IRAQI Academic Scientific Journals

العـــــراقيـة
المجلات الأكاديمية العلمية

University of Kut Journal

ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419

www.kutcollegejournal.alkutcollege.edu.iq

k.u.c.j.sci@alkutcollege.edu.iq

Vol. 10 , Issue 2 , December 2025

A Survey of Enhancements for Robust Phishing Detection Systems

Muntadher Mohammed Kareem [1] , Rawaa Ismael Farhan [2]

Abstract

What we hear most often in cybersecurity is phishing, especially at a time when social media has become widespread among all members of society. Due to its impact and risks, caused by the limited knowledge of social media users and Internet users, who make them potential victims, phishing remains a significant concern. Researchers are striving to find appropriate solutions to this serious threat. Phishing has become increasingly sophisticated over time, attracting many cybersecurity specialists to investigate its causes, limit its impact, and uncover its tools. This is because attackers use fraudulent methods to deceive users and steal their information. This paper examines different forms of deceptive tactics and addresses techniques for detecting and combating them. The objectives include describing the different phishing attack forms, explaining how attackers exploit or lure users, and showing different detection strategies to thwart phishing attempts. The main objectives include increasing awareness of phishing tactics, educating individuals about them, supplementing preventative measures against phishing, and supplementing discussion within professional circles. By adopting a systematic approach, reviews related studies and recent advanced academic publications on phishing, its attacks, and detection.

Keywords: phishing detection, deep learning, machine learning, cyber-attacks

Affiliations of Authors

[1, 2] College of Education for Pure Science, Wasit University, Iraq، Kut, 52001

[1]std.2024205.m.kareem@uowasit.edu.iq
[2] ralrikabi@uowasit.edu.iq

[1] **Corresponding Author**

Paper Info.
Published: Dec. 2025

استطلاع التحسينات حول انظمة كشف التصيد الاحتيالي القوية

منتظر محمد كريم [1] ، رواء إسماعيل فرحان [2]

المستخلص

ما نسمعه غالبًا في مجال الأمن السيبراني هو التصيد الاحتيالي (Phishing)، خاصة في وقت أصبحت فيه وسائل التواصل الاجتماعي منتشرة بين جميع أفراد المجتمع. ونظرًا لتأثيره ومخاطره الناتجة عن محدودية معرفة مستخدمي وسائل التواصل الاجتماعي والإنترنت، مما يجعلهم ضحايا محتملين، يبقى التصيد الاحتيالي مصدر قلق كبير. يسعى الباحثون لإيجاد حلول مناسبة لهذا التهديد الخطير. لقد أصبح التصيد الاحتيالي أكثر تطورًا مع مرور الوقت، مما جذب العديد من المختصين في الأمن السيبراني لدراسة أسبابه، والحد من تأثيره، وكشف أدواته، وذلك لأن المهاجمين يستخدمون أساليب احتيالية لخداع المستخدمين وسرقة معلوماتهم. تتناول هذه الورقة البحثية أشكال الخداع المختلفة وتناقش التقنيات المستخدمة لاكتشافها ومكافحتها. وتشمل الأهداف وصف أشكال هجمات التصيد الاحتيالي المختلفة، وشرح كيفية استغلال المهاجمين للمستخدمين أو استدراجهم، وعرض استراتيجيات الكشف المختلفة لإحباط محاولات التصيد. تشمل الأهداف الرئيسية زيادة الوعي بأساليب التصيد الاحتيالي، وتثقيف الأفراد بشأنها، وتعزيز الإجراءات الوقائية ضده، وإثراء النقاش داخل الأوساط المهنية. ومن خلال اتباع منهج منظم، تراجع هذه الدراسة الأبحاث ذات الصلة والمنشورات الأكاديمية الحديثة حول التصيد الاحتيالي وهجماته وأساليب اكتشافه.

الكلمات المفتاحية: كشف التصيد الاحتيالي، التعلم العميق، التعلم الآلي، الهجمات السيبرانية

انتساب الباحثين

[1] كلية التربية للعلوم الصرفة ، جامعة واسط ، العراق، الكوت، 52001

[1]std.2024205.m.kareem@uowasit.edu.iq
[2] ralrikabi@uowasit.edu.iq

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر: كانون الاول 2025

1. Introduction

In light of the spread of serious cybercrimes represented by phishing, which uses methods to deceive institutions or individuals, and through social engineering methods that exploit the user's trust and curiosity, this has led to the discovery and development of advanced adaptive technologies to detect phishing attempts [1]. Today, web applications have become important in social communication, banking services, government activities, passwords, and bank accounts [2]. Here, the importance of developing traditional methods and collaboration among researchers to create strategies adaptable to changing threats becomes evident, ensuring the effectiveness of detection systems in a rapidly changing digital environment [3]. In recent years, the use of machine learning and artificial intelligence techniques has played a role in detecting various types of phishing, employing classification and clustering methods in deep learning. This has led to the emergence of more effective and intelligent methods to handle the nature of the data [4]. One of these algorithms is Fuzzy C-Means. Recent literature (2018-2025) shows that most research has focused on using traditional algorithms such as SVM and Random Forest, while recent studies that have combined Fuzzy C-Means with modern techniques like deep learning or hybrid models are very limited. Consequently, there remains a research gap in exploring the capability of Fuzzy C-Means when integrated with other techniques to improve phishing detection accuracy [5]. Some studies indicate that clustering algorithms, including Fuzzy C-Means, have shown promising preliminary results in classifying URLs. The FCM algorithm focuses on finding suitable fuzzy groups (fuzzy C-group) for data sets, which helps mitigate errors resulting from traditional classification methods [6]. In our Arab region and in Iraq, there has recently been a reliance on electronic services via the internet, as well as banking transactions. The increase in economic growth in any country is a factor that attracts phishing, especially targeted phishing. This makes the user more susceptible to phishing and its attacks, and hence the necessity to address this issue through studies that focus on local data [7]. only Traditional security measures are insufficient because attacks exploit human vulnerabilities, as they surpass technical defenses. Therefore, adopting a multi-faceted approach works to raise user awareness [3]. Comprehensive studies related to phishing techniques can help develop strong security protocols and contribute to the strategic development of phishing methods and their mitigation [8]. This study aims to provide in-depth and comprehensive insights into the different types of phishing and the potential methods for detecting them. The research paper is organized as follows: Section Two addresses the various forms of attacks and reviews the components and techniques of phishing. Section three: It explains the detection techniques in phishing. Section Four: Reviews the latest contemporary articles and literature related to phishing and methods for detecting it. Section Five: Summarizes the results extracted from similar works and their outcomes. Section Six: It presents the conclusions drawn and suggests future research that can be pursued.

2. Phishing Components

The three main components of a phishing tactic are the phishing medium, the attack vectors for transmission, and the technological methodologies used to carry out the attack. The various parts are closely interconnected, as certain vectors are suitable for particular platforms, while specific technical tactics are solely applicable to designated assault channels. The research includes related work, followed by a comprehensive study of phishing attack techniques and their traditional, modern, and highly advanced characteristics. The objective of this research is to enhance awareness regarding phishing techniques. [9][10].

A. Phishing media

Social networks are considered the primary means of phishing due to the ease of communication between the victim and the scammer. And the types of this fraud are text messages, emails, calls, and the internet. The Facebook site contains sub-features that include traditional phishing methods, phishing methods through surveys, phishing features by sending fake security messages to users, and phishing features through fake trusted messages. These tools primarily use the same methods to collect user information, but the goal of this feature is to develop diverse attack strategies to increase the effectiveness of phishing attacks and minimize the failure rate to the lowest possible level [11]. Voice communications, which are a fundamental human means of interaction, are vulnerable to exploitation by fraudsters who seek to deceive individuals into revealing their personal information. Similarly, the Short Message Service (SMS) enables scammers to communicate with victims by sending brief text messages via mobile phone networks. With its evolution into Multimedia Messaging Service (MMS), communication methods have expanded. The Internet has continuously developed, starting from its origins as the Advanced Research Projects Agency Network (ARPANET) to the wide variety of websites and platforms currently available. This evolution provides fraudsters with many channels of interaction, from email to social media platforms such as Instagram and Snapchat. The dynamic nature of the Internet constantly introduces new communication methods, offering scammers effective opportunities to target potential victims [12].

B. Phishing Attack Vectors

The choice of method is determined by the means used by the attacker, as this means constitutes the channel or starting point from which the phishing attack begins. Below, we will briefly present the main methods of these attacks.

E-mail: Email phishing represents a prevalent cyber hazard that may result in the appropriation of confidential information and monetary damages. Phishing employs fraudulent emails intended to mislead recipients into disclosing confidential information or transferring funds, with perpetrators frequently masquerading as authentic entities or individuals [13]. As reported by the Anti-Phishing Working Group (APWG), the APWG's Q2 2025 report shows a continuous rise in phishing attacks and Business Email Compromise (BEC). In Q2 2025, the APWG recorded 1,130,393 phishing attacks, a 13% increase from Q1 2025, which had 1,003,924 attacks. The most targeted sectors include Financial Institutions, which account for 18.3% of all attacks, followed by Webmail/SaaS services at 18.2%. According to this report, the total number of phishing attacks observed in 2025 up to the end of Q2 is: 1,003,924 (Q1) + 1,130,393 (Q2) = 2,134,317 attacks [14]. Due to the significant rise in phishing emails, numerous researchers have commenced the development of anti-phishing strategies to mitigate such actions. This study intended to discover the optimal set of features from 41 existing features, along with additional new features. This method employed a feature ranking algorithm to prioritize the features and integrated it with a feature search algorithm to identify the ideal feature set [15].

EFAX: eFax operates in a manner akin to traditional faxing, although it removes the necessity for a real fax machine. eFax is similar to a conventional fax, but it does not require a physical fax machine. Sites such as efax.com utilize IP (Internet Protocol) to transmit faxes, in comparison with traditional methods that utilized phone lines. The advantage of this method is that faxes can be sent to a recipient's machine. As emails, thus removing the need for a fax machine. However, due to the online nature of this method of communication, this provides an entirely novel opportunity for phishing attacks to obtain victims' personal information. Victims' personal information [16]. As shown in Figure (1).

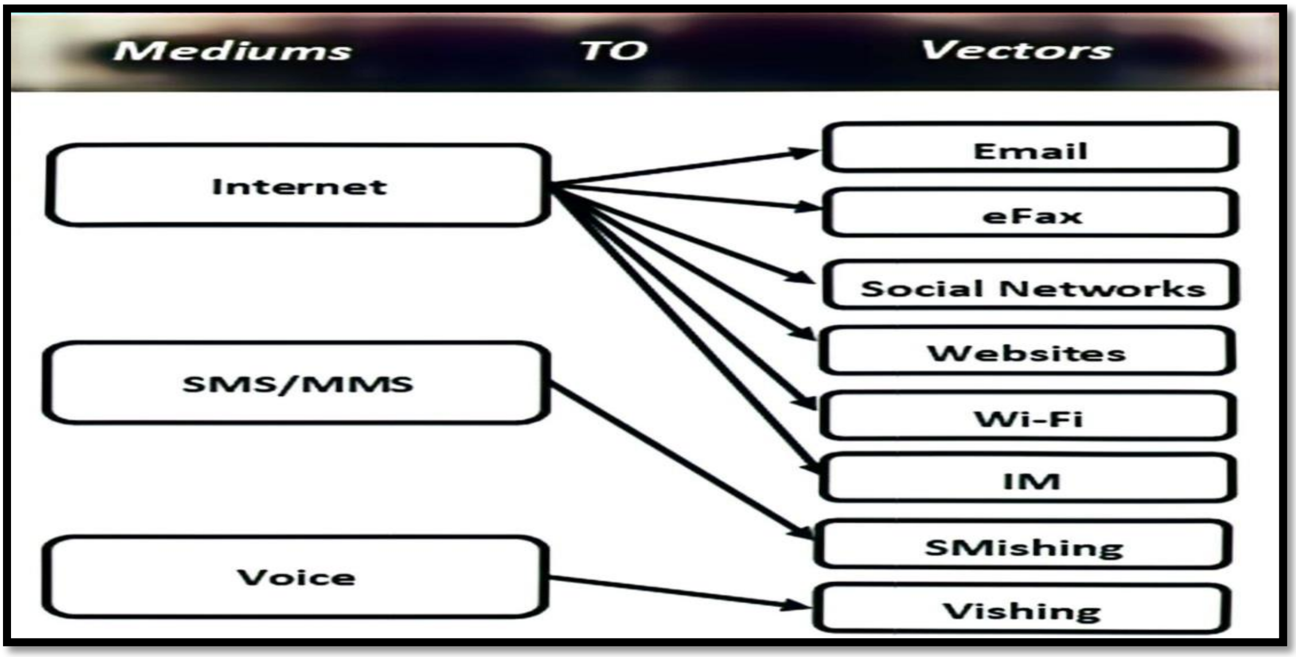

Figure (1): How media map to vectors [16]

Social Networks: Informal risk sharing, a vital strategy for crisis management, occurs through social networks. Social media has undergone significant development, providing a means for communication and the exchange of experiences among users. Platforms such as Twitter, Facebook, and LinkedIn are examples that facilitate interactions and enable users to identify others who share their interests, viewpoints, and hobbies. Although these platforms primarily focus on tracking individual posts, specialized social media platforms like Pinterest and Tumblr concentrate on specific topics or communities. However, the ease of sharing personal information online offers fraudsters opportunities to identify groups of potential targets and communicate with potential victims accordingly [17].

Phishing Website: Cybersecurity theft generates counterfeit websites that mimic authentic ones, intending to mislead unsuspecting individuals. Users are redirected to deceptive websites using links contained in emails, ads, or other methods [18]. This study examined the efficacy of Gradient and CatBoost algorithms in identifying URL-based phishing websites. The results demonstrated encouraging accuracy rates, suggesting the potential of these algorithms in improving cybersecurity measures to combat phishing attempts [19]. Users are instructed to scam. The phisher unlawfully collects sensitive information from users when they interact with the fraudulent website [(20)]. These attacks exploit counterfeit websites to deceive users into disclosing personal information or participating in detrimental activities. Furthermore, the widespread perception among typical internet users that phishing attempts predominantly transpire via emails and chat platforms results in diminished security awareness when navigating websites, hence increasing their vulnerability to such threats [21]. Various techniques are available for creating a fraudulent website, such as acquiring the source code of a certain site, replicating it, or employing specialist software. Fraudulent websites [22].

Wi-Fi: Phishing occurrences frequently transpire in public areas, representing a widespread category of phishing attacks. This method can also be employed in spear phishing or whaling attacks, when a specific public hotspot is chosen based on a particular victim's habitual use of the Wi-Fi network [12]. Spoofing and spear phishing attacks may involve creating a contact model of an email sender and utilizing a hardware processor to ascertain the statistical dispersion of the generated data. The contact model reflects the dispersion of data distribution in the developed model and how an email is received from the sender via a computer network. This includes multiple strategies, namely the deployment of malware on the victim's device to capture credentials or redirect them to fraudulent websites [23].

Phishing Over Phone: pertains to phishing and smishing. This occurs through phone calls or text messages, wherein the perpetrator impersonates an acquaintance of the victim or another credible entity with which the victim engages. The victim may be redirected to a malicious website via a link embedded in the SMS message, allowing hackers to utilize the victim's credentials to enter their instant messaging service and target contacts in their list [24].

Smishing: Smishing (SMS phishing) is a cybercrime in which criminals send fraudulent messages, including malicious links, to steal the victims' private data or cause financial losses. Also known as "SMS phishing," it leverages instant communication or text messaging platforms for malicious purposes [(25)]. To reduce the risk of becoming a victim of these attacks, exercise caution with unsolicited communications, particularly those requesting sensitive information or urging immediate action via phone or email. Always verify the legitimacy of the source before responding, and refrain from disclosing personal information unless you initiated the communication [23].

Social Media Phishing: Cyberattacks are a growing category that employs social media platforms to manipulate individuals and obtain their confidential information. This form of attack depends on the impersonation of established personalities or reputable companies to entice victims into clicking on malicious links or disclosing personal information, including usernames, passwords, and credit card details. The employed strategies consist of generating counterfeit login pages, disseminating misleading messages via integrated messaging programs on platforms, and leveraging the trust inherent among users. These assaults seek to obtain financial or personal data or to disseminate malware [11]. Specialized social media platforms exist that focus on particular domains, including sites like Pinterest and Tumblr. The act of disseminating personal information online serves as a valuable asset for phishers to pinpoint target demographics and potentially engage victims [16].

C. Phishing Technical Methods

Phishers utilize the aforementioned vectors to implement diverse technical strategies designed to obtain the victim's personal information. Technical methods function as supplementary mechanisms integrated with social engineering phishing to enhance its efficacy. Phishers employ several technical methods, leveraging one or more previously described vectors, to obtain personal information from their victims. Phishing attack methodologies can be categorized into two primary types: social engineering and malware-based methods. Social engineering exploits the user's fear of prospective losses, compelling them to reveal personal information to the phisher. In contrast, malware-based phishing assaults entail the clandestine installation of harmful software on the user's device, providing the phisher with illegal access.

Social Engineering attacks: Phishing is a form of social engineering attack designed to acquire sensitive information, such as personal identification and bank account details, from internet users by masquerading as a trustworthy institution in digital contacts. Phishing predominantly targets the digital sector over all other industries. Phishing is executed by constructing a fraudulent website, either by replicating the authentic page or by making tiny alterations, rendering it indistinguishable from legitimate sites to the internet user. Phishing assaults can transpire in multiple domains, including online payments, websites, emails, and financial institutions [26]. This strategy, regarded as one of the most ancient in the phishing and hacking communities, lacks a definitive technical defense method and has been characterized as "the art and science of persuading individuals to acquiesce to your demands" [16]. The primary objective of this assault is to undermine the victim's rational decision-making and instead induce actions driven by malleable emotions [26].

The Following section is Attack Techniques:

1-Whaling: Whaling attacks are a sophisticated form of spear-phishing that targets senior managers, CEOs, and other decision-makers in organizations. Whaling, as opposed to generic phishing, uses the power and privileges of particular people to obtain private data, carry out fraudulent financial transactions, or compromise the security of an organization. To make detection more challenging, scammers usually craft carefully crafted messages that mimic real business correspondence. Businesses are more vulnerable to these types of attacks as a result of their growing reliance on digital communication and remote corporate operations [23]. Phishers carefully build their fraud to closely mimic genuine correspondence because of its highly targeted nature. Email and eFax are frequent attack vectors for this kind of attack. [27].

2-Spear Phishing: Spear phishing, also known as targeted phishing, is a sophisticated type of targeted attack that has grown significantly recently. Targeted phishing emails cannot be adequately described by the conventional email features based on the sender's behavior profile, and they frequently make detection more difficult when the dataset is small. To address these issues, after gaining the recipient's trust, the attacker must take advantage of it by pressuring the victim to comply with their wishes. Email-based targeted phishing attacks can be carried out in two ways: An attachment can be the target of a malicious attack. The attacker frequently uses malicious attachments, and the files they attach typically contain zero-day vulnerabilities. The malicious code will run if the recipient opens and runs the attachment. attack using credentials. Credential-based targeted phishing messages are another name for phishing-based attack techniques. A phishing link that contains malware or directs to a pre-made phishing webpage is included by the attacker within the email text, script, or attachment [28]. Compared to traditional phishing, spear phishing is more personalized, making it hard to detect [23].

3-Email Scam phishing: Phishing email is another name for it, and it entails sending phony emails to several random victims from unidentified sources. These fraudulent emails pose as people or reputable financial organizations that the recipient is familiar with in an attempt to persuade them to divulge private information. The most frequent threat that attackers encounter is deception through email communications, which is still the most common type of phishing to this day [29].

4-CSRF Attack: CSRF (Cross-Site Request Forgery, commonly referred to as XSRF) is a form of attack targeting website users that takes use of vulnerabilities in the Hypertext Transfer Protocol. This constitutes an assault wherein an attacker does diverse acts on a website on behalf of authenticated users, like dispatching messages, transferring funds across accounts, or altering passwords. An attack scenario of this nature is feasible. The user is on the public services website when he receives a phishing email containing the following message: “New restrictions have been implemented in the city of N due to the threat of the coronavirus epidemic.” Kindly refer to the link for further information. Upon clicking the link, the user is redirected to the attacker's site, which accesses the browser cookie and obtains a series of authentication credentials linked to a particular session or user (token), including the login, password, and the user's private key [30].

5-Angler phishing: This constitutes a mixed assault, often described as the combination of smishing and vishing, especially prevalent on social networking platforms [31]. In this system, hackers transmit direct messages or voice notes to selected individuals, coercing them to undertake particular tasks. Consequently, it is prudent to authenticate the identities of social media users to prevent them from becoming victims of impersonation.

6-Business email compromise (BEC): The most recent instrument in cybercrime is spear phishing, particularly through executive impersonation threats, including Business Email Compromise (BEC), "CEO fraud," and "man-in-the-middle fraud." BEC assaults are intricate email fraud schemes that jeopardize firms during their routine bank transfer operations. In BEC assaults, social engineering is a crucial element, as fraudsters have proven highly adept at misleading firms and employees globally [32].

7-Wiphishing: commonly referred to as an evil-twin attack, exploits wireless networks [31].

8-Sound squatting: referred to as homophone squatting. This is a fraudulent tactic employed by cybercriminals to mislead people into accessing harmful websites by capitalizing on phonetic similarities between authentic domain names and their misleading alternatives. Malicious actors register domain names that closely resemble those of popular or renowned websites, frequently employing homophones or phonetically similar terms. These fraudulent domain names may feature misspellings, transposed characters, or differences in word endings that are too subtle for users to detect but sound virtually identical to the authentic domain name when articulated. The objective of sound squatting attacks is to exploit users' typographical errors or mispronunciations while entering internet URLs, resulting in their inadvertent navigation to hostile sites rather than the intended lawful ones. Upon arriving at these fraudulent sites, consumers may encounter numerous hazardous behaviors, including phishing schemes, malware installations, or financial deception.

9-Top-Napping: Utilized by phishers is misleading. Assault methodology. The phrase derives from the amalgamation of "tab" and "kidnapping," denoting individual webpages (tabs) accessible within a single browser window. Exploiting users' propensity to leave tabs inactive during surfing, attackers capitalize on this behavior to reroute these idle tabs to malicious webpages or unfamiliar URLs. This method enables the initiation of phishing attacks, executing scripts to retrieve sensitive data and information from the victim.

10-Typo squatting: Also referred to as URL hijacking, this cyberattack involves the registration of domain names that closely resemble those of prominent or well-known websites, incorporating common typographical errors or misspellings. In typo-squatting attacks, cybercriminals exploit frequent human errors, such as mistyping a letter, omitting a character, or transposing adjacent characters, when inputting website addresses into a web browser. Attackers register domain names that closely resemble legal websites with slight typographical errors to capture traffic from people who accidentally make such mistakes while entering URLs. Upon accessing these misleading domain names, visitors may confront harmful content or be routed to counterfeit websites intended to extract personal information, disseminate malware, or engage in other nefarious activities. Because the domain names used in typo-squatting attacks look very similar to real ones, users might not quickly realize they are on a harmful website, which increases the chances of falling victim to the attack.

11-**Malware**

Malware developers infiltrate users' mobile devices to install malicious software and expropriate personal information surreptitiously. Recent research indicates that malware developers are increasingly targeting Android mobile devices. Android mobile devices were introduced in 2008 and have since become the most prevalent operating system globally. These mobile devices are increasingly frequently utilized for diverse tasks, including payments, photography, ticket booking, and purchasing, all of which necessitate a mobile application. Over five million mobile applications are accessible for Android and iPhone platforms [(33]. Malicious software, also known as malware, is software whose author's intent is malicious [34].

12-**Keyloggers**

While having genuine applications, they are frequently employed for malicious purposes. This scenario involves the interception and transmission of every keystroke on the victim's device to the attacker, possibly exposing sensitive information, including login credentials and personal data, without the user's consent [35].

13-**Viruses**

Viruses in most of their forms replicate by spreading in other programs and incorporating their code. Malware can modify a computer's operations and conceal itself within other files. Viruses are harmful programs that seek to proliferate by inserting themselves into other files upon activation. Contrary to prevalent assumptions, merely placing an infected CD, floppy disk, or flash drive into a computer will not result in infection unless an autorun file is present; the virus must be executed to operate. Viruses infiltrate applications within a computer system and can affix themselves to executable code, utilizing extensions such as .exe to conceal their existence. Human interaction is generally necessary for the transmission of viruses, with email serving as one of the most efficient conduits. Viruses inflict considerable economic damage by inducing system failures, depleting resources, corrupting data, escalating maintenance expenses, and appropriating personal information. Infections may arise from opening email attachments, accessing compromised websites, executing files, or interacting with infected advertising. Removable storage devices, such as USB drives, can also transmit diseases. Viruses can circumvent defense mechanisms and readily penetrate computers [36].

14-Adware

Adware is commonly referred to as advertising-supported software. Such software is a distinct category of spyware that bombards consumers with an incessant flow of ads, potentially jeopardizing device functionality. Although the majority of adware is simply bothersome, several versions may monitor user actions or log keystrokes for nefarious purposes. bothersome, several versions may monitor user actions or log keystrokes for nefarious purposes [16]**.**

15-Rootkits

Rootkits are assemblages of malicious software that facilitate illegal access to a computer or network, permitting attackers to circumvent detection by system utilities. These kits enable individuals with less technological proficiency to initiate phishing assaults [37].

16-Spyware

Spyware is defined as software that is placed on a computer without the user's consent and transmits information regarding the user's computer activity. Internet. A comprehensive definition of spyware is, as paraphrased from a technology website, a category of software installed on various electronic devices, including home security systems and mobile phones, that can facilitate surveillance, acquire private information, or extract sensitive data without the user's awareness. Software planted on a party's phone before the commencement of a family court lawsuit can be converted into spyware. Nonetheless, spyware may be surreptitiously and remotely implanted [35]. Although spyware does not self-replicate across devices like viruses, it disseminates through installations conducted without explicitly informing users of the malware's presence or actions on their systems.

17-Ransomware

Ransomware is a type of virus that takes advantage of system vulnerabilities, allowing unauthorized access before encrypting certain data. It replicates like a worm and impedes users' access to their system by encrypting and safeguarding files of Vectem until a ransom is paid [38]. Ransomware generates extortion revenues amounting to millions of dollars annually. Recent versions hinder identification, facilitating the escape of numerous malware and intrusion protection systems. The malware often postpones system capture for extended periods, occasionally lasting days or even weeks after the first breach, endangering several systems. The malware can disseminate AUTORUN files between devices through internal Universal Serial Bus (USB) connections or network drives that interface with several systems. Upon initiating the encryption, the culprit simultaneously impacts all compromised systems. It utilizes many techniques to attack its victims' businesses. Prevalent attack strategies encompass exploit kits, harmful email attachments, and malicious email hyperlinks. Phishing is a prevalent and extensive method for disseminating malware to victims' systems. Ransomware attacks employ diverse infection routes, such as malicious advertisements, compromised websites, spam, social engineering, drive-by downloads, and others [3].

18-Man-in-the-Middle

Man-in-the-middle attacks consist of two types. In a conventional man-in-the-middle (MITM) attack, a nefarious individual intercepts direct communication between two parties, while a man-in-the-cloud (MITC) assault intercepts communication between the user and cloud services. In a man-in-the-middle (MITM) attack, a nefarious actor intercepts and alters data utilized by a service provider and the communicating party. The assailant subsequently contacts the service provider, impersonating the user. The assailant can thereafter get credentials, account details, and financial information, and exploit resources permitted for the user. Tools utilized for executing these attacks include Ettercap and the Metasploit Framework [16].

19-Worms

Worms are autonomous, self-replicating software programs that propagate from one machine to another inside a network. Worms are programs that autonomously propagate across systems without relying on a host file. This differs from viruses, which necessitate the transfer of an infected host [39]. Worms exploit weaknesses in operating systems, network protocols, or software applications to penetrate computers and networks. Upon infiltrating a system, a worm can duplicate and disseminate to additional susceptible devices within the same network or over the Internet. Worms can proliferate swiftly and compromise several computers within a short timeframe, rendering them quite effective for executing extensive and coordinated cyber-attacks. They are generally disseminated by email attachments, various websites, and data exchanged over the network [40].

20-Trojans

Trojans, abbreviated from Trojan horses, are a category of malicious software (malware) that impersonates legitimate applications or files to mislead users into executing them. Trojans do not multiply or propagate autonomously like viruses or worms; instead, they depend on user involvement for activation. Upon execution, Trojans can undertake numerous detrimental acts, including the theft of critical information, the installation of supplementary malware, the compromise of system security, or the provision of remote access to attackers [41].

21-**Pharming**

Commonly referred to as DNS-based phishing, this involves manipulating the domain name system to redirect people to harmful websites by compromising their DNS cache with false information. This assault can impact several users indiscriminately, potentially resulting in extensive data breaches and financial detriment [40].

22-Clone Phishing

Clone Phishing entails the fabrication of counterfeit websites with names resembling authentic ones to mislead people into believing they are visiting trusted sites. This strategy aims against individuals who visit authentic websites, deceiving them into revealing personal information and login credentials [40].

23-**URL and HTML Attacks**

URL and HTML obfuscation attacks are common in phishing schemes, wherein perpetrators conceal harmful links to divert victims to fraudulent servers rather than authentic websites. Phishers frequently utilize methods such as domain name obfuscation to replicate genuine URLs [42].

3. Phishing Detection Techniques

Phishing detection tactics include human awareness, or user education, aimed at instructing individuals to identify phishing efforts by exercising caution and vigilance when engaging with emails, texts, or websites, especially during URL verification. Nevertheless, even prudent users may succumb to phishing schemes, requiring software-based detection to verify a website's legitimacy. Phishers always refine their strategies, rendering current anti-phishing measures increasingly ineffective. Software-based detection approaches are favored for their capacity to adapt to advancing phishing strategies [12]. Detecting and preventing phishing assaults presents a considerable problem for researchers because of the adaptive strategies utilized by phishers to circumvent current anti-phishing defenses. Furthermore, intricate phishing tactics can aim at informed and seasoned users. This section will delineate and examine several software detection methodologies for phishing attacks in a thorough manner. Prior research is classified into the subsequent detection methodologies: Traditional detection techniques encompass list-based methods, visual methods, and heuristic methods. Artificial intelligence encompasses machine learning and deep learning methodologies.

The majority of the detection strategies examined in this study employ one or a mix of the previously listed methods. Table 1 illustrates the many phishing detection methodologies utilized in the model's development.

A. Database-oriented Techniques

Also known as a list-based detection Technique [3]. Upon accessing a new URL, it is juxtaposed with entries in the database. Upon detecting a match, the browser restricts access to the URL and revises the blacklist for future use. Blacklisting is frequently integrated into browser security tools, such as plug-ins and anti-phishing toolbars, to automatically detect dubious websites and safeguard users from unintentionally revealing critical information [42]. However, managing blacklists poses challenges due to the ephemeral nature of phishing websites, which generally have short lifespans and are swiftly supplanted by new ones [19]. Moreover, concerns over the authenticity of these listings, including false positives and true negatives, continue to exist, wherein good sites may be erroneously categorized as illegitimate and vice versa. Whitelisting, conversely, authenticates URLs by referencing a directory of verified sites. Although effective, list-based solutions are susceptible to URL fluctuations and necessitate [21] [22].

B. Machine Learning Detection

Methodology Machine Learning has emerged as a prevalent technique for the detection of phishing websites [43]. Collecting common qualities, such as URLs, information, website architecture, and JavaScript functionalities, is crucial for identifying phishing URLs and their corresponding websites. Phishing datasets are subsequently created utilizing these attributes, and machine learning classifiers are trained with this data. This approach analyzes URL attributes in conjunction with associated websites to develop predictive models that can differentiate between benign and dangerous URLs. Studies indicate that machine learning algorithms can proficiently detect novel malware variants [(44). Nonetheless, the limitation is that machine learning-based detection methods continue to depend on feature engineering and advanced or specialized features to complete the learning task; consequently, they exhibit a high false alarm rate due to inadequate feature selection and suboptimal classifier development, remaining vulnerable to adversarial attacks [29]. Many classification techniques require a substantial quantity of training samples to develop classification models. Polymorphic and adversarial assaults can circumvent them.

C. Deep Learning Technique

A deep neural network (DNN) is a sophisticated machine learning system employing several layers of nodes to derive high-level functions from input data [45]. Recent breakthroughs in deep learning indicate Deep neural networks surpass traditional machine learning methods. for identifying phishing websites. Diverse deep learning methods are prevalent for phishing detection. Comprehending the internal mechanisms of deep learning models is essential for their improvement and efficient utilization. Deep learning possesses the advantage of being featureless; algorithms based on deep learning do not necessitate feature selection, even when significant performance improvements are observed. A model can be developed from raw data, with deep learning algorithms facilitating the identification of the most significant patterns for the ultimate conclusion. This methodology entails examining URL data alongside associated websites to develop a predictive model that distinguishes between benign and dangerous URLs. Deep learning-based approaches achieved elevated accuracy rates and diminished false positive rates for both recognized and zero-day malware. Nonetheless, the technique's precision necessitates enhancement [45].

D. Heuristic Techniques

The heuristic method utilizes components seen in phishing websites [3] . This method depends on distinct attributes that distinguish phishing websites from authentic ones. It aggregates data from several sources, encompassing website traffic, digital certificates, textual content, DNS, and URLs. The efficacy of this method is influenced by the feature set, training samples, and classification algorithms employed. One of the advantages of this technique is its capacity to detect zero hour phishing attacks. [40]. This detecting method may be ineffective for websites with little content. Phishers frequently employ graphics to substitute text on websites, so confounding detection. Heuristics for identifying phishing efforts depend on parameters such as raw word count, Alexa rating, consistent brand names, and brevity of word length. Although these approaches demonstrate considerable effectiveness in identifying phishing attempts, they are generally employed to issue alerts to users within the web browser rather than to obstruct suspected phishing websites. The majority of the criteria included in heuristic analysis are intuitive, potentially resulting in a considerable number of false positives [3]. They are reported to require considerable time for detection and can be circumvented by polymorphic and adversarial attacks. As shown in Table (1).

Table (1): Studies on Phishing attacks and detection Techniques

S/N	AUTHER & YEAR	AIM & OBJECTIVE	METHODOLOGY	DETECTION APPROACH & ALGORITHM USED	RUSULT	LIMITATION &FUTURE RESEARCH
1	M. Irfan Uddin 2020 [46]	The proposed study is an endeavor toward the detection of phishing by using random forest and BLSTM classifiers.	Development of a hybrid feature set by evaluating thirty different feature sets and using random forest (RF) and binary long short-term memory (BLSTM) architectures for classification.	Random Forest (RF) and Binary Long Short-Term Memory (BLSTM).	The BLSTM-based phishing detection model generates a recognition rate of 95.47% compared to the conventional RF-based model that generates a recognition rate of 87.53%.	Limitations| The dataset has 30 different keywords and 2456 varying instances, so using whole of the data for the training purpose takes a long time.
2	N.S. Nordin e 2019 [47]	To explain in detail how fuzzy modeling works by using the Firefly Algorithm (FA) for detecting phishing and to propose an improved method for fuzzy modeling using FA to	The study uses fuzzy modeling with the Firefly Algorithm (FA) for automatic fuzzy parameter generation. It involves using two datasets: a phishing website dataset from the UCI machine learning repository and an	Firefly Algorithm (FA) is used for optimization and to generate fuzzy rules and membership functions.	The average accuracy for the phishing websites dataset achieved 98.86%, while the average value for the SMS dataset is 97.49%.	The text does not explicitly mention limitations of the study. However, it does mention that some previous methods are not flexible to accommodate the increasing.

		automatically generate fuzzy rules and membership functions.	SMS message dataset from the Unicamp website.			
3	Noor Syahirah Nordin 2020 [48]	To propose a method by the application of the Butterfly Optimization Algorithm (BOA) in fuzzy modelling to detect phishing, addressing the issue of manually generating fuzzy parameters in complex problems.	fuzzy modelling with the Butterfly Optimization Algorithm (BOA) to automatically tune fuzzy parameters. It involves using two datasets (Website Phishing Dataset (WPD) and Phishing Websites Dataset (PWD)) from the UCI machine learning repository and applying k-fold cross-validation for evaluation.	Fuzzy system, Butterfly Optimization Algorithm (BOA).	The proposed method achieved average accuracies of 96.80% for the Website Phishing Dataset (WPD) and 94.65% for the Phishing Websites Dataset (PWD).	The text does not explicitly state the limitations of the study.
4	K.Althobaiti 2023 [49]	explores the feasibility of using clustering algorithms to group emails into campaigns that IT staff would interpret as being similar.	DBSCAN algorithms with seven feature sets. Then, they evaluated the solutions with the Silhouette coefficient and homogeneity score and found that Mean Shift outperforms DBSCAN with email origin and URLs-based features. Finally, a user study was conducted to validate the clustering solution, finding that clustering is a promising approach for campaign identification.	The two algorithms used were Meanshift and DBSCAN.	The Mean Shift algorithm with the email origin and URL features can reduce the original set of 60K emails to <6K relatively homogeneous clusters.	First, the dataset was collected from a specific organisation over two somewhat short time frames. Second, in order to assess its effectiveness in practice,clustering needs to be integrated meaningfully into the workflow of IT teams.

5	Ali Raheem Al-Hafiz 2025 [50]	The research aims to enhance the classification process by identifying the best set of features in each group through the Genetic algorithm and applying a voting ensemble technique to combine models like Support Vector Machine (SVM)	Utilises the Genetic algorithm for feature selection, followed by the K-means clustering algorithm to divide the dataset into groups with similar traits.	The algorithms used in this research are: K-means clustering Genetic Algorithm (GA) Support Vector Machine (SVM) Random Forest (RF)	Achieved 99% accuracy using the voting ensemble technique with feature selection, compared to 77.3% without feature selection.	The text focuses on the model's effectiveness and doesn't explicitly state limitations. However, implicitly, the scalability and efficiency of such a solution in real-world applications are demonstrated.
6	Subudhi and S. Panigrahi 2017 [51]	To detect superimposed mobile phone fraud by applying possibilistic fuzzy c-means (PFCM) clustering	Behavioral profile modeling of subscribers using PFCM clustering on historical call records.	Possibilistic Fuzzy C-Means (PFCM) clustering	PFCM outperforms other clustering techniques, yielding better performance in terms of true positive rate (TPR), false positive rate (FPR), accuracy, precision, and F-score.	The text does not explicitly mention limitations of the proposed approach.
7	ZHANG Yong-jie [52]	eliminate false alarms in high resolution range profile (HRRP) target detection, which arise due to low detection thresholds needed to ensure target detection in scenarios with multiple extended targets and low signal-to-noise ratio (SNR).	The methodology combines monopulse angle measurement and weighted fuzzy C-means (WFCM) clustering with the constant false alarm detection algorithm, using prior information of target quantity and volume. This approach leverages azimuth information and clustering center parameters to distinguish between target scattering points and clutter	Constant False Alarm Rate (CFAR) Detection Used initially to provide a detection threshold.	eliminates false alarm clutter and obtains accurate HRRP of the target in simulation scenarios. The method is shown to be an improvement over extended target M / Nt binary detection.	The algorithm may struggle to eliminate clutter when it is very close to the target scattering point in both distance and azimuth.

8	Shawq Malik Mehibs 2018 [53]	create intrusion detection very important to detect outsider and insider intruders of cloud computing with high detection rate and low false positive alarm in the cloud environment.	The proposed FCM algorithm for intrusion detection (FCM-ID) consist of two phase. The first phase is training phase where the optimum cluster center obtain. The second phase is testing phase which used the cluster center result from training phase to determine the cluster of new samples.	Fuzzy c Mean (FCM) algorithm.	High detection rate with low false positive alarm. Experimental results show the effectiveness of the system in detecting attacks and recognizing normal behavior with a high detection rate (99%) and a low false alarm rate (1.9%). The accuracy of system is (99%).	The text does not explicitly mention any limitations of the proposed system.
9	Dr. Priyanka Kaushik 2023 [54]	To provide a deep learning-based method for detecting phishing attacks that combines CNN and LSTM networks. The approach aims to extract features from the URL and email content	Proposes a hybrid CNN-LSTM architecture. Involves data collection, data pre-processing (converting email and URL text into a sequence of characters and representing each character as a one-hot encoded vector), model architecture design, model training using the collected dataset and Adam optimization technique	Combination of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. CNN is used to extract features from URLs. LSTM network is used to analyze email content.	Achieves an accuracy of over 95% on a real-world dataset.	the network depends on the quality and amount of the training data. The model is not expected to be 100% accurate, as attackers are constantly adapting and evolving their techniques.
10	Alper Ozcan 2021 [55]	The main objective of this research is to develop a better phishing detection model based on deep learning algorithms in terms of accuracy metric.	long short-term memory and deep neural network algorithms for detecting phishing uniform resource locator and evaluates the performance of the models on phishing datasets. In this study, both traditional machine	The algorithms used are long short-term memory (LSTM) and deep neural network (DNN) algorithms	The hybrid model that integrates DNN and BiLSTM algorithms provided 98.79% accuracy, 0.9878 AUC, and 0.9881 F1-score on the Ebbu2017	The following limitations exist for this study: • We built a new dataset in this study and also, used a recent dataset for our experiments.

			learning methods (i.e., k-Nearest Neighbors (kNN) and tree-based methods) and deep learning algorithms (i.e., RNN and CNN-based methods)		phishing dataset when cross-validation was used for the evaluation.	
11	Shubhangi Pandey 2020 [56]	The main aim is to impulse the users to divulge their financial data, credential or sensitive information. The objective of identifying phishing emails from legitimate one's is accomplished.	Uses Natural Language Processing (NLP) techniques to analyze text and detect inappropriate statements indicative of phishing attacks. Makes use of Deep Learning frameworks with Neural Network. Feature extraction of 40 features, followed by feature selection using mRMR.	Machine Learning: Bagged decision tree, Random Forest, Extra Trees, Adaboost, Stochastic Gradient Descent, Naive Bayes, SVM, and Voting Ensemble. Deep Learning: Neural Networks	Achieved up to 97.21% accuracy with Extra Trees on Spam Assassin and 72.06% with Voting Ensemble on Ham-Spam dataset using ML. Achieved 96.7% and 80% accuracy on Spam Assassin and Ham-Spam datasets	A few of the papers have encountered a high accuracy but on a small set of data
12	Badnera Amravati 2018 [57]	to identify an email as spam or ham based on text categorization. The proposed system enables the user to have more control over the various categories of spam and allows for filter personalization.	Pre-processing of email format (stop words removing, stemming, feature reduction and feature selection) to fetch keywords. Using numeric feature representation for feature extraction. Applying fuzzy c-means algorithm for clustering feature vectors..	Fuzzy c-means clustering algorithm. Support Vector Machines (SVM).	does not explicitly state the results of the proposed methodology.	does not explicitly mention the limitations of the proposed methodology.

4-DISCUSSION

The evolving landscape of cyber threats and the countermeasures implemented to mitigate them are comprehensively understood through a survey review of phishing attacks and detection techniques. This discussion is intended to emphasize the primary findings and trends that have been identified in the existing literature, as well as the voids in knowledge that require further investigation. Phishing attacks continue to pose a significant risk to businesses, organizations, and individuals worldwide. These assaults utilize misleading strategies to manipulate users into giving confidential information, like financial data, personal particulars, or authentication credentials. Due to the increasing sophistication of offenders and technical progress, conventional detection methods have become less effective in identifying and blocking these attacks. The systematic review examines many types of phishing assaults, encompassing spear phishing and social media phishing. The investigation investigates the tactics utilized by attackers, encompassing social engineering methods, harmful attachments, and counterfeit websites, to exploit weaknesses and gain unauthorized access to confidential information. The review also explores the effectiveness of different detection methods used to identify and counteract phishing attacks. These techniques span a diverse array of methodologies, including list-based identification, anomaly detection, and machine learning algorithms, among others. The assessment analyzes the advantages and disadvantages of each method for detection accuracy, false positive rates, scalability, and adaptability to new threats. The review also addresses the issues of phishing detection, including the continual evolution of attack vectors, the emergence of new attack strategies, and the difficulty in differentiating legitimate communication from phishing attempts. It also analyzes the influence of human variables, like user awareness and education, in reducing the danger of phishing attempts. The systematic review offers significant insights into the present condition of phishing assaults and detection methodologies. The review advocates for the amalgamation of several detection methodologies to augment accuracy and resilience in detection techniques.

5-CONCLUSION.

Phishing attempts are escalating, becoming more intricate, and attracting heightened scrutiny from cybersecurity experts and developers aiming to counteract them. This study is based on an analysis of diverse phishing assaults and detection methodologies. The purpose is to inform readers, internet users, and security managers on the characteristics of phishing attacks and the detection strategies available to counteract them. The report, after a comprehensive analysis of relevant documents, identified email and internet attacks, as well as phone phishing, as the most common phishing techniques. The principal aim of this research is to furnish a comprehensive grasp of contemporary phishing and phishing detection techniques. Researchers seek to predict and assess the efficacy of investigative strategies against diverse future threats. Future studies may concentrate on developing and implementing ways to detect and minimize phishing, vishing, and smishing perpetrated via social media.

References

[1] Orunsolu AA, Sodiya AS, Akinwale AT. A predictive model for phishing detection. Journal of King Saud University - Computer and Information Sciences. 2022 Feb 1;34(2):232–47.

[2] Shah RK, Hasan MK, Islam S, Khan A, Ghazal TM, Khan AN. Detect Phishing Website by Fuzzy Multi-Criteria Decision Making. In: 2022 1st International Conference on AI in Cybersecurity, ICAIC 2022. Institute of Electrical and Electronics Engineers Inc.; 2022.

[3] Ayeni RK, Adebiyi AA, Okesola JO, Igbekele E. Phishing Attacks and Detection Techniques: A Systematic Review. In: International Conference on Science, Engineering and Business for Driving Sustainable Development Goals, SEB4SDG 2024. Institute of Electrical and Electronics Engineers Inc.; 2024.

[4] Al-Shalabi L, Jazyah YH. Phishing detection using clustering and machine learning. IAES International Journal of Artificial Intelligence. 2024 Dec 1;13(4):4526–36.

[5] Jemili F, Bouras H. Intrusion Detection Based on Big Data Fuzzy Analytics. In: Open Data. IntechOpen; 2022.

[6] Subudhi S, Panigrahi S. A hybrid mobile call fraud detection model using optimized fuzzy C-means clustering and group method of data handling-based network. Vietnam Journal of Computer Science. 2018 Sep;5(3–4):205–17.

[7] Al-Hamar Y, Kolivand H, Al-Hamar A. Phishing attacks in Qatar: A literature review of the problems and solutions. In: Proceedings - International Conference on Developments in eSystems Engineering, DeSE. Institute of Electrical and Electronics Engineers Inc.; 2019. p. 837–42.

[8] Abdolrazzagh-Nezhad M, Langarib N. Phishing Detection Techniques: A review. Data Science: Journal of Computing and Applied Informatics. 2025 Jan 31;9(1):32–46.

[9] Basit A, Zafar M, Liu X, Javed AR, Jalil Z, Kifayat K. A comprehensive survey of AI-enabled phishing attacks detection techniques. Vol. 76, Telecommunication Systems. Springer; 2021. p. 139–54.

[10] Desai V, R K. Unveiling the Depths of Phishing: Understanding Tactics, Impacts, and Countermeasures. International Journal of Innovative Research in Science,Engineering and Technology. 2024 May 22;13(05):8596–600.

[11] Ariani PC, Gede I, Widi Atmaja B, Jayanti KS, Ayu GA, Dewi A, et al. Comparative Analysis of Phishing Tools on Social Media Sites. Ultimatics : Jurnal Teknik Informatika [Internet]. 2023;15(1). Available from: www.facebook.com

[12] Professor Umesh Sindhu BR AT, Waseem N, Jadhav S. SECURITY IN SOCIAL MEDIA: AWARNESS OF PHISHING ATTACKS TECHNIQUES AND COUNTER MEASURES. International Journal of Scientific Research in Engineering and Management [Internet]. 2024; Available from: www.ijsrem.com

[13] Atawneh S, Aljehani H. Phishing Email Detection Model Using Deep Learning. Electronics (Switzerland). 2023 Oct 1;12(20).

[14] “Anti-Phishing Working Group (APWG). Phishing Activity Trends Report: 2nd Quarter 2025. 28 Aug. 2025, APWG, https://apwg.org”.

[15] Sonowal G. Phishing Email Detection Based on Binary Search Feature Selection. SN Comput Sci. 2020 Jul 1;1(4).

[16] Alabdan R. Phishing attacks survey: Types, vectors, and technical approaches. Vol. 12, Future Internet. MDPI AG; 2020. p. 1–39.

[17] Putman DS. Social network structure and the radius of risk sharing. Soc Netw Anal Min. 2025 Dec 1;15(1).

[18] Dutta AK. Detecting phishing websites using machine learning technique. Vol. 16, PLoS ONE. Public Library of Science; 2021.

[19] Deekshitha B. URL Based Phishing Website Detection by Using Gradient and Catboost Algorithms. Int J Res Appl Sci Eng Technol. 2022 Jun 30;10(6):3717–22.

[20] Narayana G, Manchala UD, Naresh U, Kiran S, Kiran MA, Ch RK. Improving Phishing Website Detection with Machine Learning: Revealing Hidden Patterns for Better Accuracy [Internet]. International Journal on Recent and Innovation Trends in Computing and Communication. Available from: http://www.ijritcc.org

[21] C S A, Ganapathy S V, E V, . R. Detection of Phishing Websites. International Journal of Innovative Science and Research Technology (IJISRT). 2024 May 15;2647–52.

[22] Jaswal P, Sharma S, Bindra N, Krishna CR. Detection and Prevention of Phishing Attacks on Banking Website. In: 2022 International Conference on Futuristic Technologies, INCOFT 2022. Institute of Electrical and Electronics Engineers Inc.; 2022.

[23] " Artificial immune system based methods for spam filtering. " 2013 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE , 2013. (Year : 2013). *.

[24] SIF-EDDINE M, MAZRI T. Detecting smishing attacks on smartphones: a comparative study between supervised and unsupervised learning techniques [Internet]. 2023. Available from: https://www.researchsquare.com/article/rs-3289212/v1

[25] Seo JW, Lee JS, Kim H, Lee J, Han S, Cho J, et al. On-Device Smishing Classifier Resistant to Text Evasion Attack. IEEE Access. 2024;12:4762–79.

[26] Proceedings of the 4th International Conference on Trends in Electronics and Informatics (ICOEI 2020) : 15-17, June 2020. IEEE; 2020.

[27] Rutvij Upadhyay, Dr. Shivam Upadhyay. A Review Paper on Detection and Mitigation of DDoS Attacks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2025 Jan 13;11(1):704–8.

[28] Ling Z, Feng H, Ding X, Wang X, Gao C, Yang P. Spear Phishing Email Detection with Multiple Reputation Features and Sample Enhancement. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Science and Business Media Deutschland GmbH; 2022. p. 522–38.

[29] IEEE International Conference on Blockchain and Cryptocurrency : 2-6 May 2020 : IEEE ICBC. IEEE; 2020.

[30] Ivanov MA, Kliuchnikova B V., Chugunkov I V., Plaksina AM. Phishing Attacks and Protection against Them. In: Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021. Institute of Electrical and Electronics Engineers Inc.; 2021. p. 425–8.

[31] Sapkal V, More N, Agme Asstprofessor R. A Briefed Review on Phishing Attacks and Detection Approaches [Internet]. Available from: https://ssrn.com/abstract=4108334

[32] Saud Al-Musib N, Mohammad Al-Serhani F, Humayun M, Jhanjhi NZ. Business email compromise (BEC) attacks. In: Materials Today: Proceedings. Elsevier Ltd; 2021. p. 497–503.

[33] Sharma M, Kaul A. A review of detecting malware in android devices based on machine learning techniques. Vol. 41, Expert Systems. John Wiley and Sons Inc; 2024.

[34] Rains Tim. Cybersecurity threats, malware trends, and strategies : mitigate exploits, malware, phishing, and other social engineering attacks. Packt; 2020.

[35] Luna FM. THE PERILS OF SPYWARE. Advocate. 2019;41(3):14–7.

[36] Zayyad MA. Systematic Study of Computer Virus using Virus Definition and Scanning Techniques. Asian Journal of Research in Computer Science. 2023 Nov 1;16(4):230–8.

[37] Yimu J, Shangdong L. Threats from Botnets [Internet]. Available from: www.intechopen.com

[38] Santangelo GV, Colacino VG, Marchetti M. Analysis, prevention and detection of ransomware attacks on Industrial Control Systems. In: 2021 IEEE 20th International Symposium on Network Computing and Applications, NCA 2021. Institute of Electrical and Electronics Engineers Inc.; 2021.

[39] Dhananjay Tangtode, Shayan Sayyad, Omkar Gelye, Sarthak Sawant, Prof. Girisha Bombale. DDOS Attack Detection. International Journal of Advanced Research in Science, Communication and Technology. 2024 Feb 29;248–51.

[40] Kumar D, Jugal B, Kalita K, Attacks D. Evolution, Detection, Prevention, Reaction, and Tolerance DDoS Attacks.

[41] Dhavlle A, Hassan R, Mittapalli M, Dinakarrao SMP. Design of hardware trojans and its impact on CPS systems: A comprehensive survey. In: Proceedings - IEEE International Symposium on Circuits and Systems. Institute of Electrical and Electronics Engineers Inc.; 2021.

[42] Opara C, Chen Y, Wei B. Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics. Expert Syst Appl. 2024 Feb 1;236.

[43] Vishesh Bharuka, Allan Almeida, Sharvari Patil. Phishing Detection Using Machine Learning Algorithm. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024 Mar 30;10(2):343–9.

[44] Almujahid NF, Haq MA, Alshehri M. Comparative evaluation of machine learning algorithms for phishing site detection. PeerJ Comput Sci. 2024;10.

[45] Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology (ICSSIT 2020) : 20-22, August 2020. [IEEE]; 2020.

[46] Wang S, Khan S, Xu C, Nazir S, Hafeez A. Deep Learning-Based Efficient Model Development for Phishing Detection Using Random Forest and BLSTM Classifiers. Complexity. 2020;2020.

[47] Nordin NS, Ismail MA, Mezhuyev V, Kasim S, Mohamad MS, Ibrahim AO. Fuzzy Modelling using Firefly Algorithm for Phishing Detection. Advances in Science, Technology and Engineering Systems. 2019;4(6):291–6.

[48] Nordin NS. Fuzzy Modelling using Butterfly Optimization Algorithm for Phishing Detection”. International Journal of Advanced Trends in Computer Science

and Engineering. 2020 Sep 25;9(1.5):355–60.

[49] Althobaiti K, Wolters MK, Alsufyani N, Vaniea K. Using Clustering Algorithms to Automatically Identify Phishing Campaigns. IEEE Access. 2023;11:96502–13.

[50] Al-Hafiz AR, Jabir AJ, Subramaniam S. K-Gen PhishGuard: an Ensemble Approach for Phishing Detection with K-Means and Genetic Algorithm. Al-Khwarizmi Engineering Journal. 2025 Jun 1;21(2):117–35.

[51] Subudhi S, Panigrahi S. Use of possibilistic fuzzy C-means clustering for telecom fraud detection. In: Advances in Intelligent Systems and Computing. Springer Verlag; 2017. p. 633–41.

[52] Liu Y, Zhang Y. Application of weighted fuzzy C-means algorithm in high resolution range profile target detection. In SPIE-Intl Soc Optical Eng; 2022. p. 22.

[53] Malik Mehibs S, Hassan Hashim S. Proposed Network Intrusion Detection System Based on Fuzzy c Mean Algorithm in Cloud Computing Environment. Journal of Babylon University/Pure and Applied Sciences.

[54] Kaushik P, Rathore SPS. Deep Learning Multi-Agent Model for Phishing Cyber-attack Detection. International Journal on Recent and Innovation Trends in Computing and Communication. 2023 Aug 1;11(9s):680–6.

[55] Ozcan A, Catal C, Donmez E, Senturk B. A hybrid DNN–LSTM model for detecting phishing URLs. Neural Comput Appl. 2023 Mar 1;35(7):4957–73.

[56] Zalavadia F, Pandey S, Pachpande P, Nevrekar A, Govilkar S. Detecting Phishing Attacks Using Natural Language Processing and Deep Learning models. 2020; Available from: www.ijcrt.org

[57] Katyarmal G. A Review on Spam Email Detection Using Fuzzy C-Mean with Machine Learning. International Journal of Recent Engineering Research and Development (IJRERD) www.ijrerd.com || [Internet]. 2018;03:29–33. Available from: www.ijrerd.com