JAIEP

The State of Anti-Phishing Platforms: A Survey

Ahmed Mohammed Rabie[1*]

[1]Information Technology Department, College of Computer Science and Artificial Intelligence, Damietta University, Egypt.

* Corresponding author: amrabie@du.edu.eg

Abstract

The insidious nature of phishing attacks remains a significant and costly challenge for digital systems. These attacks exploit both human vulnerabilities and technical errors, resulting in substantial financial losses, data breaches, and reputational damage for individuals and organizations across the globe. Recognizing this increasing threat has led to the emergence of a diverse market of anti-phishing platforms, offering a range of solutions specifically designed to detect, prevent, and reduce these malicious attempts. This paper offers a comprehensive study of this dynamic landscape, encompassing email security gateways, web filtration solutions, endpoint detection and response systems, and user awareness training platforms, including innovative technologies, functions, and main functionalities across various anti-phishing platforms. By analyzing the efficiency and inherent limitations of the current approaches, the purpose of this paper is to equip researchers, security specialists, and organizations with a deeper understanding of available tools and to inform future strategies to effectively defend against this persistent and sometimes fringe threat.

Keywords: Phishing Attacks, Anti-Phishing Platforms, Email Security, User Awareness Training, Detection Techniques
MSC: 68M25; 60G35

Doi : https://doi.org/10.21608/jaiep.2025.374715.1015
Received: April 10, 2025, Revised: May 5, 2025, Accepted: May 12, 2025

Introduction

Phishing attacks represent an important and frequent threat in the digital landscape, utilizing human vulnerabilities to obtain unauthorized access to sensitive information, financial resources and important systems. These attacks, which have developed significantly since their early forms in the 1990s, adapt and come quickly sophisticated social engineering tactics and technical subterfuges to cheat users in different communication channels [2, 1]. The results of successful phishing phenomena can be severe, cause sufficient financial loss, reputational damage data breaches and other harmful effects for individuals and organizations [3].

In response to this developed threat, a wide selection of anti-phishing platforms and techniques has emerged. These platforms use different strategies, from traditional rule -based systems to phishing efforts to detect and prevent machine learning, artificial intelligence and behavioral analysis, blacklisting [4]. In addition, user education and awareness training is still an important component of a broad anti-phishing strategy, giving individuals the opportunity to identify and avoid malicious attempts [5].

The purpose of this paper is to provide a comprehensive study of the current scenario with anti-phishing platforms. It will delay different types of platforms that are available, analyze their underlying

technologies and function, and discuss their efficiency in reducing different forms of phishing attacks. By checking the strength and limitations of the existing solutions, the study wants to provide valuable insights to researchers, specialists and organizations in its continuous efforts to handle phishing and increase digital security.

Related Work

The broader risk of phishing has inspired important research efforts to develop and analyze various anti-phishing techniques and solutions. This section emphasizes the most important areas of the related function, which provides a basis for understanding the need and contribution to extensive anti-phishing platforms.

Several studies have provided specific overviews of phishing attacks and countermeasures. For example, studies such as [9, 11] provide classifications of various phishing attack vectors, including emails and websites to more sophisticated techniques that have vishing and smishing. These surveys list-based methods (blacklists and whitelists) are approaching approaches and user education role also discuss the first-anti-phishing techniques, including the education role [9]. While these tasks provide a valuable foundation, they often occur before they widely adopted an advanced anti-phishing platforms that benefit from artificial intelligence and machine learning.

An important workplace focuses on technical aspects of detecting phishing efforts. This includes research on analysis of network traffic for email content, URLs, website characteristics and malicious indicators [7]. Machine Learning (ML) and Deep Learning (DL) techniques have quickly become prominent in the field, with studies, and discovered their efficiency in identifying phishing emails and websites by learning from a large dataset of malicious and legitimate examples [12, 6]. These studies often evaluate the performance of specific algorithms and functional sets, but cannot provide a comprehensive view of different platforms that integrate these methods.

When recognizing the human element of phishing sensitivity, researchers have also discovered user-centric approaches. This includes studies on the effectiveness of training programs for safety awareness, the design of the user interface to help users identify phishing signals, and the development of devices that allow users to report suspicious activities [10]. Important complements these user-focused approaches often technical anti-phishing platforms instead of having standalone solutions. This survey can bridge this gap by examining how platforms incorporate user education and feedback mechanisms.

Some studies have focused on evaluating the effectiveness of specific anti-phishing techniques or categories of tools, such as email security gateways, browser extensions or anti-malware software [8]. These survey often consider the effect on detection rates, false positive interest rates and system performance. The study can produce it by providing a broad comparative analysis in a wide range of anti-phishing platforms and their integrated properties.

Recent work accept the developed nature of phishing attacks and investigate new trends in anti-phishing defense. This includes the use of threat intelligence, behavioral biometrics and advanced authentication methods to combat quickly sophisticated refined phishing campaigns [6]. This study can contribute to how modern anti-phishing platforms include these state-of-the-art techniques.

Anti-phishing platforms techniques

The ongoing fight against phishing attacks has inspired the development of a diverse armor of built-in anti-phishing platforms [8, 9, 10, 11]. These platforms use a versatile approach, and utilize several methods from examining the email content and checking the web links to monitor the user's behavior and utilize the power of artificial intelligence.

1. Email Content Analysis

A basic technique used by anti-phishing platforms is email content analysis, which carefully examines the body of email messages coming for a series of suspected indicators [7, 9]. The process includes several sub technology designed to identify misleading or malicious content [5, 7]. Keywords and rule-based detection create a basic layer, with emails containing predetermined concepts or patterns usually associated with phishing fraud [5, 7]. More advanced platforms benefit from the Natural Language

Processing (NLP) to go beyond simple keywords, analyze the meaning and contextual nuances of the text to detect misleading languages and manipulation strategy [7, 12]. Stylometric analysis contributes to the writing style of email by identifying deviations, and often cheating a malicious actor trying to implement a legitimate sender [7, 9].

Proofpoint Threat Protection and Mimecast Advanced Email Security such as commercial solutions, NLP and machine learning use refined methods, which are misleading languages, signs of urgent and Business Email Compromise (BEC) and other phishing strategy [1, 4, 7] to analyze email bodies and attachments. Similarly, it is appointed platforms such as Barracuda Email Protection, Check Point Harmony Email & Collaboration, Abnormal Security, Sophos Email, Cisco Secure Email, and Microsoft Defender for Office 365, different forms of material filtering and analysis to detect suspected key and stylistic anomalies. For those looking for Apache SpamAssassin, Proxmox Mail Gateway, and MailScanner offer content-based analysis features that can be integrated into email infrastructure [9]. It's important to note that while email content analysis is an important component, the most effective platform benefits from it in combination with other techniques for a comprehensive defense against developing the threats [9, 10, 11].

2. URL and Link Analysis

Another important technique used by anti-phishing platforms is the URL and link analysis, which carefully examines the built-in URL in the email and faces websites for malicious indicators [7, 5]. This analysis includes several main approaches [7, 5]. Blacklisting and whitelisting provide a basic layer of defense by comparing the URLs database with known malicious or reliable sites [7, 5]. Heuristic analysis examines elements such as the presence of URL, domain age, the presence of type typosquatting (subtle character substitutions) and suspicious subdomain usage [7, 5]. The reputation point increases the detection by assessing the historical risk associated with the domain or IP address as hosting the link [7, 5]. Advanced platforms can use sandboxing and dynamic analysis, and certainly visit the page that is connected in a separate environment and observe their behavior and identify any malicious action before impressing the user [7, 5].

Commercial solutions like Proofpoint Threat Protection, Mimecast Advanced Email Security, and Barracuda Email Protection incorporate techniques such as blacklisting known malicious URLs, heuristic analysis to detect suspicious URL structures (like typosquatting or unusual subdomains), and reputation scoring to assess the historical risk associated with domains and IP addresses [1, 4, 7]. Platforms like Check Point Harmony Email & Collaboration and Cisco Secure Email also perform in-depth link analysis, sometimes including sandboxing or dynamic analysis to safely visit and observe the behavior of linked pages before allowing user access [7]. Additionally, services like Google Safe Browsing and open-source tools like PhishTank provide extensive databases of known phishing URLs that anti-phishing platforms can leverage for real-time blacklisting and analysis [9]. These platforms often combine multiple URL analysis techniques to provide a robust defense against link-based phishing attacks [9, 11, 12].

3. Website Content and Structure Analysis

Once a user clicks on a link, anti-phishing platforms employ website content and structure analysis to determine the legitimacy of the destination page, particularly focus on the presence of malicious content [7, 5]. This analysis uses several main techniques [7, 5]. Visual similarity analysis compares visual elements of a website, such as layout, branding and form design, against known legitimate login pages to detect impersonations [7, 5]. DOM (Document Object Model) analysis delves into the underlying structure and scripts of the webpage, examining the HTML, CSS, and JavaScript for suspicious or malicious code [7]. Content-based heuristics identify red flags within the website's content, such as the absence of crucial legal information like privacy policies, the presence of unusual or excessive forms, or requests for sensitive data on unexpected or unsecure pages [7, 5].

Solutions like Proofpoint Threat Protection and Mimecast Advanced Email Security often employ visual similarity analysis to compare the layout and branding of a website against known legitimate sites [1, 7]. Check Point Harmony Email & Collaboration and Cisco Secure Email delve deeper with DOM analysis, examining the underlying code and scripts for suspicious elements [7]. Furthermore, platforms like Barracuda Email Protection and others utilize Content-Based Heuristics, identifying red

Doi : https://doi.org/10.21608/jaiep.2025.416022
Received: Janu 7, 2025 Accepted: March 10, 2025

flags such as missing privacy policies, unusual forms requesting sensitive information, and inconsistencies in website content that are characteristic of phishing sites [7, 5]. Browser extensions like Netcraft and Bitdefender Traffic Light also perform real-time analysis of website content and structure to warn users about potentially malicious pages [9, 10]. These platforms often combine these techniques to provide a comprehensive assessment of a website's legitimacy [9, 10, 11].

4. Reputation-Based Filtering

An important component of modern anti-phishing platforms is reputation-based filtration, which benefits from extensive data on the reliability of various online institutions [7, 5]. The technique considers the risk of examining the email sender, domain, IP address and URLs [7, 5]. For email, Email Sender Reputation, utilizing protocols like SPF, DKIM, and DMARC, helps verify the authenticity of the sender and prevent domain spoofing [7].The IP address reputation evaluates the historical malicious activity associated with the original IP address, and flags communication from well-known bad actors [7]. Similarly, Domain reputation assesses factors such as the domain's age, registration details, and historical behavior to identify potentially suspicious or newly created domains often used in phishing campaigns [7, 5].

Commercial solutions like Proofpoint Threat Protection, Mimecast Advanced Email Security, and Barracuda Email Protection leverage extensive threat intelligence data to evaluate the reputation of email senders (using protocols like SPF, DKIM, and DMARC), IP addresses, and domains, blocking or flagging communications from sources with a history of malicious activity [1, 4, 7]. Platforms such as Cisco Secure Email and Check Point Harmony Email & Collaboration also incorporate reputation scoring as a key element in their multi-layered defense [7]. Additionally, numerous threat intelligence feeds and services contribute to the reputation data used by these platforms, providing real-time information on emerging threats and suspicious actors [9, 10].

5. Behavioral Analysis

A more advanced approach planned by anti-phishing platforms is behavioral analysis, which goes beyond a static content inspection for the user's behavior and monitoring of the user interaction for abnormal patterns that can generate a phishing attack or a compromised account from a [7, 5]. This technique is often involved in anomaly detection, including identifying deviations from installed criteria, such as unusual login locations or times, unexpected data access patterns or deviant communication frequencies [7, 5]. In addition, User and Entity Behavioral Analytics (UEBA) plays an important role in establishing basic behavior for individual users and different institutions in the system, so that the platform can flag of any significant deviation that can indicate malicious activity as a result of a successful phishing effort [7, 5].

Commercial solutions employing this technique often fall under the umbrella of User and Entity Behavioral Analytics (UEBA) [1, 4]. Vendors like Proofpoint, Mimecast, Abnormal Security, and Cynet utilize UEBA to establish baseline behaviors for users, analyzing patterns in login attempts, data access, communication patterns, and other activities to identify deviations that could signal malicious activity stemming from a successful phishing attempt [1, 4]. These platforms often leverage machine learning algorithms to continuously refine their understanding of normal behavior and improve the accuracy of anomaly detection [1, 4, 11].

6. Machine Learning and Artificial Intelligence

A company with modern anti-phishing platforms is the integration of a foundation machine learning (ML) and artificial intelligence (AI), which benefits from the huge dataset for both phishing and legitimate content to identify and increase the accuracy of identifying complex patterns and detection [11, 12]. These platforms use different ML/AI techniques, including monitored learning, where the model is trained on the data labeled to classify as email, URLs or websites malicious or benign [11, 12]. Unsupervised learning algorithms are also used to identify nonconformities and the first unsettled patterns in data without a clear label, which is able to detect the new phishing attacks [11, 12]. Furthermore, deep Learning techniques, utilizing neural networks, allow platforms to learn intricate features from raw data, such as performing sophisticated image analysis to detect subtle forgeries in logos or website layouts [11, 12].

Commercial Solutions proceeds to explain other industry leaders such as Proofpoint which utilizes AI for advanced threat detection systems, including BEC [1, 4, 7]. Mimecast also uses AI and machine learning to scan email bodies, URLs, and attached files for phishing indicators [1, 4, 7]. Abnormal Security is exceptional for its behavioral AI, which detects normal communication patterns to identify abnormal signposts typical of phishing [1, 4, 7]. Microsoft Defender for Office 365 adds an AI module to email message analysis for identifying phishing attempts within the Microsoft ecosystem [1, 4, 7]. Other pertinent examples include Barracuda Phishing and Impersonation Protection, which combines AI and ML technologies to detect and obstruct email attacks, and anti-phishing expert IRONSCALES, who uses AI to adapt and counter phishing attempts [1, 4, 7]. Additionally, Google's capabilities with Gmail includes an AI, TensorFlow, that daily blocks millions of phishing emails, while the Safe browsing API machine learns to tell good links from bad ones [1, 4, 7]. These examples show increasing dependence on AI and ML technology to effectively respond to advancing phishing strategies and improve detection precision [11, 12].

7. User Awareness and Training Platforms

To accept that only technology cannot completely eliminate the threat of phishing, user awareness and training platforms, focusing on strengthening individuals to become an important defense team [5, 9, 10]. These platforms appointed a suit with educational appliances, including simulated phishing attacks designed to mimic real landscape and assess user monitoring [5, 9, 10]. Interactive training modules provide structured learning experiences, cover different strategies used with the knowledge to identify and avoid them [5, 9, 10]. It is important that these platforms also include reporting mechanisms, which can easily flag users, which contributes valuable intelligence to the organization's security efforts and facilitates the reaction to the event in time [5, 9, 10].

A multitude of platforms specialize in User Awareness and Training to combat phishing effectively [5, 9, 10]. Prominent commercial examples include KnowBe4, renowned for its extensive training content and simulated phishing attacks, including Kevin Mitnick's security awareness training [5, 9, 10]. Proofpoint Security Awareness Training offers a diverse library of customizable training materials and realistic threat simulations [1, 7]. Infosec IQ provides comprehensive training modules, micro-learning videos, and a vast library of phishing email templates for simulations [5, 9, 10]. Cofense PhishMe focuses on real-world relevant simulations derived from actual phishing threats reported globally [5, 9, 10]. Other notable platforms include Hoxhunt, which uses AI and gamification to personalize training, Phished, offering personalized simulations and "snackable" training, and SANS Security Awareness, known for its expert-curated training content and robust simulation capabilities [5, 9, 10]. These platforms equip organizations to educate their employees, test their susceptibility through simulated attacks, and foster a security-conscious culture [5, 9, 10].

8. Multi-Factor Authentication (MFA) Enforcement

While the enforcement of multifactor authentication (MFA) stands as an important preventive measure that significantly reduces the effect of successful phishing attacks on the identification [4, 5, 7]. Users must provide a new form of confirmation beyond their password, MFA adds a sufficient layer of security [4, 5, 7]. General MFA techniques include One-Time Passcodes (OTP) generated through authenticator apps or sent via SMS, push notifications, which require users to approve login inserts on a reliable device, and fingerprints or face recognition [4, 5, 7]. Although a phisher manages to steal the user's password, the enforcement of the MFA makes it quite difficult for them to obtain unauthorized access to accounts and sensitive information [4, 5, 7].

Multi-Factor Authentication Enforcement does not specifically focus on detecting phishing, it is well known that credential phishing is a great threat to organizations regardless of the security architecture in place. Many identity management solutions include sophisticated MFA features that mitigate the adverse effects of successful credential phishing [4, 5, 7]. For example, Duo Security (now a part of Cisco) has numerous methods of MFA such as push notifications, one-time passcodes, and even biometric authentication [4, 5, 7]. Microsoft Entra ID (formerly Azure AD) provides comprehensive ecosystem MFA features within the Microsoft family, alongside extensive comprehensive MFA options [4, 5, 7]. Okta, widely recognized as a top identity and access management service provider, has advanced MFA enforcement capabilities [4, 5, 7]. It is important to note that many endpoint security and email security gateway solutions, while not dedicated to MFA, offer or can be adapted to

Doi : https://doi.org/10.21608/jaiep.2025.416022
Received: Janu 7, 2025 Accepted: March 10, 2025

work with MFA frameworks to strengthen the security defense against credential phishing attempts [4, 5, 7].

Table 1: Comparison of Cybersecurity Techniques Across Various Security Platform Categories

Technique	Email Security Platforms	Web Security Platforms	Endpoint Security Platforms	User Awareness Training Platforms	Phishing Simulation Platforms	AI-Powered Platforms
Email Filtering	In-depth content analysis, sender reputation checks (SPF, DKIM, DMARC), attachment scanning, behavioral analysis, spam filtering.	Limited direct application. May integrate with email security.	May flag malicious links within emails.	Educates users on identifying suspicious email characteristics.	Used to send simulated phishing emails to test user vigilance.	Enhance filtering accuracy by identifying patterns and anomalies.
URL Analysis & Blocking	Real-time analysis of links within emails, sandboxing of linked pages, reputation checks of domains.	Real-time scanning of visited URLs, blocking access to known phishing sites, analyzing website content for malicious indicators.	May block access to known phishing URLs clicked within applications.	Teaches users to hover over links and identify suspicious URLs.	Often used within simulated emails with malicious or lookalike URLs.	Improve detection of malicious URLs and identify new phishing sites.
Attachment Scanning	Heuristic and signature-based scanning of email attachments, sandboxing to analyze behavior in a safe environment.	Downloads may be scanned upon reaching the endpoint.	Scans downloaded files for malware.	Warns users about the risks of opening unexpected attachments.	May include attachments in simulations to test user behavior.	Enhance detection of malicious attachments through behavioral analysis.
Behavioral Analysis	Analyzes email sender and recipient patterns, communication styles to detect anomalies.	Monitors user browsing behavior for unusual activity or access to suspicious sites.	Tracks application behavior for signs of malicious activity originating from phishing attempts.	Educates users on typical attacker behaviors and red flags.	Simulates realistic phishing scenarios to observe user behavior.	Identify subtle anomalies in email content, sender behavior, and website characteristics.
Multi-Factor Authentication (MFA) Enforcement	May integrate with MFA solutions to ensure account security even if credentials are compromised.	May enforce MFA for access to web applications to prevent takeover after phishing.	Can be a component of endpoint security to protect access to the device and applications.	Emphasizes the importance of MFA as a preventative measure.	Not directly simulated but its importance is often highlighted.	Can identify compromised accounts by detecting unusual login attempts despite MFA.
Anti-Spoofing Techniques	Implementation and verification of SPF, DKIM, and DMARC records to prevent sender address forgery.	May identify and warn users about potentially spoofed websites.	May alert users to applications or communications with spoofed identities.	Educates users on how to identify signs of email spoofing.	Simulated phishing emails often test user recognition of spoofed addresses.	Improve the accuracy of identifying spoofed emails and websites.
User Reporting Mechanisms	Provide buttons or easy ways for users to report suspicious emails for analysis.	May allow users to report suspicious websites.	May include options for users to report potential phishing attempts encountered through various applications.	Encourages users to actively participate in identifying threats.	Provides a feedback loop based on user reports of simulated attacks.	Analyze user-reported items to improve detection rules and identify new threats.
Threat Intelligence	Integration with databases of	Utilize feeds of malicious	Leverage threat intelligence to	Informs users about current	Simulations can be based	Enhance detection

Feeds	known phishing domains, URLs, and malware signatures.	websites and infrastructure.	identify known malicious indicators.	phishing trends and tactics.	on real-world threat intelligence.	accuracy by incorporating the latest threat information.

Future Work

The landscape of the phishing attacks is constantly evolving, and seeks innovation and research in anti-phishing platforms. In order to construct on the ongoing study, future research should detect intensive integration between different anti-phishing platform components and other safety devices such as Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), and threat intelligence platforms. Investigating standardized data sharing formats and APIs could facilitate more effective threat detection and response across different layers of security infrastructure. In addition, expanding the collaboration between different anti-phishing platforms and threat intelligence providers to detect mechanisms for sharing information can lead to more active and comprehensive defense against new phishing campaigns.

While AI and ML are quickly widespread in anti-phishing solutions, further research is needed to increase efficiency towards sophisticated and adaptable phishing attacks. This involves developing stronger models that are able to understand fine linguistic signals, detect subtle visual deception on websites and identify asymmetrical patterns with high accuracy and less false positive prices. The discovery of the explainable of AI (XAI) in anti-phishing can also improve the understanding of trust and identification mechanisms.

Future work should also focus on adapting anti-phishing platforms to address emerging attack vectors beyond traditional email and web-based phishing This includes effective defense against phishing attacks through SMS (smishing), voice call (Vishing), social media platforms and other developed communication channels. Cross platform analysis will significantly significant correlation of research and phishing efforts in different vectors.

When you go beyond the reactive identity, future research should examine the active and future anti-phishing techniques. This includes taking advantage of advanced threat intelligence to estimate and block the potential phishing campaigns before reaching users, as well as developing predictive models to identify individuals or organizations at higher risk of being targeted.

Despite technological progress, human element is still an important vulnerability in the fight against phishing. Therefore, future work should detect innovative methods to increase the user's awareness and flexibility against these attacks. This includes research in individual and adaptive security training programs, more comfortable user interfaces for reporting suspected activities, and user -friendly devices that provide real -time risk assessment and guidance. Achieving psychological factors affecting the sensitivity to phishing and designing interventions based on behavioral science also attracts further attention.

Developing standardized metrics and methodologies is still a challenge to evaluate the effectiveness of various anti-phishing platforms. Consequently, future research should focus on establishing a strong structure to assess the total effect of these platforms on reducing the frequencies of future research, false positive prices, flexibility against stolen techniques and successful phishing events. Comparative evaluation in different platforms and techniques performed in the realistic environment will provide valuable insight to both researchers and specialists.

Finally, future research can detect the extensive economic and social effect of phishing attacks and the efficiency of anti-phishing platforms to reduce these results. This involves analyzing the costs of investments to distribute various anti-phishing solutions associated with successful phishing events. By pursuing these research directions, the anti-phishing area can continue to evolve and develop more efficient and adaptable defense against this frequent and harmful cyber threats.

Conclusion

This survey has provided a comprehensive observation of the current scenario with anti-phishing platforms, which highlights the techniques and various matrices to function to fight this wide cyber threat. In order to increase the integration of traditional rules-based systems and reputation filtration to

Doi : https://doi.org/10.21608/jaiep.2025.416022
Received: Janu 7, 2025 Accepted: March 10, 2025

sophisticated AI and machine learning algorithms, these platforms represent an important defense layer for the protection of individuals and organizations with harmful consequences of phishing attacks. We have introduced various detection mechanisms, including email and URL analysis, website content, behavioral monitoring and an important role as user awareness learning in increasing the general security currency.

Modern anti-phishing platforms quickly benefit from several levels, and integrate many of these techniques to integrate these techniques to increase the accuracy and flexibility of sophisticated theft strategy. The emergence of AI and ML provides a significant promise of identifying micro - discrepancies and adapting the new phishing campaigns, while the user constantly emphasizes education outlines the importance of human element in a strong security strategy.

However, despite the progress of anti-phishing technologies, the danger is important. The attackers are constantly refining their techniques, utilizing new weaknesses and benefiting from social engineering strategy with increasing sophistication. It requires continuous research and development in anti-phishing platforms, improved integration, active defense mechanisms focus on more efficient user-centered security solutions.

Finally, the study of anti-phishing platforms emphasizes the complexity and importance of this domain. Although there has been significant progress in developing effective defense, it requires the ongoing arms race between the attackers and the guards innovation and a holistic approach that combines technological progress with user strength to reduce the permanent threat of phishing. In this study, the insight provided a valuable basis for understanding the current status of anti-phishing platforms and exposing important areas to future research and development in this important field of cyber security.

References

1. Proofpoint. (n.d.). What Is Phishing? - Meaning, Attack Types & More. Retrieved from https://www.proofpoint.com/us/threat-reference/phishing
2. Verizon Business. (2020). The History of Phishing Attacks. Retrieved from https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/
3. Imperva. (n.d.). What is phishing | Attack techniques & scam examples. Retrieved from https://www.imperva.com/learn/application-security/phishing-attack-scam/
4. Cybersecurity. (2024, September 3). Understanding Anti-Phishing Solutions and 5 Quick Anti-Phishing Tips. Retrieved from https://www.cynet.com/cybersecurity/understanding-anti-phishing-solutions-and-5-quick-anti-phishing-tips/
5. CrowdStrike. (n.d.). What is Phishing? Techniques and Prevention. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/phishing-attack/
6. CEUR-WS.org. (n.d.). Phishing Attacks Detection. Retrieved from https://ceur-ws.org/Vol-3384/Short_7.pdf
7. Check Point Software. (n.d.). Phishing Detection Techniques. Retrieved from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/phishing-detection-techniques/
8. Emerald Insight. (2012). Phishing counter measures and their effectiveness – literature review. Journal of Small Business and Enterprise Development, 19(4), 669-684.
9. IJCST. (n.d.). A Survey on Phishing and Antiphishing Strategies. Accessed from: https://www.ijcstjournal.org/volume-6/issue-2/IJCST-V6I2P13.pdf
10. KIT. (n.d.). Literature Review: Misunderstandings Regarding Phishing. Accessed from: https://publikationen.bibliothek.kit.edu/1000176659/155838351
11. Malaya Journal of Mathematics. (2021). An analysis of anti-phishing methods: From traditional techniques to machine learning. Malaya Journal of Mathematics, S(1), 54-60.
12. MDPI. (2023). An Advanced Phishing Detection Method Using Deep Learning and Security with Uniform Resource Locators. Sensors, 23(9), 1 4403.