International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Phishing Attacks and Prevention Techniques

Krunal Belpande, Aniket Pote

G H Raisoni University, Amravati, Maharashtra, India

Abstract

These messages usually create a false sense of importance. People are tricked into giving passwords or money because they believe the sender knows what they're talking about. Fake websites also copy popular services to make users think they're on familiar ground. Sometimes voices on phones act like tech support just to get passwords spoken aloud. The goal is always to steal private details through clever deception. Phishing shows up in many ways - email scams, precise attacks, big fish tricks, text messages, voice calls - each hitting differently depending on who gets chased and how it arrives. Getting smarter, these scams keep pushing limits, putting people, companies, and officials at real danger across the planet.

One way to fight phishing is through hands-on awareness programs. These sessions help people recognize risky messages. Another layer comes from requiring extra identification steps when logging in online. Strong passwords matter too - using confusing strings makes cracking easier. Staying current with the latest system fixes also blocks gaps left by older versions. Tools that scan incoming emails can flag suspicious subject lines or links. When questions arise, checking whether claims match known company practices add clarity.

KEYWORDS: *One way to stop phishing? Strong safeguards at work and home - two-factor login can block intruders, just like layered email checks. Tools that flag suspicious messages make a difference too, whether built into inboxes or used separately. Protection grows when viruses are kept away by reliable software, while guarded networks limit outside risks. Messages stay safe if they travel encrypted, using trusted seals like HTTPS or secure certificates. Big players' tricks include signing emails with DMARC, confirming senders via SPF, or sealing content with DKIM - each step counts. Cyber awareness training helps guard against phishing. Strong passwords matter just as much, along with how people manage them. Staying current with software changes builds resistance too. Tools like IDS and IPS add layers of protection. Training stands out when it becomes part of daily routine.*

1. Introduction

Phishing has emerged as one of the most common and dangerous cyberattacks in the modern digital landscape. Unlike traditional cyber threats that focus on exploiting software vulnerabilities, phishing primarily targets human behavior and trust. Attackers manipulate individuals through deceptive communication in order to obtain sensitive information such as login credentials, financial details, and confidential organizational data. Because phishing relies on psychological manipulation rather than technical weaknesses, it has become highly effective and continues to evolve as attackers develop more sophisticated techniques. Recent cybersecurity reports indicate that phishing remains a major contributor to global cyber incidents and is frequently used as an entry point for many large-scale data breaches [9].

In recent years, phishing campaigns have grown significantly in scale and complexity due to the rapid development of automation tools and artificial intelligence technologies. Modern phishing attacks can generate highly personalized messages that appear authentic to the recipient. Even when sent to thousands of users simultaneously, these messages can include customized information that increases their credibility and makes them harder to detect. Security analyses suggest that a large proportion of social engineering attacks now involve automated phishing tools that can produce convincing emails, websites, and communication templates within seconds. As a result, organizations are facing a rapidly expanding threat landscape where phishing attacks are becoming more frequent and more difficult to identify [5]. Another major factor contributing to the rise of phishing attacks is the increasing reliance on digital communication platforms. Email systems, messaging applications, and social media networks are widely used for both personal and professional communication, making them attractive targets for cybercriminals. Phishing attacks often appear in the form of emails that impersonate trusted organizations such as banks, online services, or workplace administrators. These messages typically include malicious links that redirect victims to fraudulent websites designed to steal login credentials or financial information. Studies show that phishing attacks are responsible for a significant portion of cyber intrusions, with many security breaches occurring after attackers successfully obtain legitimate user credentials through deceptive communication [7]. In addition to traditional email-based phishing, attackers have expanded their strategies to include multiple communication channels. Smishing attacks use SMS or mobile text messages to deliver fraudulent links or fake security alerts, while vishing attacks involve phone calls where attackers impersonate customer service representatives or technical support agents. These multi-channel phishing strategies increase the likelihood of reaching victims through different platforms and communication habits. As cybercriminals diversify their attack methods, phishing continues to spread across various digital environments, affecting individuals, businesses, and government institutions worldwide [10]. The effectiveness of phishing attacks is largely driven by social engineering techniques that exploit common human emotions and decision-making patterns. Attackers often design messages that create urgency, fear, curiosity, or trust to manipulate victims into taking immediate action. For example, a phishing email may claim that a user's account has been compromised and request immediate verification through a provided link. Because these messages appear to originate from trusted sources, many users respond without

verifying the authenticity of the communication. Research has shown that such psychological manipulation significantly increases the success rate of phishing attacks compared to purely technical cyber threats [3].

To address the growing threat of phishing, cybersecurity researchers and organizations have developed various detection and prevention mechanisms. Traditional approaches include techniques such as spam filtering, signature based detection, and URL blacklisting systems that block known malicious websites. These methods analyse incoming emails and web links to identify suspicious patterns and prevent potentially harmful messages from reaching users. However, traditional detection mechanisms often struggle to identify newly created phishing websites or previously unseen attack strategies, as attackers continuously modify their tactics to bypass existing security systems [6]. More advanced solutions have emerged with the adoption of machine learning and artificial intelligence technologies. These systems analyse large volumes of data and identify subtle patterns associated with phishing activities. Machine learning models can evaluate multiple features such as domain characteristics, hyperlink structures, email content, and website design elements in order to classify potential threats. By learning from historical attack data, these models improve their ability to detect previously unknown phishing campaigns. Such intelligent detection systems are increasingly integrated into modern cybersecurity infrastructures to enhance threat detection capabilities [8]. Despite these technological advancements, cybersecurity experts emphasize that technical defenses alone cannot fully eliminate phishing risks. Because phishing primarily targets human behavior, user awareness and cybersecurity education remain essential components of effective defense strategies. Training programs that educate individuals about recognizing suspicious messages, verifying email sources, and avoiding unknown links play a critical role in reducing the success rate of phishing attacks. Organizations that combine technological protection with user awareness initiatives are better equipped to defend against the constantly evolving phishing threat landscape [1].

Furthermore, recent cybersecurity reports highlight the growing role of artificial intelligence in accelerating cyberattack processes. AI-driven tools can rapidly collect information, generate convincing phishing content, and automate large-scale attack campaigns. According to global cybersecurity assessments, artificial intelligence has significantly increased the speed and efficiency of cyberattacks, enabling attackers to execute complex phishing operations with minimal effort. These developments demonstrate the urgent need for stronger security frameworks, continuous monitoring systems, and collaborative cybersecurity strategies to protect individuals and organizations from future phishing threats [5].

Furthermore, the rapid digital transformation across industries has increased the exposure of individuals and organizations to phishing threats. As businesses increasingly rely on cloud services, remote communication platforms, and online collaboration tools, attackers have gained more opportunities to distribute malicious messages and fraudulent links. Phishing campaigns often take advantage of everyday digital interactions such as online banking notifications, workplace communication, or service verification emails. Because these messages appear to originate from trusted platforms, users often fail to recognize subtle warning signs. Cybersecurity studies indicate that many successful cyber incidents begin with a single phishing email that leads to unauthorized system access and further exploitation of organizational networks [9]. In addition to technological solutions, organizations are now focusing on developing stronger security cultures to reduce the effectiveness of phishing attacks. Security awareness training programs, simulated phishing exercises, and strict authentication policies are increasingly implemented to improve user resilience against social engineering attacks. Multi-factor authentication, secure email gateways, and advanced threat monitoring systems are also widely adopted to strengthen organizational defenses. When combined with continuous cybersecurity education, these protective measures significantly reduce the risk of credential theft and unauthorized access. Therefore, a combination of technological safeguards, proactive monitoring, and informed user behavior remains essential for effectively combating the evolving challenges posed by phishing attacks in modern digital environments [1].

2. Literature Review

Phishing is considered one of the most common and dangerous cybercrimes committed over the internet. It is a form of cyberattack in which an attacker uses social engineering techniques to manipulate victims into revealing sensitive information such as usernames, passwords, banking details, and other personal data. Unlike traditional hacking methods that exploit technical vulnerabilities, phishing focuses on exploiting human psychology and trust. Attackers often disguise themselves as legitimate organizations such as banks, online service providers, or corporate authorities to convince victims that the communication is genuine. As digital communication continues to grow, phishing has become one of the most widely used techniques for initiating cyberattacks and gaining unauthorized access to information systems [9].

Over time, phishing techniques have evolved significantly. In the early stages, attackers mainly relied on largescale spam emails sent to thousands of users without targeting specific individuals. However, as users and organizations became more aware of these threats, attackers started developing more sophisticated approaches. Modern phishing campaigns now include targeted strategies such as spear phishing and whaling. Spear phishing focuses on specific individuals within an organization, while whaling targets high-level executives and decisionmakers who often have access to critical corporate resources. In addition to email-based attacks, phishing techniques have expanded to other communication platforms such as SMS messages and voice calls, commonly referred to as smishing and vishing. These techniques allow attackers to reach victims through multiple communication channels, increasing the likelihood of a successful attack [10]. One of the key reasons phishing remains highly successful is its ability to exploit fundamental elements of human psychology. Social engineering tactics used in phishing attacks commonly rely on emotions such as trust, urgency, fear, and curiosity. For example, attackers may create messages that appear to come from a trusted authority or warn users about urgent security issues requiring immediate action. These messages often encourage victims to click on malicious links or provide sensitive information without carefully verifying the source of the communication. Because these psychological triggers

influence human decision-making, phishing attacks often achieve higher success rates compared to many other types of cyber threats [7].

Another factor contributing to the growing effectiveness of phishing is the increasing use of automation and artificial intelligence technologies by cybercriminals. Modern phishing campaigns can generate large volumes of personalized messages by analysing publicly available data from social media platforms, online profiles, and organizational websites. AI-driven tools can mimic writing styles, replicate legitimate email formats, and automatically generate convincing phishing content. As a result, phishing emails are becoming more difficult for users and traditional security systems to detect. This technological advancement has significantly contributed to the continued rise in financial fraud incidents and data breaches associated with phishing attacks [5]. To prevent and detect phishing activities, researchers and cybersecurity professionals have proposed several technological solutions. Traditional detection mechanisms include techniques such as URL blacklisting, signature-based detection, and rule-based filtering systems.

These methods rely on previously identified malicious domains or known phishing patterns to block suspicious content. While these approaches can be effective against known phishing websites, they often fail to detect newly created phishing pages or previously unseen attack strategies. Attackers frequently generate new domains and modify phishing content, making it difficult for static detection systems to keep up with the evolving threat landscape [3]. In response to these limitations, more advanced detection approaches have been developed using machine learning and deep learning technologies. These systems analyse various features of emails, URLs, and websites to classify them as legitimate or malicious. Machine learning models can examine characteristics such as domain age, hyperlink structure, webpage layout, and textual patterns within messages. By learning from large datasets of phishing and legitimate samples, these models can identify subtle patterns that indicate potential phishing attempts. Studies have shown that machine learning-based detection systems can achieve significantly higher accuracy compared to traditional filtering techniques [6].

Another important technological approach involves the use of Natural Language Processing (NLP) techniques to analyses the textual content of emails. NLP models examine the structure, tone, and language patterns used in email messages to detect suspicious communication. For instance, phishing emails often contain unusual grammatical structures, urgent instructions, or requests for confidential information. By analysing these linguistic patterns, NLP-based systems can identify potentially malicious messages and alert users before they interact with harmful links or attachments. This approach helps security systems provide more detailed and context-aware analysis of suspicious emails [8]. Despite the effectiveness of modern technological solutions, research consistently shows that technical defenses alone cannot fully eliminate phishing threats. Attackers continuously adapt their strategies to bypass detection systems and exploit human vulnerabilities. Therefore, effective phishing prevention requires a combination of advanced technology, user awareness, and organizational security policies. Security awareness training programs help users recognize phishing attempts and develop safer online behaviours, while authentication mechanisms such as multi-factor authentication add an additional layer of protection against credential theft. By integrating technological defenses with human-cantered security practices, organizations can significantly reduce the impact and success rate of phishing attacks in modern digital environments [1].

Furthermore, the continuous growth of digital communication platforms and online services has expanded the opportunities for phishing attackers to target a larger number of users. As individuals increasingly rely on email, mobile applications, and social media for both personal and professional communication, attackers exploit these platforms to distribute deceptive messages and malicious links. This growing dependency on digital technologies makes users more vulnerable to sophisticated phishing campaigns. Cybersecurity reports also indicate that phishing remains one of the primary initial attack vectors used in many large-scale cyber incidents and data breaches across organizations worldwide [9]. Therefore, strengthening both technological defenses and user awareness programs is essential to minimize the risks associated with phishing attacks and to ensure a safer digital environment for individuals and organizations.

Fig 2: Phishing Attack vs Prevention Visual Map

Research Methodology

Phishing attacks represent one of the most challenging cybersecurity problems because they rely primarily on manipulating human behaviour rather than exploiting purely technical vulnerabilities in software systems. Unlike traditional cyberattacks that target weaknesses in code, phishing attempts aim to deceive users into revealing sensitive information such as passwords, financial details, or organizational credentials. This human-cantered nature makes phishing particularly dangerous, as even the most advanced technical security systems can fail if users are tricked into voluntarily providing confidential information [9]. Early academic studies highlighted the importance of understanding the social dimension of cyber threats. One of the foundational works in this area was the study titled *"Social Phishing,"* conducted by Jagatai and colleagues in 2007. Their research demonstrated how attackers could exploit social relationships and communication networks to increase the success rate of phishing campaigns. By analysing social networking data, the researchers found that attackers who appeared to possess insider knowledge about a victim's connections could establish a higher level of trust [3]. The study emphasized that phishing attacks become significantly more convincing when they incorporate personal details about the recipient. Instead of sending generic spam messages, attackers began developing more targeted strategies. This led to the rise of spear phishing, a technique in which attackers carefully collect information about their targets from social media platforms, professional networking sites, and public databases. These personalized attacks often include references to the recipient's workplace, colleagues, or recent activities, making them appear highly authentic [7]. As communication technologies evolved, phishing techniques also expanded across multiple communication channels. While email remains the most common medium for phishing attacks, cybercriminals have increasingly shifted toward alternative platforms to reach potential victims. One example is smishing, a phishing technique that uses SMS or text messages to deliver fraudulent links or requests for sensitive information. Because mobile users often respond quickly to text messages, smishing attacks can be particularly effective [10]. Another related technique is vishing, which involves voice-based phishing through phone calls. In these attacks, criminals impersonate representatives from banks, technical support teams, or government agencies to persuade victims to share confidential information. The emergence of these techniques demonstrates how phishing has evolved into a multi-channel threat that operates across digital communication systems. Social media platforms have also become an important target for phishing campaigns where attackers distribute malicious links through compromised or fake accounts [2].

In response to the growing sophistication of phishing attacks, researchers and cybersecurity professionals have focused on improving authentication and verification mechanisms for digital communication. One widely adopted approach involves implementing email authentication protocols such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). These protocols help verify whether an email message actually originates from the domain it claims to represent. By checking the authenticity of the sending server and validating cryptographic signatures attached to messages, these mechanisms significantly reduce the chances of domain spoofing [4]. Another important area of research focuses on the use of machine learning techniques to detect phishing attacks. Machine learning-based detection systems analyse various attributes of incoming messages and websites in order to classify them as legitimate or malicious. These attributes may include characteristics such as email headers, language patterns, link structures, domain registration details, and webpage design elements. Research conducted within cybersecurity institutions has demonstrated that intelligent detection models can significantly improve the identification of phishing attempts compared with traditional filtering techniques [3] Despite these advancements, machine learning systems still face challenges when dealing with newly emerging phishing campaigns, often referred to as zero-day attacks. Because these attacks use previously unseen techniques, detection systems may initially fail to recognize them as malicious. This limitation highlights the need for continuous model training and the integration of threat intelligence data from multiple sources. Modern cybersecurity organizations continuously monitor threat patterns and analyse global attack data to identify new phishing techniques at an early stage [5].

Researchers have also explored behavioral monitoring as a complementary strategy for detecting phishing-related incidents. Instead of focusing solely on message content, behavioral analysis examines patterns of user activity within digital systems. Unusual login attempts, unexpected location changes, or abnormal email-sending behavior can indicate that an account has been compromised. For example, if an employee account suddenly begins sending a large number of emails containing suspicious links, this may signal that the account has been hijacked by an attacker [8]. In addition to technological defenses, the human factor remains a critical component of effective phishing prevention. Numerous studies emphasize the importance of cybersecurity awareness and user training programs in reducing the likelihood of successful phishing attacks. Employees who are trained to recognize common phishing indicators—such as suspicious links, unexpected attachments, urgent requests for confidential information, or unusual sender addresses—are less likely to fall victim to deceptive messages. Many organizations now conduct simulated phishing campaigns as part of their training programs to improve awareness and strengthen organizational security practices [6]. Observations from cybersecurity research conducted in recent years highlight the importance of adopting a comprehensive and adaptive defense strategy. Phishing threats continue to evolve as attackers experiment with new technologies and communication platforms. Consequently, organizations cannot rely on a single defensive mechanism to protect their digital infrastructure. Effective protection requires a combination of technical safeguards, user awareness programs, and collaborative threat intelligence sharing between organizations and industries [1].

4. Result

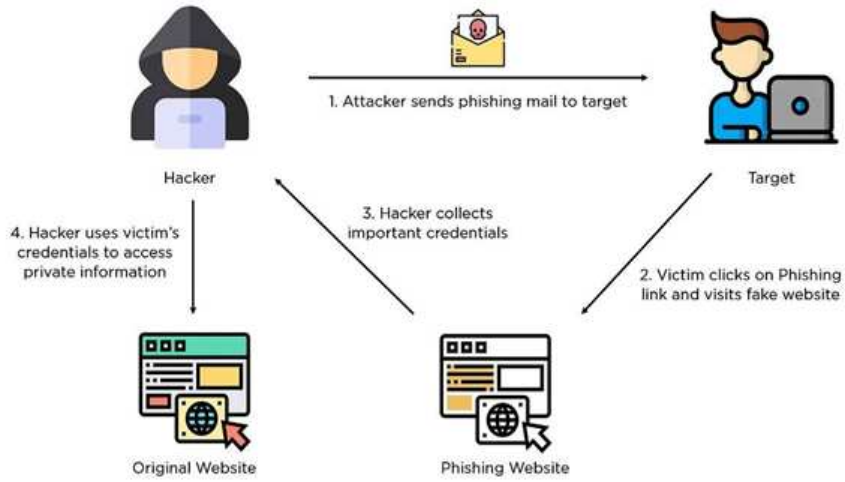

Fig.3Phishing Attack Flow Diagram

The results obtained from the analysis of phishing attack patterns demonstrate how cybercriminals successfully exploit human trust and communication channels to gain unauthorized access to sensitive information. The attack process typically begins when an attacker sends a carefully crafted phishing email to the target. This message often appears to come from a trusted organization such as a bank, company administrator, or well-known online service provider.. At this stage, the victim is often asked to enter sensitive information such as login credentials, personal identification details, or financial data. The attacker then collects these credentials through the phishing website and stores them for further exploitation. After obtaining the victim's information, the attacker can use these credentials to access the legitimate system, allowing them to steal confidential data, perform fraudulent transactions, or gain deeper access to the organization's network infrastructure. The results highlight how a seemingly simple interaction— such as clicking a malicious link— can lead to serious cybersecurity consequences.

Further observations indicate that phishing attacks succeed not only because of technical weaknesses but primarily due to human behavior and lack of awareness regarding cybersecurity risks. The study shows that many users fail to verify the authenticity of emails, websites, and digital communication before responding. Attackers exploit this behavior by designing phishing messages that create urgency, curiosity, or fear, which encourages victims to act quickly without carefully evaluating the situation. Additionally, the results reveal that phishing campaigns are becoming more sophisticated with the integration of automation tools and artificial intelligence techniques. Attackers are now capable of generating highly personalized phishing messages using publicly available information gathered from social media platforms and online databases.

These targeted attacks, commonly known as spear-phishing, significantly increase the success rate compared to generic phishing attempts. The findings also indicate that phishing attacks are no longer limited to email communication alone. Modern attackers frequently use multiple communication channels such as SMS messages (smishing), phone calls (vishing), and social media messaging platforms to reach potential victims. Because users interact with these communication platforms daily, attackers can exploit routine digital behavior to increase the likelihood of successful attacks. These results demonstrate that phishing has evolved into a multi-channel threat that can affect individuals, organizations, and digital infrastructures across various sectors. The implementation of authentication frameworks such as SPF, DKIM, and DMARC has also contributed to reducing domain spoofing attacks by verifying the authenticity of email senders. However, the results show that technological defenses alone are not sufficient to eliminate phishing threats. Attackers continuously adapt their strategies to bypass security filters by modifying message structures, using compromised accounts, or hosting phishing pages on newly registered domains. As a result, organizations must adopt a layered security approach that integrates technical protection with user education and behavioral awareness.

Another important finding of this study is the role of cybersecurity awareness training in reducing successful phishing attacks. Organizations that conduct regular security awareness programs and simulated phishing exercises tend to experience lower incident rates compared to those that rely solely on automated security tools. Training programs help users recognize common phishing indicators such as suspicious links, unusual sender addresses, grammatical errors, or unexpected requests for sensitive information. MFA requires users to provide multiple forms of authentication, such as one-time verification codes or biometric identification, thereby reducing the effectiveness of credential theft attacks. Overall, the results emphasize that effective phishing defense requires a comprehensive cybersecurity strategy that combines advanced security technologies, strong authentication mechanisms, continuous monitoring systems, and user awareness programs. By integrating these approaches, organizations can significantly strengthen their resilience against evolving phishing threats and minimize the risk of data breaches and financial losses in modern digital environments.

5. Conclusion

Phishing continues to remain one of the most persistent and dangerous cybersecurity threats in the modern digital environment. Despite the development of advanced security technologies, phishing attacks continue to succeed because they primarily exploit human behavior rather than technical vulnerabilities. Cybercriminals constantly refine their

techniques to appear more legitimate and convincing, making it increasingly difficult for individuals and organizations to detect malicious attempts. As a result, phishing strikes continue to impact users across the globe, often causing financial loss, data breaches, and reputational damage. These attacks are designed to be deceptive and subtle, allowing them to remain unnoticed while quietly compromising systems and stealing sensitive information. Different forms of phishing attacks have emerged to target users through the communication channels they rely on most. Traditional phishing attacks commonly occur through email, where attackers impersonate trusted organizations such as banks, government institutions, or well-known companies. By sending deceptive emails that appear authentic, attackers encourage victims to click malicious links or provide sensitive information such as login credentials and financial details. In addition to email phishing, newer forms of attacks have become increasingly common. Smishing, for example, uses text messages instead of emails to reach potential victims. Since people often trust and respond quickly to messages on their mobile devices, smishing has become a powerful tool for cybercriminals. Another advanced form of phishing is whaling, which specifically targets highlevel executives and senior decision-makers within organizations. These individuals often have the authority to approve large financial transactions or access sensitive corporate data, making them attractive targets for attackers seeking high-value gains. The increasing sophistication of phishing techniques demonstrates that cybersecurity cannot rely solely on technical defenses. While technologies such as spam filters, threat detection systems, and email security gateways are essential components of modern cybersecurity infrastructure, they cannot fully eliminate phishing threats.

Attackers continuously adapt their strategies to bypass security systems, making human awareness and vigilance a critical line of defense. Therefore, maintaining strong cybersecurity awareness among users is essential in reducing the effectiveness of phishing attacks. Staying safe in the online environment requires individuals to adopt careful digital habits and maintain a proactive mindset when interacting with digital communications. Users should always verify the authenticity of emails, messages, and links before clicking or responding. Suspicious messages that create a sense of urgency, request confidential information, or come from unknown sources should always be treated with caution. Additionally, organizations should encourage employees to report suspicious messages so that potential threats can be identified and addressed quickly. Developing a culture of cybersecurity awareness within organizations can significantly reduce the likelihood of successful phishing attacks. Education and continuous awareness programs play a crucial role in strengthening cybersecurity defenses. By regularly training users about the latest phishing techniques, organizations can help individuals recognize warning signs and respond appropriately to potential threats. By continuously monitoring emerging cyber threats, improving security technologies, and educating users about safe online practices, individuals and organizations can strengthen their defenses against phishing attacks.

In conclusion, staying informed about evolving cybersecurity risks and adopting responsible online practices remain essential steps in protecting both individuals and organizations from cyber threats. Phishing attacks may continue to evolve, but with increased awareness, vigilance, and strong security measures, their success can be significantly reduced. Proactive defense strategies and continuous learning will remain key factors in ensuring a safer and more secure digital environment for everyone.

Reference

[1] Verizon Enterprise Solutions, “Data Breach Investigations Report (DBIR),” 2025.

[2] Anti-Phishing Working Group (APWG), “Phishing Activity Trends Report,” 2025.

[3] SANS Institute, “SANS Whitepaper,” 2024.

[4] National Institute of Standards and Technology (NIST), “Cybersecurity Framework,” 2023.

[5] European Union Agency for Cybersecurity (ENISA), “Cybersecurity Threat Landscape Report,” 2024.

[6] Kaspersky Security Team, “Internet Security Threat Report: Global Threat Intelligence Findings,” 2025.

[7] Cisco Talos Intelligence Group, “Cisco Annual Cybersecurity Report,” 2024.

[8] Microsoft Defender Research Team, “Social Engineering and Email Threat Intelligence Report,” Microsoft Security, 2025.

[9] Verizon, “Data Breach Investigations Report (DBIR): Global Analysis of Cyber Breaches,” 2025.

[10] Anti-Phishing Working Group (APWG), “Phishing Activity Trends Report: Quarterly Analysis of Global Phishing Activity,” 2025

[11] William Stallings: Essentials of Network Security.

[12] Security Bulletin and Phishing Reports from Kaspersky.

[13] Cisco's yearly cybersecurity report.

[14] Microsoft: Security Intelligence Report.

[15] Google: Research on Safe Browsing and Phishing Prevention.

[16] Research on phishing awareness and prevention, SANS Institute.

[17] The International Journal of Computer Applications publishes studies on phishing detection.