A comprehensive study on Phishing Attacks: Evolution, Detection Models, and Prevention Techniques.

Chewang Dukpa
Sikkim Manipal Institute of Technology

Abstract- Phishing remains a major concern in the field of cybersecurity, as it continues to deceive users through deceitful messages, websites, and emails. This paper offers a detailed study of phishing attacks, covering their history, methods, and the techniques used to recognize and stop them. The main aim is to understand how phishing has changed over time and to examine the effectiveness of different solutions used to prevent it. The paper discusses various approaches to identifying phishing, compares older methods and evaluates their strengths and weaknesses. A summary table is included to compare recent studies based on their focus and results. The discussion highlights the growing complexity of phishing tactics and the need for better protection methods. The paper concludes by outlining possible future developments, such as improved safety practices, better user training, and stronger security systems to reduce the risks caused by phishing.

1. INTRODUCTION

Phishing is a form of network-based threat where attackers use misleading methods—such as imitation websites, fraudulent emails, or false messages—to deceive individuals into providing confidential details like usernames, passwords, or financial information. These attacks rely on both technical tricks and psychological manipulation to take advantage of users' trust in familiar sources. The intent is often to gain unauthorized access to personal or organizational systems.

1.1 Why phishing remains a major cybersecurity threat

Phishing attacks remain successful because they take advantage of how people naturally think and react. Unlike other cyber threats that depend only on system weaknesses, phishing tricks people by playing on their trust, sense of urgency, and curiosity.

Attackers send fake emails, messages, or make phone calls that look like they come from trusted sources such as banks, coworkers, government offices, or well-known companies. These messages often create a feeling of urgency, warning that something bad might happen—like a frozen account or missed payment—if the person doesn't act quickly.

This kind of pressure makes people ignore their usual caution and click on harmful links or share private information without checking carefully.

Social media has made this problem worse, as attackers use the personal information people share online to send more believable, targeted messages. Even careful and knowledgeable users can be tricked when they are tired, distracted, or stressed.

Since these attacks rely on human nature, which is hard to change, phishing will continue to find ways around even the best technical protections.

1.2 Global statistics and impact

Phishing continues to be one of the most effective and widespread forms of cybercrime, adapting rapidly to technological changes and user behavior. As of 2024, cybercriminals are sending an estimated 3.4 billion phishing emails daily, totaling more than 1 trillion phishing attempts annually, highlighting the massive scale at which these campaigns operate [1]. Unlike traditional cyberattacks that often require exploiting software vulnerabilities, phishing is rooted in psychological manipulation, targeting human weaknesses such as trust, fear, and urgency. Roughly 80% of all phishing campaigns are designed specifically to steal login credentials, with attackers increasingly focusing on cloud services like Microsoft 365, Google Workspace, and other enterprise platforms [2].

Phishing attacks are not just limited to random mass emails. In 64% of reported business email compromise

(BEC) incidents, attackers used more sophisticated and targeted approaches—often impersonating high-level executives or trusted contacts—leading to average financial losses of $150,000 per incident [2]. Alarmingly, modern phishing campaigns are becoming harder to detect, with around 80% of phishing websites now using HTTPS, giving victims a false sense of security as the browser displays the familiar padlock symbol [2].

The phishing landscape is also diversifying in terms of delivery channels. Nearly 40% of attacks now go beyond email, appearing in tools such as Slack, Microsoft Teams, SMS, and popular social media platforms [2]. These multi-channel attacks exploit the trust people place in instant communication tools and often take advantage of relaxed user vigilance in informal environments. For instance, QR code phishing (or quishing) has emerged as a growing threat, with a 25% year-over-year increase, as attackers place malicious QR codes in physical locations like posters, flyers, or even fake customer service stands, tricking users into scanning them and visiting harmful sites [2].

Voice phishing (vishing) is also gaining traction, with 30% of organizations reporting attempts where attackers posed as company officials or public authorities over phone calls to pressure employees into revealing sensitive information [2]. At the same time, the availability of phishing kits on the dark web has surged by 50%, making it easier for inexperienced criminals to launch convincing and well-designed attacks without any coding skills [2].

Another alarming trend is the use of brand impersonation. In just one year, over 44,750 phishing domains were created to mimic Facebook, tricking users into entering credentials on lookalike login pages [2]. These attacks are often further enhanced by data scraped from social media platforms, allowing cybercriminals to craft personalized messages that increase the success rate of their scams. The growing use of social engineering combined with modern technology means even educated and cautious users can be deceived—especially during moments of distraction or stress [3].

In summary, phishing's continued dominance is a result of its low cost, high return, and adaptability to new platforms and user habits. Its shift from simple email-based deception to sophisticated, multi-channel attacks shows that technical defences alone are not enough. Effective protection now requires comprehensive user education, real-time monitoring, cross-platform security solutions, and strong authentication practices [4].

2. OBJECTIVES

Phishing has become one of the most troubling cybersecurity issues in today's digital world. Unlike attacks that focus on software vulnerabilities, phishing deceives people directly by using false messages, fake websites, and impersonated identities. Its methods are simple but powerful, relying on emotions such as fear, urgency, or trust to trick individuals into revealing sensitive information. Despite improvements in security tools, phishing remains highly effective because it targets human behaviour—something that cannot be easily patched or upgraded. The rise of social media, mobile apps, and remote work tools has given attackers more ways to reach victims, often in places where users feel safe and less cautious.

The continued success of phishing highlights a serious gap between technical defences and user awareness. As attacks grow more convincing and widespread, there is a clear need to explore how phishing tactics are changing and how current security systems are keeping up. This study is driven by the need to better understand phishing's impact, how it adapts to new environments, and which detection or prevention methods are most effective. By reviewing both old and new techniques and looking at global trends, the study aims to help strengthen defences, improve awareness, and support safer digital practices for individuals and organizations alike. Therefore, this study sets out clear objectives:

- To analyse the evolution of phishing
- To compare modern and traditional detection techniques
- To Identify prevention strategies and their effectiveness

3. OVERVIEW

3.1 Historical timeline

Date	Findings
1994–1995	The word "phishing" came about when AOHell was released, a program that made it easier to deceive AOL users into giving away their passwords and credit card details. This was the start of many similar attacks aimed at everyday users. [5]
2001	Phishing grew to focus on online payment platforms like e-gold. These early attempts showed a move toward targeting financial services, but they had only limited success.[6]
2003–2004	Phishing attacks increased against e-commerce sites such as PayPal and eBay, where scammers set up fake websites and sent forged emails to trick users into giving up their login details.[6]
2007–2008	Botnets such as Storm and Asprox appeared, sending out massive waves of phishing emails to infect devices and break into systems. This highlighted how large-scale and automated phishing had become[6]
2013	Cryptolocker ransomware was spread through phishing emails containing harmful attachments. It locked users' files and demanded payment to restore access, showing how phishing had evolved into more damaging and aggressive attacks.[6]
2020	A significant phishing incident hit Twitter, where attackers used social engineering to break into internal systems. This showed that even major platforms are vulnerable to such threats.[6]
2023	Phishing kits started circulating widely on the dark web, allowing attackers to easily create realistic fake websites and emails. This led to a rise in both the number and complexity of phishing attempts.[6]

3.2 Common types of Phishing

Phishing attacks have become increasingly diverse and sophisticated, utilizing a variety of strategies to deceive individuals and gain access to sensitive information. The most widespread forms include email phishing, spear phishing, voice phishing (vishing), and SMS phishing (smishing). Each of these methods relies heavily on social engineering techniques, which manipulate human psychology to trick users into revealing confidential data such as passwords, financial details, or personal identification [5], [8].

In recent years, Business Email Compromise (BEC) has emerged as a particularly dangerous variant, where attackers impersonate high-ranking officials or trusted contacts within an organization. These attacks often aim to fraudulently authorize financial transactions, and because they typically avoid using malicious links or attachments, they can bypass many traditional security measures [9]. Another significant threat comes from pharming attacks, which manipulate domain name system (DNS) configurations or local host files to silently redirect users from legitimate websites to counterfeit ones without their awareness, complicating detection efforts [5].

Additionally, search engine phishing involves attackers influencing search results to promote fraudulent websites designed to closely resemble legitimate services, thus trapping users who are searching for familiar brands or products [8]. Man-in-the-Middle (MITM) phishing is also a concern, especially on unsecured networks like public Wi-Fi. In these attacks, cybercriminals intercept data transmissions in real time, capturing sensitive information such as login credentials before it reaches the intended destination [8].

A more recent development in phishing is angler phishing, which exploits social media platforms by creating fake customer support profiles. These profiles engage with users seeking help, then manipulate them into sharing confidential information or making unauthorized payments [9].

The continuous evolution of phishing techniques demonstrates how attackers adapt to new technologies and communication channels, exploiting users' trust and behaviour patterns. This growing complexity means that traditional email-based defences are no

longer sufficient. To effectively counter these threats, organizations and individuals must adopt a multi-layered security approach. This includes ongoing user education to recognize phishing attempts, implementation of multi-factor authentication, and deployment of advanced detection systems capable of monitoring threats across various platforms in real time.

3.3 Phishing Lifecycle

A mastermind stages the attack in a procedural manner, to maximize the chance of success, Understanding the sequence is very important. Understanding these stages is crucial for developing effective detection and prevention strategies.

a. Baiting

At this stage, attackers prepare something that looks trustworthy to catch the victim's attention. It could be an email, text message, phone call, or fake website that appears to come from a reliable source like a bank or a well-known company or sometimes even someone the victim knows. The goal is simple, make the victim believe the message is genuine by using emotional triggers such as fear, urgency, love or curiosity. Research shows that attackers have become better at making their messages look real and convincing [8]

b. Delivery

Next, the fake message is sent to the target using different ways such as email, text messages, phone calls, scanner, or social media. Attackers pick the method the target is most likely to use. Social media and instant messaging are popular because they are harder for security measures to catch.

c. Execution

This is when the victim interacts with clickbait, for example by clicking a link, downloading a file, or entering login details on a fake page. This step turns the trick into a real attack. Attackers often use fake login pages or malware to steal information or gain access. Studies show that combining technical methods with psychological tricks increases the chances of success [3].

d. Data Theft

Finally, the attacker collects the information entered by the victim, such as passwords, credit card numbers, or personal data. This information can be used for identity theft, financial fraud, or further attacks. Modern phishing tools often automate this process, making it easier for attackers to steal and use the data quickly.[8]

3.4 Read World Case Scenario

2020 Twitter Attack

In July 2020, Twitter experienced a significant security breach when several employees were targeted through spear phishing attacks, which allowed unauthorized individuals to gain access to internal administrative tools. The attackers impersonated Twitter's IT personnel and contacted employees who were working remotely, persuading them to disclose their login credentials. With these compromised credentials, the attackers accessed high-profile Twitter accounts belonging to public figures such as Elon Musk, Barack Obama, Jeff Bezos, as well as major corporations including Apple and Uber. These hijacked accounts were used to post fraudulent messages soliciting Bitcoin donations, resulting in approximately $180,000 being transferred to the attackers' wallets. This incident exposed critical weaknesses in Twitter's cybersecurity infrastructure, including insufficient email phishing protections on employee devices and inadequate privileged access management and monitoring systems. The breach led to a 4% drop in Twitter's stock price and forced the company to postpone the rollout of new API features aimed at improving security protocols. This case underscores the importance of robust cybersecurity practices, including comprehensive employee training on social engineering threats and the implementation of strict access controls, to prevent similar attacks in the future.[13]

2013-2015 Facebook/Google Breach

Between 2013 and 2015, Facebook and Google were targeted by a well-planned spear phishing attack that caused significant financial damage. The attacker, a man from Lithuania, sent fake emails that looked like they came from a trusted manufacturing partner. These emails tricked employees into approving large payments, which were then sent to the attacker's accounts. The attack was revealed in 2017 after the man was charged for his actions. Although Facebook was able to recover most of the lost money, the two companies together lost over $100 million. This case shows how dangerous it is to trust messages without verifying their source. Attackers who study their

targets closely can easily pretend to be someone trusted. It highlights the importance of double-checking the sender's identity through other means before sharing money, sensitive information, or passwords. [14]

4. ANALYSIS

Signature based detection method

Signature-based phishing detection is one of the oldest and most common ways to find phishing emails and threats on a network. It works by looking for known patterns, called "signatures," which come from previously identified phishing attacks. These patterns include things like suspicious URLs, IP addresses, email subjects, types of attachments, or typical phrases used by phishers. When a new email arrives, the system checks its parts—such as the header, message content, links, and attachments—and compares them against the stored signatures. If it finds a match, the email is marked as phishing. Examples of tools that use this method include SpamAssassin and commercial email filters like Proofpoint and Mimecast, which keep their signature lists updated regularly and check emails in real-time. This approach works well for catching known phishing attacks and usually has fewer false alarms because it relies on clear rules. As Garera et al. (2007) noted, signature-based systems are good at detecting emails that follow previously seen phishing patterns. But the main problem is that they can't catch new phishing methods, especially ones where attackers change URLs or disguise content to avoid detection. This happens because the system only looks for signatures it already knows.

Also, the method depends on how often the signature list is updated. If updates are slow, new phishing tricks can slip through. Signature-based detection also struggles with attacks that change slightly every time to avoid matching the stored signatures. [11]

In short, signature-based detection is fast and effective at finding repeated, known phishing threats but isn't good at handling new or specially crafted attacks. It works best when combined with other security methods as part of a larger defence system. [11]

Feature signatures – what they mean:

Feature	What it could be!
Header abnormalities	Unusual sender address, spoofed domains
Message content	Incorrect grammar, "ACTION REQURIED URGENT" etc, threats
URLS	Mismatched texts/links
Attachments	.exe file or some macro enabled documents
Fingerprinting	To match previously seen email

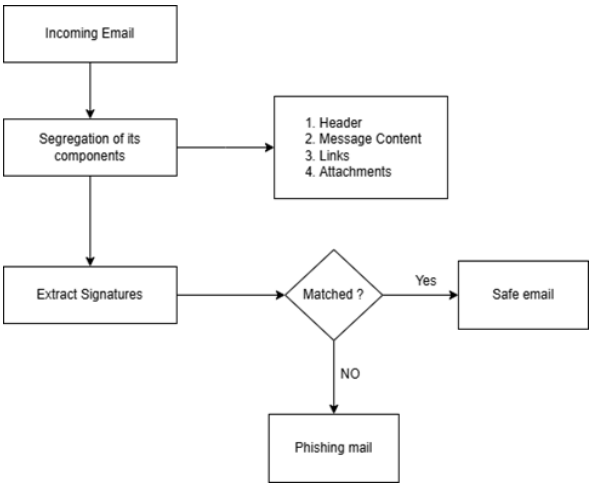

Fig. Depicts the workflow of the signature-based detection

Signal-based phishing detection has both strengths and weaknesses. One advantage is its ability to quickly identify suspicious activity by monitoring specific signals, such as unusual login times, location mismatches, or unexpected changes in user behaviour. It works well in real-time and does not rely on complex computations, making it efficient and easy to implement in many systems. However, it also has limitations. Signal-based methods may produce false alarms when legitimate behaviour happens to match a phishing signal. They can also miss new or subtle phishing attempts that do not trigger predefined signals, making them less effective against evolving or well-crafted attacks. [11]

Heuristic method:
Heuristic techniques play an important role in phishing detection by analysing the content and structure of websites, emails, or messages based on known warning signs. These signs include elements such as the use of shortened or misspelled URLs, the absence of security certificates (HTTPS), excessive use of urgent phrases like "verify now" or "account locked," and mismatches between displayed and actual link destinations. Heuristics also check for the presence of input fields requesting sensitive information—such as passwords or credit card numbers—on pages where such requests are unusual.

In emails, heuristic methods might flag messages that use generic greetings like "Dear user," poorly written grammar, or unfamiliar sender addresses. In website analysis, they may evaluate the visual structure, checking for copied logos, inconsistent branding, or imitation of well-known page layouts.[16].

These methods do not rely on stored examples of past attacks. Instead, they use rule-based analysis to spot traits commonly found in fraudulent activity. Because of this, heuristic detection is especially useful for catching new or modified phishing attempts that may not yet be part of any known list or database. However, for the rules to remain effective, they must be updated regularly to reflect changes in phishing tactics. This allows heuristic systems to provide early warnings and act as a frontline defence against both common and emerging phishing threats. [12] [16].

Some of the ways and methods are:
Url analysis:
1. Check for misspellings – faceebook.com instead of facebook.com
2. Use of Internet protocol addresses in place of domain names.
3. Confusing urls
4. Link labelled as one thing but directing elsewhere.

Content Features:
1. Marked as “URGENT or ACTION REQURIED”
2. Request for personal or financial details
3. Ways that are asking password or pins

Technical Features:

1. Http not secured – HTTPS not used but http
2. Embedded scripts
3. Hidden frames or invisible texts
4. Sender and header checks

Heuristic-based phishing detection offers a practical approach by using rules and patterns to identify suspicious behaviour or content. One of its main advantages is that it can detect unknown phishing attempts by looking for characteristics commonly found in phishing, such as misleading URLs, suspicious keywords, or fake login forms. It is also faster than some complex detection systems and does not depend on large databases. However, it has certain limitations. Heuristic methods can sometimes flag safe content as phishing if it shares similar traits, leading to false positives. They also require regular updates to the rules as attackers find new ways to bypass them, and they may not catch highly sophisticated or carefully disguised phishing attempts. [16].

Machine learning and Deep Learning Techniques
Models based on machine learning and deep learning offer reliable methods for detecting phishing by uncovering patterns in data that are difficult to detect through manual methods. These approaches support flexible and large-scale analysis for recognizing harmful content across websites, emails, and other digital communication channels. [17]

Data collection and extraction :
These models require a labelled dataset- consisting of phishing and legitimate examples. Features are extracted based on these examples and good vs bad is picked up by the machine, which serves as a learning curve. These features vary with structure, format, visual depending upon how the algorithm choses to pick out the differences. [17]

For example:

Based on:	Features:
URL	1. length 2. Presence of IP address 3.Number of sub-domains
Site	SSL certificate – HTTPS or HTTP
Context – in email for example	1. Use of Urgency 2. Asking intricate details 3. Presence of numerous subdomains 4.Sender domain inconsistency 5. Incorrect grammar

Machine learning Models:

Machine learning models use organized data features to develop systems that distinguish between phishing attempts and genuine cases. [17]

Model Type	Description
Decision Tree	Makes decisions by asking a series of yes/no questions based on the data's features.
Random Forests	Combines many decision trees to make better and more reliable predictions.
Support Vector Machine	Draws a line (or boundary) between phishing and safe examples to separate them clearly.
Logistic Regression	Calculates how likely it is that something is phishing, using a formula based on the data.
k-Nearest Neighbors	Looks at the closest known examples and decides based on what they are labelled as.

Deep learning models:

Deep learning models are useful when working with complex and unorganized data, such as full email text or images of websites. These models can automatically find important patterns in the data without needing the features to be manually defined. This makes them especially useful for detecting phishing in situations where the content varies widely in form and structure. [17]

Model Type	Used for	Description
Feed forward	Structured information such as URL length, link count, or presence of forms	Learns from known phishing characteristics to separate suspicious from safe content.
Convolutional Neural Network (CNN)	Visual content like screenshots of fake websites or login pages	Recognizes fake logos, copied layouts, and unusual design patterns found in phishing sites.
Recurrent Neural Network (RNN) / LSTM	Email messages, subject lines, or message body text	Examines how words are arranged to spot common language tricks used in phishing attempts.

Evaluation metrics:

To assess the performance of phishing detection models, several evaluation metrics are used:

Metric	Definition
Accuracy	Proportion of total emails or websites correctly identified as either phishing or legitimate.
Precision	Proportion of items marked as phishing that were phishing.
Recall	Proportion of actual phishing items that were correctly identified as phishing.
F1 score	A balanced measure that considers both precision and recall.
False Positive rate	Proportion of safe emails or websites that were wrongly labelled as phishing

Although these learning-based methods work well for phishing detection, they also have some drawbacks. If the data used for training is incorrect or not balanced, the system may give wrong results. Some models also need a lot of computer power and memory, which can be difficult to manage. In some cases, attackers may design phishing content in a way that tricks the system into thinking it is safe. Lastly, certain methods are hard to understand, making it unclear why a specific email or website was marked as phishing or not. [17]

5. TRADITIONAL VS MODERN PHISHING DETECTION TECHNIQUES

Phishing detection has progressed significantly, shifting from basic traditional techniques to more advanced and adaptive modern methods. Traditional approaches mainly rely on predefined lists, rule-based systems, and signature matching. These include blacklists of known phishing domains, spam filters that detect specific keywords or phrases, and checks for known malicious attachments or links. Such methods are straightforward, easy to deploy, and

provide fast results, making them effective for identifying repeated or widespread phishing campaigns. However, they have clear limitations. Since these techniques depend on prior knowledge, they often fail to detect new or slightly modified phishing attempts that have not yet been added to the system's database. This makes them less effective against targeted or evolving attacks.[18]

Modern phishing detection techniques aim to overcome these shortcomings by focusing on real-time analysis and pattern recognition. Instead of only comparing data to known threats, they examine various elements such as the structure of a URL, the behaviour of a website, or the tone and language used in an email. These techniques can detect suspicious activity based on traits commonly found in phishing, even if the exact form of the attack has never been seen before. For example, they might flag emails with mismatched sender addresses and domain names, or websites that mimic the appearance of trusted platforms but lack valid security certificates. By looking at how messages are written, where they originate, and what actions they request, modern methods provide a more dynamic form of protection. Although they may require more processing resources and constant updates, these newer techniques are better suited to identify, and block sophisticated or zero-day phishing attacks. When used together, traditional and modern approaches create a more complete and resilient system for detecting and stopping phishing threats.[18]

Aspect	Traditional	Modern
Detection	Predefined rules, blacklists, and known signatures	Real-time analysis of structure, behaviour, and content
Data Dependency	Relies on known phishing examples or static patterns	Focuses on characteristics and behaviour patterns even in unseen cases
Adaptability	Low adaptability to new or evolving threats	High adaptability to new and dynamic phishing attempts
Speed	Fast, low resource usage	Slightly slower, may require more processing power
False Positives	Moderate; based on rigid rules	Can be reduced through context-based analysis
Examples	Blacklist filtering, spam keyword matching	URL structure analysis, email content inspection, page behaviour analysis
Limitation	Misses new or cleverly disguised attacks	May require higher computational resources
Strength	Simple, fast, and effective for well-known threats	Flexible, better at detecting advanced or unknown phishing attacks

6. RESULTS AND DISCUSSION

This study examined various phishing detection methods and assessed their usefulness in handling different forms of online deception. Traditional approaches, such as blacklists, keyword-based filters, and static rule checks, were found to be effective for identifying repeated or known phishing sources. These techniques offer quick responses and are easy to implement but fall short when facing newly crafted or slightly altered threats. Heuristic methods, which rely on common warning signs like suspicious URLs, unusual wording, or urgent messages, performed reasonably well at spotting unknown attempts. However, they require regular updates to remain accurate and may still allow more cleverly disguised attacks to slip through.

More advanced detection methods that analyse the structure, wording, and behaviour of emails or websites in real time showed stronger results overall. These techniques consider factors such as mismatched sender addresses, suspicious web layouts, and requests for sensitive information. Systems that combine both

content analysis and behavioural signals—such as irregular login times or unusual activity—were the most successful in identifying threats before users could be harmed. Despite their improved performance, these newer methods may be slower or more demanding on system resources. Overall, the findings support a layered defence strategy that blends older and newer techniques. Relying on a single method is not enough; a mix of early warning signs, system checks, and user awareness offers the best protection against phishing.

7. CONCLUSION

Phishing continues to be a serious threat in the cybersecurity landscape, tricking users through fake emails, misleading websites, and convincing messages. This paper explores the evolution of phishing attacks, tracing their development and uncovering how these schemes have adapted to bypass protective systems. A detailed look is taken at the different strategies used to detect phishing, with special attention to how early tools like blacklists, rule-based filters, and manual checks offered simple but limited defence. These older methods, while quick and easy to use, often failed to stop newer or more sophisticated attempts, especially those designed to mimic legitimate communication more closely.

The paper goes further by comparing these traditional methods to more modern techniques that examine the structure, language, and behaviour of suspicious content. Rather than relying on known threats, newer approaches look for signs of danger in real time—such as unusual patterns in website design or warning signs in how an email is written. A summary table is included to showcase recent studies; each reviewed for its focus area and results. Through this comparison, the paper highlights that while traditional tools are still useful in some cases, they are no longer enough on their own. The growing complexity of phishing tactics requires smarter, layered approaches that combine early detection with user awareness and stronger safeguards. In conclusion, the paper emphasizes the need for constant updates, better training, and more responsive systems to stay ahead of phishing threats.

REFERENCE

[1] StationX, “Phishing Statistics: 100+ Scary Phishing Facts [2024 Update],” *StationX Cybersecurity Blog*, 2024. [Online]. Available: https://www.stationx.net/phishing-statistics/

[2] Hoxhunt, “Phishing Trends Report 2024: Human Risk Review,” *Hoxhunt Cybersecurity Insights*, 2024. [Online]. Available: https://hoxhunt.com/guide/phishing-trends-report

[3] Anti-Phishing Working Group (APWG), “Phishing Activity Trends Report – Q2 2023,” *APWG*, 2023. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf

[4] Terranova Security, “What is Spear Phishing? The Targeted Threat Explained,” *Terranova Security*, 2023. [Online]. Available: https://terranovasecurity.com/what-is-spear-phishing/

[5] M. Jakobsson and S. Myers, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley, 2007. https://onlinelibrary.wiley.com/doi/book/10.1002/0470086106

[6] Phishing.org, "History of Phishing," 2023. [Online]. Available: https://www.phishing.org/history-of-phishing. [Accessed: May 20, 2025].

[7] K. Chiew, G. Yong, and C. Tan, “A survey of phishing attacks: Their types, vectors and technical approaches,” *Computers & Security*, vol. 68, pp. 1–24, 2018, doi: 10.1016/j.cose.2018.06.004. https://www.sciencedirect.com/science/article/pii/S0957417418302070

[8] FBI Internet Crime Complaint Center (IC3), “2023 Internet Crime Report,” 2023. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[9] “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” *Frontiers in Computer Science*, 2021. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

[10] Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). *A framework for detection and measurement of phishing attacks*. Proceedings of

the 2007 ACM Workshop on Recurring Malcode. https://dl.acm.org/doi/abs/10.1145/1314389.1314391

[11] OWASP Foundation, "OWASP: Open Web Application Security Project," *OWASP*, https://owasp.org (accessed Jun. 12, 2025).

[12] J. Tidy, "Twitter hack: Staff tricked by phone spear-phishing scam," *BBC News*, 31-Jul-2020. [Online]. Available: https://www.bbc.com/news/technology-53607374.

[13] "Facebook and Google lost $100 million to spear phishing scam," *Wired*, 2017. [Online]. Available: https://www.wired.com/story/facebook-google-spear-phishing-100-million-scam/. [Accessed: 20-May-2025]

[14] E. Dymoke, "GTA 6 leaks and Uber hacked through social engineering," TechCrunch, Sep. 19, 2022. [Online]. Available: https://hoxhunt.com/blog/gta-6-leaks-and-uber-hacked-through-social-engineering

[15] "Methods of Phishing Detection," *ResearchGate*, Publication No. 385526291, Available: https://www.researchgate.net/publication/385526291_METHODS_OF_PHISHING_DETECTION

[16] D. M. Divakaran and A. Oest, "Phishing Detection Leveraging Machine Learning and Deep Learning: A Review," *arXiv*, May 16, 2022. doi: 10.48550/arXiv.2205.07411

[17] S. Kavya and D. Sumathi, "Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection," *Artificial Intelligence Review*, vol. 58, no. 2, art. no. 50, Dec. 2024, doi: 10.1007/s10462-024-11055-z. https://link.springer.com/article/10.1007/s10462-024-11055-z