Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Phishing Attacks Detection and Prevention Techniques: An Overview

Ali A. Alani[a], Adil Al-Azzawia[b]*

[a]*University of Diyala, College of Science, Computer Science Department, Diyala, Iraq.Email: alialani@uodiyala.edu.iq*

[b]*University of Diyala, College of Science, Computer Science Department, Diyala, Iraq.Email: adil_alazzawi@uodiyala.edu.iq*

ARTICLE INFO

Article history:
Received: 27 /1/2025
Rrevised form: 3 /2/2025
Accepted : 2 /3/2025
Available online: 30 /3/2025

Keywords:

Phishing, Websites, Attacks, Cybersecurity, Machine Learning, Search Engine.

ABSTRACT

The rapid rise in global internet usage has resulted in many online services in numerous fields, such as e-commerce, buying and selling goods or services, social networking, and e-government. As a result, there has been a significant rise in sensitive information like personal data exchanged online. The convenient access to this data has caught the attention of cybercriminals, who have invented a type of cyberattack called phishing. The most crucial difficulty in identifying phishing websites is that attackers always develop sophisticated strategies. Creating phishing websites has become progressively easier, enabling attackers to bypass many protections measures easily. To gain a deeper understanding of this phishing strategy and the techniques used by cybersecurity guys to overcome it, a survey will be conducted about the types of phishing attacks and how it is carried out against online users, besides that we will explore the protection techniques and identify their powers and weaknesses. Finally, some solutions will be proposed to maintain the availability, robustness, and integrity of phishing attacks proposed solutions models.

MSC..

https://doi.org/ 10.29304/jqcsm.2025.17.11972

1. Introduction

Due to the huge size and fast growth of online information, significant challenges arise in providing internet users with the most related and more secure information, depending on their queries. The search engine has become one of the irreplaceable tools for retrieving online information or navigating through a vast digital resource. Current search engines usually bring inaccurate and unsafe search results, such as phishing sites. The ability of search engines to handle complex user queries and retrieve secure sites points is still one of the most challenging problems. The concept of "phishing" was first reported in 1996. The term arises from the word "fishing," exchanging "ph" for "f." Phishing is officially known as an attempt by an unauthorized individual to steal sensitive information like usernames, passwords, or credit card details by mimicking a reliable source in digital communications. Phishing is a notable attack that can significantly affect people's lives. Often, these attacks present themselves as emails or webpages and follow a sequence defined as the bait, the hook, and the catch [1].

While numerous studies have explored phishing detection and prevention techniques, many focus on specific aspects such as machine learning-based detection or user awareness training. However, a comprehensive review that synthesizes various approaches, compares their effectiveness, and highlights recent advancements is still

∗Corresponding author

Email addresses:

Communicated by ‘sub etitor’

lacking. This paper aims to bridge this gap by providing an in-depth overview of phishing attack techniques and evaluating different mitigation strategies, ranging from traditional security measures to modern AI-driven detection methods.

The bait is prepared to catch the user's attention. It usually takes the form of a message that looks like one from a trusted source and contains a clickable link. This bait may seem like appealing deals, critical messages, or alerts about account security problems. When the user clicks on this link, they are redirected to the hook, a webpage similar to a legitimate site from a reliable institution like a bank service provider. This phishing webpage is designed to device the user to steal their data, such as usernames and passwords or credit card information [2]. Phishing can occur through various channels like emails, text messages, instant messaging, and social media. Typically, these messages contain fraudulent links to malicious attachments or fake bogus. When users click and visit these likes or open attachments, they will be taken to the deceptive websites designed by the attacker to appear legitimate. The primary goal of creating these websites is to obtain sensitive information from the user and then use this information for identity theft or financial fraud. Moreover, attackers often use phishing attacks as a main entry point for larger data breach attacks, which can cause significant operational and financial impacts on individuals and organizations. As stated in the 2024 IBM Cost of a Data Breach Report, the average data breach cost rose from USD 4.45 million in 2023 to USD 4.88 million in 2024 (see Fig. 1). These data breach costs involve operational downtime, lost business, and post-breach responses, like regulatory fines and customer support. This increase in the price of data breaches highlights the urgent need to find practical solutions to mitigate phishing attacks, which have become one of the most widespread causes of security incidents [3].

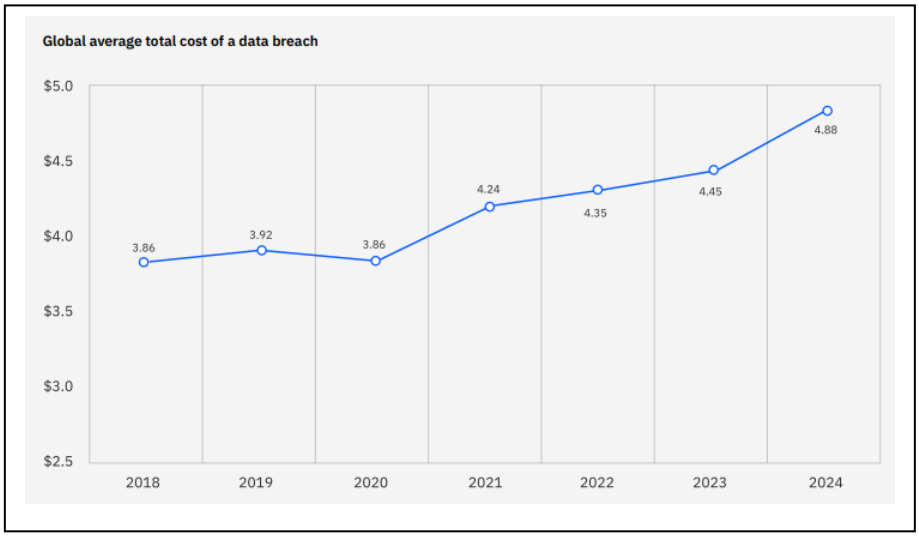

Fig. 1 - Cost of data breach from 2018 to 2024 [3]**.**

The following is a list of this survey's primary contributions:

1. Explore the recent phishing attack techniques that are applied by attackers and their effectiveness in tricking victims.

2. Review the recent studies have been proposed using different strategies to protect internet users against phishing website attacks.

The remainder of this paper is structured as follows: Section 2 discusses various phishing distribution techniques. Section 3 provides a detailed review of existing phishing mitigation strategies, including human-related and software-based approaches. Section 4 presents a review of recent research efforts in phishing detection and prevention. Finally, Section 5 concludes the paper by summarizing key findings and suggesting future research directions.

2. Techniques for Distributing Phishing

Phishing websites apply numerous distribution techniques to increase their reach and effectiveness in tricking potential victims. One standard method of distributing phishing emails is for attackers to pretend to be trustworthy entities, such as banks or government agencies, hiding malicious links or attachments that direct users to malicious websites. These emails often use social engineering techniques to exploit the recipient's trust and urgency. Beyond emails, many techniques are also used to distribute phishing websites, such as text messages, instant messaging platforms, and social media, leveraging their widespread usage and accessibility. Cybercriminals also use search engine poisoning, manipulating search engine rankings to promote malicious websites, often disguising them as legitimate pages. Additionally, attackers utilize compromised websites to hide phishing links or redirect mechanisms to lure unsuspecting users. These methods are increasingly supplemented by automation, where phishing kits and botnets enable the large-scale generation and distribution of phishing sites, increasing the difficulty of detection and mitigation efforts. The evolution variety of these distribution methods underlines the pressing need for advanced detection methods to proactively address the dynamic threat landscape [4]. Fig. 2 presents the different techniques employed by phishers to distribute phishing websites to their targeted users.

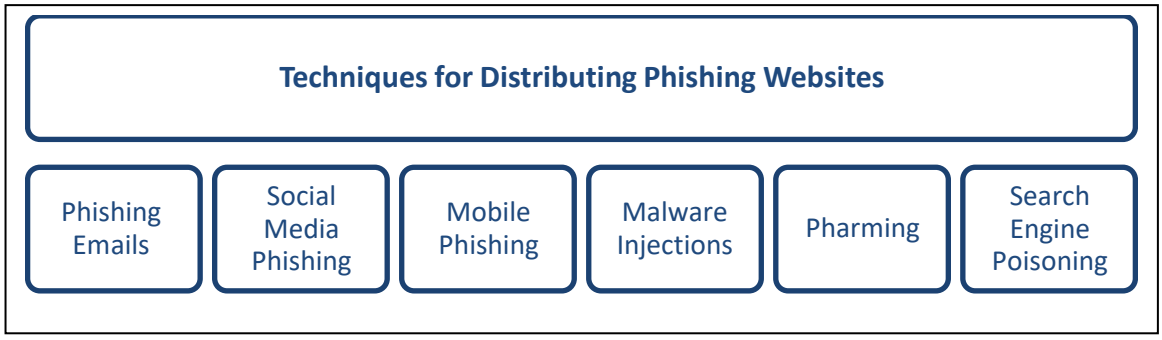

Fig. 2 - Various Techniques Employed by Phishers to Distribute Phishing Websites.

1. **Phishing Emails:** Since the early days of phishing, email-based attacks have remained the most common technique. Phishing emails are crafted to entice users into sharing their personal information using various bait types. Common examples include offers of free goods, services, or vouchers and notifications about account activations needed to maintain access to specific services. These emails are carefully designed to look like they come from legitimate businesses or trusted individuals with whom the recipients have associations. The emails usually contain hyperlinks that direct users to phishing websites created to mimic actual sites. Once users provide their personal information, like financial details, it is captured and sent to phishing email accounts or the servers controlled by the phishers. Phishing email tactics often include sending generic emails to a broad audience. However, attackers have progressively developed more advanced techniques to extend their success rates. These advanced tactics include crafting highly personalized emails, such as spear phishing attacks that target specific individuals and Business Email Compromise (BEC) attacks that exploit organizational vulnerabilities [5].

2. **Social Media Phishing:** Phishers can also use social media platforms to send spam to target users using fake or compromised original accounts. In the case of fake accounts, phishers create new profiles that mimic well-known organizations or individuals. Then, these fake accounts are used to distribute phishing messages to contacts collected through prior malicious activities such as malware or data breaches.

   On the other hand, phishers may obtain unauthorized access to legitimate social media accounts through phishing emails, brute-force attacks, or exploiting weak security measures. Once these accounts are compromised, they can spam the account holder’s contacts and exploit the trust between the original and their network. Phishing messages sent through social media look like traditional phishing emails. They often contain links that take recipients to phishing websites created to steal sensitive information. These messages can be distributed through direct messaging features, like Facebook Messenger, or appear as posts shared from the compromised accounts to increase their reliability. Using social media platforms to target users by exploiting their trust in seemingly legitimate accounts explains the increasing sophistication of phishing strategies [6].

3. **Mobile Phishing:** The swift increase in internet access using mobile devices has given phishers a new golden opportunity to target users through a well-known method known as SMS-based phishing, also called smishing. This SMS-based phishing method is usually carried out by using popular messaging apps like WhatsApp, and these spam messages, similar to phishing emails, often contain malicious links that direct recipients to phishing websites created to steal users' personal information. Research by Lockout [7] Highlights the alarming growth of mobile-targeted phishing. Their findings revealed that the rate at which mobile users receive phishing SMS messages and click on embedded phishing URLs has been increasing at an annual rate of 85%.

   This shift toward mobile-based phishing emphasizes attackers' advanced strategies. They take advantage of mobile devices' everyday use and users' tendency to trust messages received on these personal platforms. The increase in smishing attacks and app-based phishing campaigns reveals the need for stronger mobile security measures and user awareness to combat this rising threat. [5].

4. **Malware Injections:** Software vulnerabilities give phishers a critical entry point to carry out phishing attacks. These vulnerabilities, usually found in web browsers, plug-ins, and other software components, are exploited to install malware that deceives users and redirects them to phishing websites even when they attempt to visit legitimate ones. This technique allows attackers to control web traffic and trick users without awareness.

   In more advanced scenarios, malware can simplify man-in-the-middle (MITM) attacks, where the malicious software intercepts and collects sensitive data exchanged between the user and a legitimate website. Attackers will then use this stolen data for fraudulent purposes. Moreover, some malware can directly scan the infected devices for stored sensitive data, like saved passwords, financial information, login credentials, or payment details, which can then be extracted and misused. Phishers typically separate this malware software through different methods, like Phishing email attachments, web page content injections, or Corrupted file distribution.

   Strong software security practices, such as frequent updates and using trusted antivirus software, must be implemented to overcome these malware threats. Moreover, users must be trained and educated to recognize these phishing tactics and avoid interacting with suspicious files or links to decrease the risk of malware infection tools [8].

5. **Pharming: Pharming**, also known as DNS hijacking or DNS poisoning, is a modern technique that attackers use to redirect users from legitimate web pages to phishing ones. In a pharming attack, the attacker can get unauthorized access to the DNS provider's administrative account or the targeted organization's domain registrar account. This access is usually obtained from compromised credentials, phishing, or utilizing security vulnerabilities. Once the attacker gets inside, he/she can manipulate the DNS records by replacing the legitimate site IP address with the IP address of a malicious phishing site.

   As a result, when visitors try to access a legitimate website, the DNS service unknowingly directs them to the phishing website instead. Fake websites are usually designed to closely mimic legitimate websites to trick visitors into entering sensitive information such as login credentials or financial details. Pharming is dangerous because it does not require the user to interact with suspicious emails or links; it utilizes the infrastructure that directs web traffic. This makes it harder to discover and block without advanced DNS security measures and works for teaching users about potential red flags, like unexpected changes in website appearance or behavior [9].

6. **Search Engine Poisoning:** Search Engine Poisoning (SEP) is a strategy attackers use to control search engine ranking algorithms, ensuring their malicious websites appear in search results for specific keywords. This method utilizes the trust users place in highly ranked search results, making it a powerful tool for directing easily deceived users to phishing websites.

   Attackers execute SEP using different techniques, with one of the most usual techniques including the compromise of legitimate websites that already have a well-built reputation and high rankings on search engines. These compromised websites are injected with hidden keywords inserted by attackers and redirect scripts that lead users to phishing Websites. When users search for these keywords, the compromised websites appear in top positions within the search results. Upon visiting legitimate websites, users are directly taken to phishing pages, where their sensitive information can be stolen [8].

Another common SEP strategy involves embedding the links of the attackers' phishing websites across many compromised, reputable websites. This embedding process creates legitimacy and authority for phishing sites, while search engines suppose the high volume of links from reputable sources marks trustworthiness. As a result, the phishing websites reach higher rankings in search results.

3. Overview of Existing Phishing Mitigation Solution

Many studies have been proposed using different techniques to protect internet users against phishing. This endeavor can generally be classified into two classes: human-based and software-based. The first class focuses on a human to educate them and enhance their skills to recognize and identify suspicious websites. These proposed techniques assist users in making knowledgeable decisions when they face a possible phishing threat.

The second class focuses on developing software to identify and block phishing websites without requiring any action from the user. This software works to differentiate between legitimate and phishing websites and take steps to block malicious sites. Moreover, this software can contact users to help them be aware and make the right decisions when facing a phishing site. Fig. 3 presents the classification framework for these existing solutions.

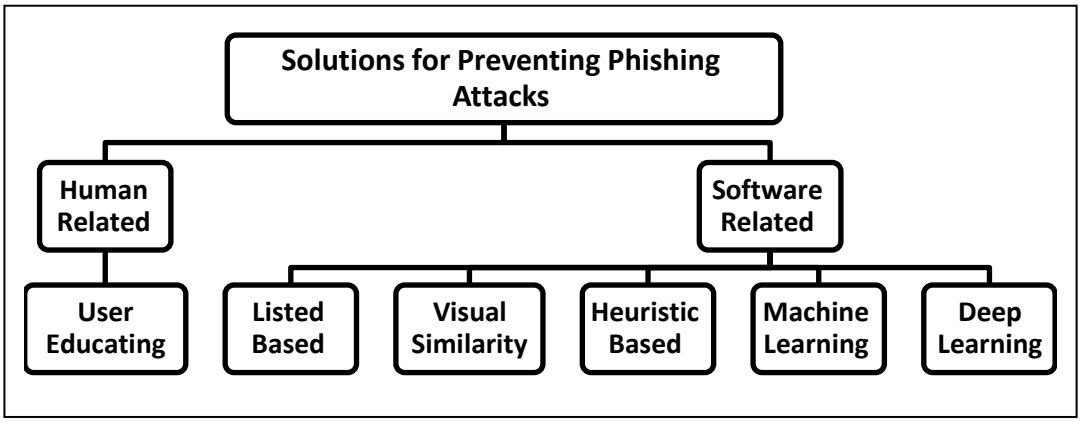

Fig. 3 - Methods to Prevent Phishing Website Attacks.

Table 1 provides an overview of key phishing mitigation techniques, distinguishing between human-based training methods and software-based automated detection strategies. The software-based approaches are further divided into blacklist-based, heuristic-based, visual similarity-based, machine learning-based, and deep learning-based detection, each with unique characteristics.

Approach	Key Features	Advantages	Limitations
Human-Based Approaches	User education, phishing awareness training, simulated phishing exercises	Enhances user awareness, helps recognize phishing attempts	Dependent on user vigilance, not effective against sophisticated attacks
Blacklist-Based Detection	Maintains lists of known phishing sites to block access	Simple, low false positives	Ineffective against zero-day attacks, requires constant updates
Heuristic-Based Detection	Uses predefined rules to identify phishing attempts based on URL structures and content	Detects unknown phishing attempts, works without a blacklist	Higher false positive rate, may misclassify legitimate sites
Visual Similarity-Based Detection	Analyzes website design, logos, and layout to detect phishing attempts	Effective for sites mimicking well-known brands	Computationally expensive, may struggle with minor variations

Machine Learning-Based Detection	Trains models using phishing and legitimate website features	High accuracy, adaptive to new threats	Requires large datasets, prone to adversarial attacks
Deep Learning-Based Detection	Uses neural networks for feature extraction and classification	Highly accurate, can detect complex patterns	Requires extensive computational resources and labeled training data

3.1. Human-Related Approaches

Human-related approaches to stopping phishing attacks emphasize raising awareness, training, and encouraging cautious online behaviors. A most used strategy is to educate users about recognizing phishing attempts by observing suspicious URLs, refining deceptive email headers, and avoiding unwanted requests for sensitive information. Furthermore, simulated phishing exercises and frequent cybersecurity training programs can test and strengthen users' ability to detect phishing websites. Moreover, encouraging multi-factor authentication (MFA) can help mitigate the risks of phishing attacks by adding an extra layer of security. Also, enabling users to report phishing events and keep up with the latest updates on the more recent phishing tactics can enhance protection. These human-centered strategies are crucial for reducing the success of phishing attacks and producing a more alert online community.

Internet users are the main targets of attackers, so educating users is essential to empowering and protecting them against these threats. Despite their frequent internet use, many users still suffer from phishing websites. Therefore, comprehensive educational resources and training programs are needed to help them differentiate between legitimate and phishing web pages to enhance user awareness and boost their ability to recognize phishing sites.

For example, Steve Sheng et al. developed an online game to educate users on recognizing phishing attacks depending on learning science principles. Their results show that the participants who played the game performed better than those who utilized another training program in identifying phishing websites. This strategy of using game-based technology has proved to be highly effective in improving cybersecurity awareness among users [10]. Furthermore, Nalin Asanka et al. developed a mobile game prototype to educate Internet users on identifying phishing attacks. Their results showed that the game notably increased the participants' threat awareness and their behaviors to detect it. This awareness was driven by elements like threat perception, the effectiveness of safeguards, and self-efficacy. These results highlight the effectiveness of games as attractive tools for advancing cybersecurity education [11].

3.2. Software-Based Approach

Software-related approaches to identifying and preventing phishing attacks mainly focus on advanced security applications that recognize and block phishing attacks. For example, Web browsers and security applications often incorporate built-in phishing detection tools that notify users about suspicious websites by comparing them against known blocklists or using machine learning algorithms to examine website attributes. Moreover, anti-phishing toolbars and browser extensions can warn users about possible phishing attacks in real-time. Secure email gateways and spam filters also help to block phishing emails before they reach users' inboxes and reduce the risk of interacting with malicious links. Software-based approaches typically combine with multi-factor authentication (MFA) systems to ensure that even if login information is compromised, the extra layers of verification can help protect sensitive information. This technological software can provide an automated, reactive layer of defense against phishing attacks.

1. **Listed Based-Approach:** The list-based technique can differentiate between legitimate and malicious web pages by keeping a whitelist and a blacklist. The allowlist involves legitimate websites, and the blacklist involves known suspicious or phishing websites. Therefore, when a user wants to access a website, the system checks this website against these lists using a string-matching algorithm. If the website is found on the blacklist, then the access is blocked immediately, and the user is warned of a potential phishing attack. On the other hand, if the website is found in the whitelist, it will be considered legitimate. This dual approach helps keep users safe from phishing attacks by preventing users from accessing phishing websites and ensuring that legitimate web pages remain accessible [4][12].

The list-based approach is widely used in phishing detection, particularly blacklist-based methods, due to their simplicity and low false-positive rate. For example, [4] discusses how blacklists help browsers block malicious URLs, while [12] evaluates their effectiveness in real-world scenarios. However, as noted in [14], blacklist-based detection struggles with zero-day phishing websites, requiring frequent updates. This approach is used in well-known browsers such as Google Chrome, Mozilla Firefox, and Safari, which use services like Google Safe Browsing (GSB) for URL classification. This approach cannot detect zero-day phishing websites or new phishing websites that have not yet been added to the blocklist, leaving users in danger of emerging attacks [13]. Moreover, blacklists must be up-to-date, and human intervention and confirmation consume resources and are prone to error. To overcome these limitations, research tries to integrate the list-based method with other advanced techniques to improve its ability to detect zero-day attacks while keeping its low false-positive rate [14].

2. **Visual Similarity-Based Approach:** Since more than 90% of users rely on a website's visual appearance to assess its legitimacy, attackers often generate phishing websites that neatly imitate the look of legitimate ones [48]. This visual similarity can convince users that the site is trustworthy. As a result, researchers have used visual similarity as a critical feature to distinguish between legitimate and phishing websites [49]. By examining design elements and other visual aspects, researchers aim to develop techniques for effectively detecting phishing sites, even when these phishing web pages are very similar to their legitimate counterparts. For example, Rao and Ali developed a defense technique against zero-day phishing attacks by combining whitelist verification with visual similarity evaluation. Using the SURF detector to extract key features from web pages, this method compares phishing websites with legitimate ones to assess similarity. This method effectively detects phishing attacks, especially recently emerging ones, while minimizing the probability of false positives [15].

   Despite the success of visual similarity-based methods in detecting phishing websites. However, it comes with several limitations. First, most of these methods rely on predefined legitimated assets for legitimate sites, making this approach less effective against zero-day attacks or sites that are not yet recorded. Second, these methods often need high computational resources due to image processing and neural network evaluations, which may slow real-time detection in environments with restricted resources. Therefore, visual similarity methods can be more effective if combined with other detection methods to enhance robustness and efficiency.

3. **Heuristic-Based Approach:** Researchers have developed sophisticated techniques to analyze the structural and content features of URLs and webpages content to overcome the limitations of traditional list-based techniques in identifying zero-day phishing attacks. These techniques were called heuristic-based phishing detection methods that extract distinct patterns and features from URLs and webpage contents. These features are often manually prepared and fed into classifiers to build effective detection models. Heuristic-based methods can more comprehensively differentiate between fake and legitimate sites by examining and assessing these features. This approach enhances the classification process by analyzing and identifying the suspicious URL patterns and comparing them to known phishing and legitimate features, thus addressing the limitations presented in the list-based methods [16]. For example, Ma et al. developed an automated URL classification method that recognizes phishing websites using statistical analysis of lexical and host-based features. Their system collects a set of features from URLs to build predictive models that can distinguish phishing URLs from legitimate ones. The method reaches 95% to 99% accuracy, offering a reliable solution for recognizing phishing websites based on URL analysis [17].

   Heuristic methods provide a higher generalization ability and allow the detection of new phishing attacks that may not be registered in current blacklists. However, their effectiveness is restricted to common threats and may suffer to recognize newly developed phishing strategies. Moreover, heuristic-based methods tend to have a higher false-positive rate than blacklist methods, which leads to marking legitimate websites as phishing. So, heuristic methods are usually integrated with other detection methods to alleviate this limitation and provide a more stable and reliable solution to reduce false positives while preserving detection accuracy.

4. **Machine Learning-Based Approach:** Machine learning (ML) has become a highly successful phishing detection method thanks to its ability to recognize complex patterns and find correlations within data. ML algorithms operate in two main stages: the learning stage, where the ML model learns from a labeled example, and the testing stage, where the model accuracy is evaluated. The success of these methods mainly

depends on the features extracted and the classification method employed. Standard ML techniques used for phishing detection include Naïve Bayes (NB), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), k-nearest Neighbor (kNN), and others [18][19][20]. These techniques show distinct advantages compare to blacklisting and heuristic methods. ML-based systems can recognize new phishing attacks, adapt quickly to the latest phishing strategies, and reach this with a lower false-positive rate. For example, Xiang et al. developed CANTINA+, an ML anti-phishing system that combines 15 features from different sources, such as the HTM model. The system was designed to minimize false positives by implementing a near-duplicate phishing detector and a login form classifier. CANTINA+ reached more than 92% accurate favorable rates for unique phishing pages and a low false positive rate of 0.4%. These results demonstrate the system's success despite dataset bias and privacy limitations [21].

Even though machine learning-based approaches result in high accuracy and improved performance, they are not without limitations; the ML models are highly affected by the quality of the database used and the feature selection process. For example, while ML operates efficiently on the client side, hyperlink-based models may suffer from dynamically obfuscated links or content generated. Also, algorithms that use handcrafted features can face challenges in discovering innovative phishing or zero-day attacks. Finally, these models may require highly computational resources for feature extraction and training, and that can limit its scalability in real-time applications.

5. **Deep Learning-Based Approach:** Deep learning (DL) techniques have gained popularity in phishing detection because they can handle complex data and automatically extract features without earlier knowledge [22]. DL relies on neural network architectures that discover hidden patterns in data from hierarchical learning. In phishing detection, DL techniques convert the input URLs into a matrix representation, where each row represents a character encoded and converted into numerical values. While DL methods require larger datasets and a longer training time compared to ML algorithms, their ability to extract features directly from raw data and adapt to complex patterns makes them valuable methods in the fight against phishing attacks [16].

   Recently, numerous deep learning (DL)-based methods were used to improve classification performance in phishing detection and frequently used DL architectures used are: Convolutional Neural Networks (CNNs) [16][23], Deep Neural Networks (DNNs) [24][25], Recurrent Neural Networks (RNNs) [26][27], Long Short-Term Memory (LSTM) networks [25][27], Gated Recurrent Units (GRUs) [28][29], and Multi-Layer Perceptrons (MLPs) [30], among others.

   Despite the high accuracy achieved by DL methods in detecting phishing attacks, this is without limitations. For example, Most DL models typically require massive labeled datasets for successful training, which may not always be reachable. Moreover, these models require unusual computational resources and much training time compared to traditional machine-learning methods. In addition, DL methods can face challenges with interpretability that make it very difficult to explain the reasoning behind classification decisions. Finally, the effectiveness of these models may decrease when they face unseen data or highly disguised phishing patterns, highlighting the need for continual updates and model retraining to adapt to evolving attacks.

4. The Current Related Work to Overcome Phishing Attacks

This section explores and reviews recent research efforts in web security and phishing detection techniques. The selected research papers involved many methods and algorithms that aimed to enhance the accuracy and reliability of phishing detection, such as deep learning, machine learning, human awareness initiatives, and visual similarity detection methods. This review provides an essential background for positioning our proposed system with the current approach and also highlights the current methods strengths and limitations.

1. In 2025, Doe, Do et al. [31] By efficient analysis of URL formats throughout integrating the character-level and word-level embeddings to improve the features selection process and also use a Multi-Head Self-Attention (MHSA) and Temporal Convolutional Networks (TCN) to solve the defect of Recurrent Neural Networks (RNNs) and conventional Convolutional Neural Networks (CNNs) authors were developed a phishing detection system to classify the URL as a phishing or legitimate URLs. By utilizing MHSA, the proposed system improved its attention on the essential features, which helped the model reach an outstanding accuracy of 98.78%. On the other hand, the results indicated that the introduced TCN method in the system provided an efficient solution that enhanced the system's ability to detect phishing attacks.

The study's main limitation is its potentially missing content-based phishing tactics and only focusing on URL structure. Moreover, this system may require highly computational resources due to MHSA.

2. In 2024, Sarker et al. [32], Incorporating insights from 69 research papers, this study revealed 20 challenges and 23 success factors. It thoroughly examines the obstacles and key factors critical to the successful design, implementation, and evaluation of phishing education, training, and awareness (PETA) initiatives. It focuses on addressing the gaps in knowledge by using tailored approaches and creating explainable anti-phishing techniques. As well as to overcome the challenges and improve the PETA performance, the study provides practical advice throughout, connecting the challenges with their related success factors. In addition, it helps to build real-world research and automated tools to pass over the gap between theory and practice. This awareness provides an efficient plan for organizations to build up a strong firewall against phishing attacks and empower the user with great knowledge to identify and avoid potential risks.

3. In 2024, Li et al. [33] In this study, the authors highlighted the importance of user education to help users differentiate between legitimate and phishing sites. The results prove that the education strategy represents a fundamental part of any successful phishing prevention system and significantly decreases the possibility of successful phishing attacks. However, the main limitation of this approach is that even when users are educated, not every user retains or applies their knowledge, and recent phishing techniques can still deceive users. Therefore, promoting the education factor with sophisticated technical measures such as automated detection systems and immediate alerts is essential to provide users with a strong defense against phishing attacks.

4. In 2023, Adebowale et al. [34] Developed an Intelligent Phishing Detection System (IPDS). By incorporating features from webpages content such as text, images, or frames and URLs, the proposed system is developed by combining the Convolutional Neural Networks (CNN) and Recurrent Nural Network (RNN) networks to enhance the system's accuracy in identifying the phishing site. It achieved an outstanding accuracy rate of 93.28% with an average detection time of only 25 seconds when trained on a large dataset featuring one million URLs and over 10,000 images. The application of the CNN model for feature extractions and RNN to identify the temporal pattern on a large data set gives a great performance and enhances the classification. However, the dependence on the large dataset is the main limitation of this approach in terms of scalability and real-time implementation in resource-limited settings.

5. In 2022, Mughaid et al. [35] Proposed a machine learning model to reduce the threats of phishing attacks and their impact on governments, organizations, and individuals. The proposed model's results demonstrated the effectiveness of this approach by reaching a reasonable accuracy rate of 0.97 for a boosted decision tree over multiple datasets. This study highlights the importance of user awareness, in addition to the state-of-the-art machine learning model and an adequate data set sample to detect phishing attacks effectively. However, although the boosted decision tree yields higher performance than others, the proposed model did not consider the scalability of the model when applied to real-time scenarios with dynamic data.

6. In 2021, Lin et al. [36] Developed the Phishpedia model by using the Siamese Neural Network. The Phishpedia was designed to resolve the accuracy and computational efficiency problem in detecting visual-based phishing. The model showed high accuracy when comparing webpage images to detect phishing sites with their targeted brands. The Phishpedia model was evaluated on a six-month collected dataset from the OpenPhish site. The results showed the model successfully detected 1,704 phishing sites within 30 days. However, the main drawback of the Phishpedia model is its complete dependency on visual similarity, and this approach could have a high false positive rate when the phishing website uses obfuscation methods or generates dynamic content.

7. In 2020, Rao et al. [37] Used handcrafted and TF-IDF-based features to Introduce a model called CatchPhish for detecting phishing sites by looking at their URLs without needing to visit the entire website. By collecting a data set from different resources, such as OpenPhish for phishing samples and Alexa for legitimate samples, the model trained and reached an accuracy of 94.26% using the RF algorithm. On the other hand, the model also trained on the benchmark datasets and reached a high accuracy score of 98.25% and an F1-score of 98.23%, which overcame baseline results. However, depending on the handcrafted features are considered the main limitation of the CatchPhish model because of these features may not

apply to new phishing techniques or unique attack strategies. Moreover, depending on the specific dataset limits the model's applicability in real-time situations.

8. In 2020, Aljofey et al [16] By relying on URL character-level and convolutional neural networks (CNN), the authors proposed an efficient deep-learning model to detect phishing sites. The proposed model overcomes the limitations of machine learning algorithms that use handcrafted features by directly capturing sequential patterns from URL strings. By comparing the performance of the proposed model with the sets of traditional machine learning algorithms, the results demonstrated the remarkable performance of the proposed model by reaching a high accuracy of 95.02% on its dataset and exceeding 95% on several benchmark datasets, overcoming existing methods for detecting phishing URLs. However, the limitations of the deep learning model lie in applying the model in real-time environments with limited resources.

9. In 2019, Jain & Gupta [38] Trained several machine learning algorithms such as Logistic Regression (LR), Random Forest (RF), and Support Vector Machines (SVM) to introduce an innovative client-side model that examines URL contents to detect phishing attacks. There are 12 URLS features extracted, such as internal and external links, CSS references, redirect links, errors, links to login forms, and favicons to train the models. All these features were extracted from the phishing dataset collected from PhishTank and the legitimate dataset collected from different resources like Alexa, Stuffgate, and online payment services. The results showed the effectiveness of the Logistic Regression model, where it achieves a valid positive rate of 98.39%, an actual negative rate of 98.48%, and an overall accuracy of 98.42%. However, the limitation is the difficulties in recognizing phishing sites that use sophisticated obfuscation techniques because the model depends only on the web page URL-specific features that could be potentially altered or not preserve typical URL structures.

10. In 2019, Yi et al. [39] Developed a deep learning model, specifically the Deep Belief Network (DBN), to identify phishing websites. Different features are used to train the models, such as the number of special characters in URLs, the domain's age, website interaction metrics, and the in-degree and out-degree of URLs. The proposed model was first trained on a smaller dataset to fine-tune its detection parameters. After that, it was tested on a larger dataset. The results showed that an actual positive rate was close to 90% and a false positive rate of merely 0.6%. These results highlighted the promising performance of deep learning algorithms in detecting phishing attacks by extracting phishing sites' structural and behavioral features. However, applying such models in real-time may affect scalability because such models may lead to increased training times and greater computational demands.

11. In 2018, Le et al. [40] Proposed URLNet model by utilizing Convolutional Neural Networks (CNNs) and examining the characters and words in URL strings to identify the phishing site. In contrast to the machine learning techniques that depend on handcrafted features, URLNet utilizes convolutional neural networks (CNNs) to grasp URLs' semantic and sequential patterns automatically. In addition, it incorporates advanced word embedding methods to address the issue of infrequent words typically found in phishing URL detection tasks. The experiments conducted on large datasets have shown an excellent performance of the proposed model compared to existing approaches, demonstrating the proposed model's effectiveness in generalization and capturing a wide range of semantic information within URL structure. However, the main limitation of URLNet lies in its dependence on the extensive data set to train the model, which may not always be accessible for specific phishing domains, potentially limiting its usefulness in specialized areas.

Table 1 - Summary Current Related Work to Overcome Phishing Attacks.

Publication (Authors, Year)	Contribution	Limitation
Doe et al., 2025 [31]	Introduced a framework for phishing detection combining TCN and MHSA to enhance URL classification	Focused only on URL structure, missed content-based phishing tactics; computationally expensive due to MHSA.
Sarker et al., 2024 [32]	Explored challenges and success factors in phishing education, training, and awareness (PETA) initiatives	Lacked practical evaluation of proposed recommendations

Li et al., 2024 [33]	Emphasized the role of user education in preventing phishing	Education alone is inadequate and needs technical measures as well
Adebowale et al., 2023 [34]	Developed an Intelligent Phishing Detection System (IPDS) for improved detection accuracy using hybrid features	It relies on large datasets that may not be scalable for real-time applications.
Mughaid et al., 2022 [35]	Proposed machine learning model for phishing detection using email text and features	Limited generalizability due to dataset reliance did not evaluate scalability.
Lin et al., 2021 [36]	The Phishpedia model detects phishing sites by comparing webpage images	Dependent on visual similarity; ineffective with obfuscated or dynamic content
Rao et al., 2020 [37]	Developed CatchPhish to classify phishing URLs using feature extraction and machine learning classifiers	Static datasets may not adapt to new phishing techniques and may rely on handcrafted features.
Aljofey et al., 2020 [16]	Proposed deep learning model for phishing detection based on sequential URL patterns	Relies on benchmark datasets, may struggle with new phishing patterns or dynamic content
Jain & Gupta, 2019 [38]	Proposed client-side detection model analyzing hyperlinks in the HTML source code	It is challenging to detect phishing sites with obfuscation or non-standard structures.
Yi et al., 2019 [39]	Proposed framework using DBN with structural and behavioral features for phishing detection	A small initial dataset could limit effectiveness; DBN's complexity demands extended training times.
Le et al., 2018 [40]	Developed URLNet, a CNN-based framework for detecting malicious URLs	Relies on large datasets; computationally expensive for real-time detection

4. Conclusion

Phishing causes significant threats to both individuals and organizations, leading to serious financial, reputational, and operational consequences. For organizations, phishing attacks can lead to unauthorized access to confidential information, economic losses, and interruptions of operations. Major data breaches often originate from successful phishing attempts, putting companies under regulatory penalties and diminishing customer trust. Phishing can also affect organizational work efficiency, as organizations must invest resources and money to recover from attacks and enhance their security protocols. Individually, phishing attacks can cause financial scams and emotional strain when personal information like banking credentials and social security numbers is stolen. These organizations or individuals may suffer from these attacks, such as damage to credit scores or legal issues. This paper provides a comprehensive survey of phishing attacks, their distribution techniques, and various mitigation strategies. We reviewed and categorized existing solutions into human-based and software-based approaches, offering a comparative analysis of their strengths and limitations. Additionally, we introduced a classification framework that organizes phishing detection methods into heuristic-based, machine learning-based, and deep learning-based approaches.

Our findings highlight that while human-based approaches enhance awareness, they are not sufficient alone, whereas software-based methods, particularly AI-driven detection, offer higher accuracy but require ongoing adaptation. These insights can help organizations and cybersecurity professionals choose the most effective anti-phishing strategies tailored to their needs. This study addressed the research gap identified in the introduction by

providing a structured and comparative analysis of phishing mitigation techniques. Unlike previous surveys that focused on isolated aspects, our work offers a holistic perspective by combining detection strategies, evaluation of recent advancements, and discussion of ongoing challenges.

5. Future works

Despite advancements in phishing detection, several challenges remain unaddressed. One promising direction is the development of explainable AI (XAI) techniques, ensuring that machine learning models provide transparent reasoning behind phishing classification decisions. Additionally, emerging threats such as advanced spear phishing require adaptive defenses capable of detecting highly personalized attacks. Another crucial area is cross-platform and cross-lingual phishing detection, as phishing attacks are now targeting users across multiple devices, languages, and communication platforms. Future research should focus on integrating these advancements into robust, real-time phishing detection systems to ensure better protection against evolving threats.

Acknowledgements

The authors thank the reviewers for their time and effort reviewing this paper.

References

[1] V. Bharath, H. L. Gururaj, B. C. Soundarya, and L. Girish, “Introduction to Social Engineering: The Human Element of Hacking,” in Social Engineering in Cybersecurity, CRC Press, 2024, pp. 1–25.
[2] S. Kavya and D. Sumathi, “Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection,” Artif Intell Rev, vol. 58, no. 2, p. 50, 2024.
[3] IBM, “Cost of a Data Breach,” 2024. Accessed: Jan. 10, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach
[4] A. S. O. K. E. H.-V. A. H. F. NGUYET QUANG DO, “Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions,” 2022.
[5] P. H. Kyaw, J. Gutierrez, and A. Ghobakhlou, “A Systematic Review of Deep Learning Techniques for Phishing Email Detection,” Electronics (Basel), vol. 13, no. 19, p. 3823, 2024.
[6] R. K. Ayeni, A. A. Adebiyi, J. O. Okesola, and E. Igbekele, “Phishing Attacks and Detection Techniques: A Systematic Review,” in 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), IEEE, 2024, pp. 1–17.
[7] Lookout, “The Global State of Mobile Phishing,” 2022. Accessed: Jan. 15, 2025. [Online]. Available: https://www.lookout.com/documents/reports/Global-State-of-Mobile-Phishing-Report.pdf
[8] E. Yuvarani and P. M. Gomathi, “Security issues on Forensics Applications by Dynamic Malware injection–A Review,” in 2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, 2024, pp. 573–579.
[9] F. M. Teichmann and S. R. Boticiu, “Phishing attacks: risks and challenges for law firms,” International Cybersecurity Law Review, pp. 1–8, 2024.
[10] S. Sheng et al., “Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish,” in Proceedings of the 3rd symposium on Usable privacy and security, 2007, pp. 88–99.
[11] N. A. G. Arachchilage, S. Love, and K. Beznosov, “Phishing threat avoidance behaviour: An empirical investigation,” Comput Human Behav, vol. 60, pp. 185–197, 2016.
[12] A. Kulkarni, V. Balachandran, and T. Das, “Phishing Webpage Detection: Unveiling the Threat Landscape and Investigating Detection Techniques,” IEEE Communications Surveys & Tutorials, 2024.
[13] A. Oest, Y. Safaei, A. Doupé, G.-J. Ahn, B. Wardman, and K. Tyers, “Phishfarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists,” in 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 1344–1361.
[14] I. Skula and M. Kvet, “Domain blacklist efficacy for phishing web-page detection over an extended time period,” in 2023 33rd Conference of Open Innovations Association (FRUCT), IEEE, 2023, pp. 257–263.
[15] R. S. Rao and S. T. Ali, “A computer vision technique to detect phishing attacks,” in 2015 Fifth International Conference on Communication Systems and Network Technologies, IEEE, 2015, pp. 596–601.
[16] A. Aljofey, Q. Jiang, Q. Qu, M. Huang, and J.-P. Niyigena, “An effective phishing detection model based on character level convolutional neural network from URL,” Electronics (Basel), vol. 9, no. 9, p. 1514, 2020.
[17] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, “Beyond blacklists: learning to detect malicious web sites from suspicious URLs,” in Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining, 2009, pp. 1245–1254.
[18] A. K. Jain and B. B. Gupta, “PHISH-SAFE: URL features-based phishing detection system using machine learning,” in Cyber Security: Proceedings of CSI 2015, Springer, 2018, pp. 467–474.
[19] J. Kumar, A. Santhanavijayan, B. Janet, B. Rajendran, and B. S. Bindhumadhava, “Phishing website classification and detection using machine learning,” in 2020 international conference on computer communication and informatics (ICCCI), IEEE, 2020, pp. 1–6.
[20] Y. Sonmez, T. Tuncer, H. Gokal, and E. Avci, “Phishing web sites features classification based on extreme learning machine,” in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018, pp. 1–5.
[21] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, “Cantina+ a feature-rich machine learning framework for detecting phishing web sites,” ACM Transactions on Information and System Security (TISSEC), vol. 14, no. 2, pp. 1–28, 2011.
[22] A. Odeh, I. Keshta, and E. Abdelfattah, “Machine learningtechniquesfor detection of website phishing: A review for promises and challenges,” in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2021, pp. 813–818.
[23] N. Al-Milli and B. H. Hammo, “A convolutional neural network model to detect illegitimate URLs,” in 2020 11th International Conference on Information and Communication Systems (ICICS), IEEE, 2020, pp. 220–225.
[24] S. Mahdavifar and A. A. Ghorbani, “DeNNeS: deep embedded neural network expert system for detecting cyber attacks,” Neural Comput Appl, vol. 32, no. 18, pp. 14753–14780, 2020.
[25] M. Somesha, A. R. Pais, R. S. Rao, and V. S. Rathour, “Efficient deep learning techniques for the detection of phishing websites,” Sādhanā, vol. 45, pp. 1–18, 2020.

[26] Y. Huang, Q. Yang, J. Qin, and W. Wen, "Phishing URL detection via CNN and attention-based hierarchical RNN," in 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, 2019, pp. 112–119.
[27] H. Wang, L. Yu, S. Tian, Y. Peng, and X. Pei, "Bidirectional LSTM Malicious webpages detection algorithm based on convolutional neural network and independent recurrent neural network," Applied Intelligence, vol. 49, pp. 3016–3026, 2019.
[28] T. Feng and C. Yue, "Visualizing and interpreting rnn models in url-based phishing detection," in Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, 2020, pp. 13–24.
[29] L. Yuan, Z. Zeng, Y. Lu, X. Ou, and T. Feng, "A character-level BiGRU-attention for phishing classification," in Information and Communications Security: 21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers 21, Springer, 2020, pp. 746–762.
[30] S. Al-Ahmadi, "PDMLP: phishing detection using multilayer perceptron," International Journal of Network Security & Its Applications (IJNSA) Vol, vol. 12, 2020.
[31] N. Q. Do, A. Selamat, O. Krejcar, and H. Fujita, "Detection of malicious URLs using Temporal Convolutional Network and Multi-Head Self-Attention mechanism," Appl Soft Comput, vol. 169, p. 112540, 2025.
[32] O. Sarker, A. Jayatilaka, S. Haggag, C. Liu, and M. A. Babar, "A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness," Journal of Systems and Software, vol. 208, p. 111899, 2024.
[33] D. Li, Q. Chen, and L. Wang, "Phishing Attacks: Detection and Prevention Techniques," Journal of Industrial Engineering and Applied Science, vol. 2, no. 4, pp. 48–53, 2024.
[34] M. A. Adebowale, K. T. Lwin, and M. A. Hossain, "Intelligent phishing detection scheme using deep learning algorithms," Journal of Enterprise Information Management, vol. 36, no. 3, pp. 747–766, 2023.
[35] A. Mughaid, S. AlZu'bi, A. Hnaif, S. Taamneh, A. Alnajjar, and E. A. Elsoud, "An intelligent cyber security phishing detection system using deep learning techniques," Cluster Comput, vol. 25, no. 6, pp. 3819–3828, 2022.
[36] Y. Lin et al., "Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages," in 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 3793–3810.
[37] R. S. Rao, T. Vaishnavi, and A. R. Pais, "CatchPhish: detection of phishing websites by inspecting URLs," J Ambient Intell Humaniz Comput, vol. 11, pp. 813–825, 2020.
[38] A. K. Jain and B. B. Gupta, "A machine learning based approach for phishing detection using hyperlinks information," J Ambient Intell Humaniz Comput, vol. 10, pp. 2015–2028, 2019.
[39] P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, and T. Zhu, "Web phishing detection using a deep learning framework," Wirel Commun Mob Comput, vol. 2018, no. 1, p. 4678746, 2018.
[40] H. Le, Q. Pham, D. Sahoo, and S. C. Hoi, "URLNet: Learning a URL representation with deep learning for malicious URL detection. arXiv 2018," arXiv preprint arXiv:1802.03162, 2018.