].

G. AI-Generated and Adversarial Phishing Content

Generative AI has transformed the phishing landscape by enabling attackers to create highly personalized, grammatically accurate, and stylistically convincing phishing messages. Studies from 2024–2025 show that AI systems can mimic writing patterns, generate fake websites, and even produce adversarial inputs designed to evade ML-based detectors [29], [30]. Attackers also use AI to automate phishing kit development, produce synthetic screenshots, and personalize phishing content at scale. This new class of AI-enhanced phishing poses significant challenges to traditional filters, blacklists, and signature-based detection systems.

3.Phishing in Modern Web Application

Modern web applications rely on highly dynamic interfaces, API-driven logic, federated authentication, and mobile-first usage patterns. Recent studies show that these architectural shifts expand the phishing attack surface by introducing complex URL flows, reduced visibility of security cues, and increased dependence on trust-based identity systems [1], [3], [6]. Attackers now exploit cloud hosting, QR codes, AI-generated content, and deceptive UI elements to bypass traditional defences and manipulate user trust more effectively [12], [28], [29], [30].

3.1 Dynamic Web Interfaces and Attack Surface

Single-page applications (SPAs), script-heavy pages, and modular frontend frameworks increase DOM complexity, enabling attackers to create highly realistic replicas and inject deceptive elements without altering major visual cues. ML/DL detection studies show that modern phishing sites use obfuscation, dynamic redirects, and script-based manipulation to evade static feature detectors [2], [5], [12], [13].

3.2 Browser-Based Security Indicators (and How Attackers Bypass Them)

Research confirms that browser padlocks, URL bars, and warning messages are often ignored or misunderstood by users, making UI-based indicators ineffective [17], [19], [25]. Attackers exploit this by using HTTPS certificates, Punycode domains, and minimal URL differences, which several ML-based studies identify as major sources of misclassification and user deception [6], [10], [14].

3.3 OAuth & API-Centric Phishing

Modern authentication systems relying on OAuth tokens and API redirection chains introduce opportunities for consent phishing, malicious app authorization, and token theft. Several reviews highlight that attackers increasingly mimic OAuth permission screens and exploit multi-step login flows that are hard for users to verify [1], [3], [6]. These vectors are underrepresented in classical ML URL datasets, creating blind spots in existing models.

3.4 Cloud-Hosted & Template-Based Phishing Kits

Recent studies report increasing use of prebuilt phishing kits hosted on cloud services, enabling attackers to deploy spoofed login pages rapidly and at scale [1], [3], [12]. Multimodal DL research shows that these kits closely imitate legitimate branding and layout, reducing the effectiveness of single-view URL classifiers and pushing the need for screenshot-based or hybrid detection models [9], [12].

3.5 Mobile-First Web Usage and Phishing

Survey and behavioural studies consistently show higher phishing susceptibility on smartphones due to limited screen size, hidden URLs, and simplified security indicators [18], [19], [24], [26]. QR-based phishing ("QRishing") specifically targets mobile workflows and exploits users' tendency to trust physical codes without verifying embedded URLs [28].

4.User Awareness, Human Factors, And Anti-Phishing Techniques

User behaviour remains one of the most influential factors determining phishing susceptibility. Recent behavioural and awareness-focused studies consistently show that users often understand phishing conceptually yet fail to detect real attacks due to cognitive overload, misplaced trust, and interface-driven misperception [17], [19], [25]. Several works highlight that risky practices-such as password reuse, ignoring browser warnings, or relying on superficial visual cues-significantly increase vulnerability to phishing attempts in both web and mobile environments [18], [24], [26].

User-level decision errors are strongly shaped by psychological triggers including authority, urgency, familiarity, and emotional framing, which attackers exploit to drive rapid, uncritical action [17], [20], [25]. These behavioural weaknesses are amplified in modern web applications where multi-step authentication, mobile-first interfaces, and dynamic content reduce users' ability to verify legitimacy.

To address these human-centric vulnerabilities, many studies evaluate awareness training and behavioural interventions. Controlled phishing simulations demonstrate that repeated exposure with contextual feedback improves user resilience over time, though effectiveness varies significantly across populations and organisational environments [20], [21], [22]. Higher-education–focused studies show that students and academic staff, despite having high digital usage, often possess weak practical phishing-recognition skills, indicating a persistent awareness–practice gap [19], [24], [26]. Framework-based approaches propose structured awareness models and institutional training programs aimed at reducing behavioural risk through targeted education, scenario-based learning, and continuous reinforcement [23], [27].

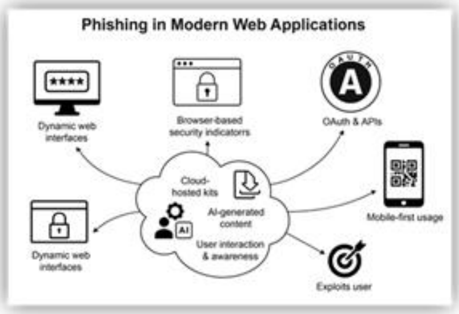

Figure 1: Modern Web Application Phishing Ecosystem

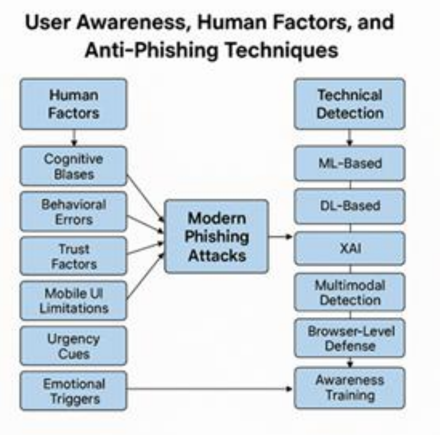

Figure 2: Interaction Between Human Factors and Technical Defenses in Modern Phishing Ecosystems

Alongside behavioural strategies, technical **anti-phishing techniques** remain central to detection and mitigation. Machine-learning–based systems employing models such as Random Forest, SVM, and ensemble classifiers continue to dominate classical detection pipelines, leveraging URL and domain features to classify phishing attempts [8], [10], [14], [15]. Deep-learning architectures-including CNN, GRU, and hybrid CNN–GRU networks-show improved performance by learning patterns directly from raw URLs, HTML, or visual webpage structure [5], [6], [9], [12]. Explainable-AI-driven feature selection enhances interpretability of ML models and highlights critical indicators that contribute to accurate phishing detection [7], [13]. Emerging techniques integrate multimodal features-combining URL text, HTML structure, and page screenshots-to detect visually deceptive phishing pages that bypass traditional classifiers [9], [12]. Recent studies also address novel threats such as AI-generated phishing content and propose stylometric ML approaches to distinguish human-written from LLM-generated emails [29], [30]. Overall, the literature shows that effective phishing prevention requires a combination of **technical detection mechanisms** and **human-centric behavioural strengthening**. While advanced ML/DL models provide strong backend defences, user awareness-especially within modern mobile and web application environments-remains a critical but still insufficiently addressed component of phishing resilience.

5.Conclusion

Phishing has evolved into a highly adaptive and multidimensional threat, shaped by the increasing complexity of modern web applications and the growing influence of mobile-first and AI-driven communication environments. The reviewed literature shows that attackers now exploit dynamic interfaces, multi-step authentication workflows, cloud-hosted phishing kits, and sophisticated AI-generated content that closely mimics legitimate digital interactions. While machine learning and deep learning models-ranging from classical classifiers to multimodal architectures-offer promising detection capabilities, they remain constrained by outdated datasets, adversarial evasions, and limited real-world deployment. Conversely, studies on user awareness consistently highlight that human behaviour continues to be the most vulnerable link, with cognitive biases, trust cues, and interface limitations significantly contributing to phishing susceptibility.

The findings underscore that technical solutions alone cannot mitigate the expanding threat landscape. Effective defence in modern web ecosystems requires an integrated approach that combines advanced detection techniques with sustained user education, behavioural reinforcement, and organisational awareness programmes. Moreover, the emergence of mobile-centric phishing and generative-AI-enabled attacks reveals clear gaps in existing research, particularly in the areas of dataset diversity, cross-platform detection, and psychological resilience. Addressing these gaps will be essential for developing robust, user-centric, and adaptive anti-phishing strategies capable of protecting users as web technologies continue to evolve.

References

[1] M. Naqvi, A. Maddila, and H. Naeem, "Mitigation strategies against phishing attacks," Computers & Security, vol. 130, 2023.
[2] M. Safi, A. A. Mohammed, and F. Alshamrani, "A systematic literature review on phishing website detection," Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 7, 2023.
[3] O. Rashed, "A comprehensive review of machine and deep learning approaches for phishing website detection," International Journal of Science and Engineering Research, vol. 15, no. 1, 2024.
[4] M. Wilk-Jakubowski, K. Grochowina, and A. Janiszewski, "Machine learning and neural networks for phishing detection: A comprehensive review," Electronics, vol. 14, no. 18, 2025.
[5] A. Almujahid et al., "Comparative evaluation of machine learning algorithms for phishing detection," Journal of Big Data, vol. 11, 2024.
[6] I. Haq, M. Raza, and H. Kim, "Detecting phishing URLs based on a deep learning approach," Applied Sciences, vol. 14, no. 22, 2024.
[7] M. Shafin and N. Islam, "An explainable feature selection framework for web phishing detection," Machine Learning with Applications, vol. 16, 2024.
[8] R. Parvathy et al., "Phishing website detection using machine learning algorithms," AJCE, 2022.
[9] S. Ahmed, "Phishing website detection using GRU and CNN hybrid architecture," PowerTech Journal, vol. 3, no. 2, 2025.
[10] S. Sharma and V. Kumar, "Advanced machine learning algorithms for phishing website detection," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 4, 2024.
[11] M. Gowtham, "Deep learning empowered phishing URL detection using FRCNN architecture," IJISAE, vol. 12, 2024.
[12] A. Singh, "Phishing website detection using deep learning with URL, HTML and screenshot features," IJSREM, vol. 8, no. 1, 2025.
[13] R. Wang and J. Li, "Machine learning techniques for phishing detection: A survey," Security Informatics, vol. 9, no. 2, 2025.
[14] S. Khan and P. Singh, "Comparative study of machine learning algorithms for phishing detection," IJACSA, vol. 14, no. 9, 2023.
[15] A. Verma, "Machine learning algorithms for detecting phishing websites: A comparative study," ResearchGate Preprint, 2023.
[16] G. Chauhan, "Intelligent phishing link detection to enhance web security," ResearchGate Preprint, 2023.
[17] A. Gallo et al., "The human factor in phishing: Collecting and analyzing user susceptibility," Computers & Security, vol. 131, 2024.
[18] R. Kalla, "Exploring how user behavior shapes cybersecurity awareness in phishing contexts," ResearchGate Preprint, 2023.
[19] S. Pradhan, "Exploring phishing awareness and user behavior: A survey-based investigation," IJRASET, vol. 12, no. 4, 2024.
[20] M. Morić et al., "Evaluating end-user defensive approaches against phishing: A real-world study," Journal of Cybersecurity and Privacy, vol. 5, no. 3, 2025.
[21] J. Marshall et al., "Exploring the evidence for email phishing training: A systematic review," Computers & Security, vol. 132, 2024.
[22] M. Wambui, "Effectiveness of cybersecurity awareness programs," WJARR, vol. 10, no. 2, 2024.
[23] P. Kayomb, "A phishing attack awareness framework for South African universities," SAJIM, vol. 27, no. 1, 2025.
[24] T. Moyo, "Awareness of phishing attacks in institutions of higher learning," IJRIAS, vol. 9, no. 2, 2024.
[25] A. Sharma, "User awareness and psychological factors in falling for phishing attacks," ResearchGate Preprint, 2025.
[26] M. Gwenhure, "University students' security behavior against email phishing attacks," Journal of Cybersecurity, vol. 11, no. 1, 2025.
[27] . Althobaiti et al., "A review of organization-oriented phishing research," Journal of Cybersecurity and Privacy, vol. 4, no. 4, 2024.
[28] D. Sharevski et al., "Phishing with malicious QR codes: Understanding QRishing," ACM Conference on Computer and Communications Security, 2022.
[29] M. Jabir et al., "Phishing attacks in the age of generative AI," Machines, vol. 6, no. 8, 2025.
[30] E. Opara, "Evaluating spam filters and stylometric detection of AI-generated phishing emails," Expert Systems with Applications, vol. 242, 2025.