The State of Phishing Attacks and Countermeasures

Sameer Abufardeh *abufards@erau.edu*
Computer, Electrical, and Software Engineering Dept
Embry–Riddle Aeronautical University
Prescott, AZ, 86301, USA

Bouchaib Falah *b.falah@aui.ma*
School of Science and Engineering
Al Akhawayn University
Irfan, Morocco

Abstract

Phishing is a cybercrime where criminals employ various deceptive techniques to obtain personal information from individuals. There are multiple facets of phishing attacks. These include what Phishing is, known phishing types, and methods used to protect users' personal information. While many tools are being used to protect users from phishing attacks, phishing attacks are increasing, its methods and tactics are changing, and more victims are falling for them. The first line of defense in protecting people from phishing attacks is, understanding the dynamics of Phishing and the psychology of both the attacker and the victim, and analyzing users' decision-making strategies in reaction to phishing attacks. This paper is intended to examine the multiple facets of phishing attacks to enhance our understanding of an extremely challenging issue for the IT community as the first step to curb the effects of this persistent crime.By understanding and implementing robust phishing defenses, individuals and organizations can mitigate the risks posed by this prevalent cyber threat, fostering a safer and more secure online environment for everyone.

Keywords: Phishing Email, Social Engineering, Phishing Types, Phishing Countermeasures, Phishing Prevention.

1. INTRODUCTION

Phishing is “a type of social engineering attack in which phishers, i.e., attackers, trick the victims into disclosing sensitive information under false pretenses” (Danuvasin, 2011; Aracindhan,2016). The attacker then exploits this information for fraudulent purposes. Examples of sensitive or confidential information include usernames, passwords, PINs, bank information, credit card details, etc. Despite being an age-old strategy, Phishing remains widely utilized and favored due to its simplicity and high success rate. Its primary focus is exploiting the most vulnerable security aspect, namely the user. According to the CISCO 2021 Cyber Security Threat Trends report, Phishing is responsible for a whopping 90% of data breaches (Cisco Umbrella, 2021).

Phishing is considered one of the most popular social engineering crimes today, and it continues to pose many challenges for researchers in both academia and industry. Most often,Phishing is an opportunistic attack with no discriminate target, but recently, the most damaging are those targeted ones. Phishing is commonly associated with email messages that imitate banks, credit card companies, or popular online platforms like Amazon, eBay, PayPal, etc. These deceptive messages are designed to appear genuine and trick victims into divulging their personal information. However, email messages are just one component of a phishing scam. The attacker's message generally includes credible sources or external references within a phishing attack. In some cases, phishers may include references to legitimate organizations, well-known individuals, or popular news articles to make their fraudulent communications appear more

authentic and convincing. By leveraging familiar names or reputable sources, they aim to gain the recipient's trust and increase the likelihood of successful deception. Phishers evaluate the successes and failures of their previous scams to coordinate future attacks. Phishing scams exploit vulnerabilities in software and security systems on both the client and server sides. Despite the use of sophisticated techniques, phishing scams ultimately rely on the age-old principles of confidence tricks, where the perpetrator convinces their target of their reliability and trustworthiness.

Phishing attacks are particularly dangerous due to their ability to exploit human vulnerabilities and manipulate individuals into revealing sensitive information (Threat Group-4127, 2016).Here are a few reasons why phishing attacks can be more dangerous compared to common security attacks:

- Social engineering: Phishing attacks often utilize social engineering techniques to exploit human psychology and emotions. By impersonating trusted entities or creating a sense of urgency, attackers can manipulate victims into bypassing their usual security precautions and providing their personal information willingly (Threat Group-4127, 2016).
- Targeted deception: Phishing attacks can be highly targeted, known as spear phishing. Attackers research their victims and tailor the phishing messages specifically to their interests, job roles, or affiliations. This personalized approach increases the likelihood of victims falling for the scam as the messages appear more legitimate and relevant.
- Wide reach: Phishing attacks can be launched against many individuals simultaneously. Attackers can send out thousands or even millions of phishing emails, increasing the potential for a significant number of victims to be tricked into divulging their information.
- Sophistication: Phishing attacks have become increasingly sophisticated over time. Attackers employ advanced techniques such as creating convincing email or website replicas, using URL manipulation, and utilizing social media platforms for reconnaissance. These tactics make it difficult for users to distinguish between genuine and fraudulent communications.
- Credential theft: One of the primary objectives of phishing attacks is to steal login credentials, such as usernames and passwords. With this information, attackers can gain unauthorized access to various accounts, including email, banking, or social media, leading to potential financial loss, identity theft, or unauthorized access to sensitive data.
- Infection vectors: Phishing attacks often serve as an entry point for other malicious activities, such as delivering malware or ransomware. Users are tricked to clicka malicious link or to download infected attachments, and attackers can gain control over systems or networks, leading to further data breaches or system compromise.
- Human error: Phishing attacks exploit the weakest link in cybersecurity, i.e., the human factor. Even with robust technical security measures in place, individuals can still be susceptible to manipulation or mistakes, making them vulnerable to phishing attacks.

The first step in combating Phishing is to understand how it works, educate individuals about phishing techniques, promote safe online practices, and employ robust technical solutions, including email filters, anti-phishing software, and multi-factor authentication, to mitigate the risks associated with these attacks. In the following sections, we will introduce a general description of the phishing process, then a brief discussion of common types of Phishing, then a brief discussion of phishing techniques, explore a few common types of Phishing and discuss various countermeasures employed to combat them.

1.1 Review Methodology

Among the vast number of peer-reviewed articles and conference papers on Phishing, only a small fraction of the sampled manuscripts from well-known databases like IEEE, Scopus, ScienceDirect, SpringerLink, Gale, Ebsco, and Google Scholar focused prominently on the prevention and reduction of Phishing through user-oriented analyses and strategies. To conduct our literature review, we followed the following steps:

Step 1: Keyword Search
Initially, we performed a broad search using keywords such as "phishing," "phishing countermeasures," "social engineering," "anti-phishing, “phishing techniques," “phishing Email,”“phishing types,” “phishing types,” and “phishing prevention.”This resulted in thousands of articles that met our criteria.

Step 2: Refinement
Next, we refined the search to include only studies concentrating on countermeasures, prevention, and anti-phishing. This resulted in fewer articles that met our criteria.

Step 3: Backward Search
To ensure thoroughness, we performed a backward search on the selected articles based on abstract reading. This helped us identify other relevant works done by the same author/s.

Step 4: Selection
Based on the relevance to the purpose of our study, we carefully selected articles from the pool of identified publications. Any publications that were found to be irrelevant were excluded.

2.1 Limitation and Survey Purpose
Phishing research spans a vast and intricate landscape, encompassing various techniques and mitigation strategies. However, a significant limitation lies in the persistent reliance on users to identify and thwart phishing attempts, highlighting the need for more comprehensive and user-friendly solutions in this ongoing battle against cyber threats.

We aim to provide a brief overview of various phishing techniques, types, and mitigation approaches. The aim is to present this information without delving into intricate details, making it accessible to a wider audience, including business managers, undergraduate students, and those with a casual interest in understanding phishing challenges. The literature review highlights that current solutions have not effectively reduced phishing attacks because they often overlook the human security vulnerabilities that phishers exploit. Users continue to fall victim to these attacks because they lack knowledge about how Phishing begins and struggle to visually distinguish legitimate emails and websites from fraudulent ones. Existing solutions still heavily depend on users to detect anomalies in emails or websites, indicating a need for more user-friendly and effective measures against Phishing.

2. A TYPICAL PHISHING PROCESS
Phishing is a cybercrime technique malicious actors use to deceive individuals and gain access to the victim'ssensitive information, such as passwords, credit card information, and personal data. A typical process of phishing Figure 1 involves several steps designed to trick the target into providing their confidential information. The following is an overview of the typical phishing process:

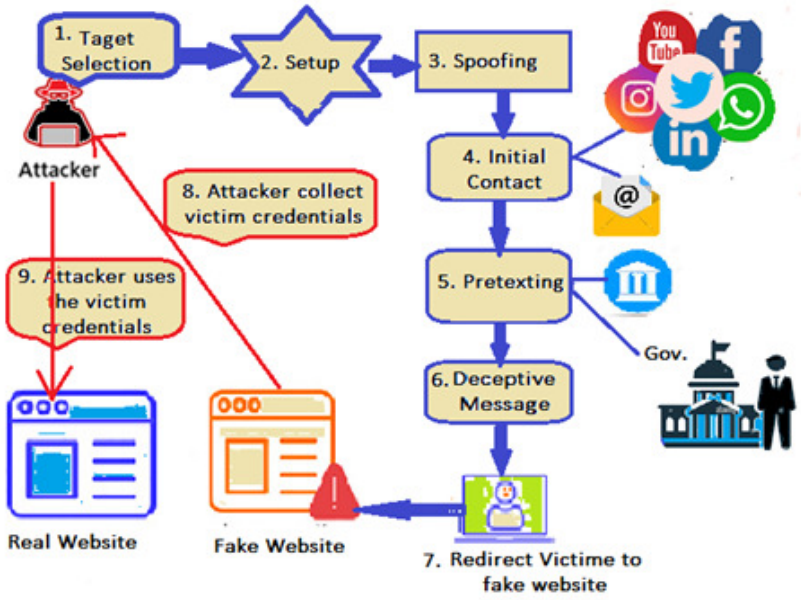

FIGURE 1: Typical Phishing Process.

1) Research and Target Selection: Phishers often conduct research to identify potential targets. They may focus on specific individuals, organizations, or a broad audience, depending on their objectives.
2) Setup: Phishers set up the infrastructure required to execute their phishing campaign. This includes creating fake websites, email accounts, or other communication channels that resemble legitimate ones.
3) Spoofing: Phishers may use techniques to spoof their identity, making it appear that their communications come from a trusted source. For example, they might use email addresses that look similar to legitimate ones or use domain names that mimic well-known brands.
4) Initial Contact: Phishers initiate contact with the target through various means, such as email, instant messaging, social media, or even phone calls. They will try to gain the target's trust by posing as someone reputable or trustworthy.
5) Pretexting: Phishers use a pretext, such as claiming to be a bank, government agency, IT support, or a reputable company, to create a sense of urgency or importance. They may state that there is a security issue, an account problem, or a limited-time offer to entice the target to respond quickly.
6) Deceptive Message: The message often contains a call to action that prompts the target to take immediate action. This could involve clicking on a link, downloading an attachment, or providing sensitive information.
7) Malicious Link/Attachment and Redirect to Fake Website: In many phishing attempts, the message contains a web link to a fake website that resembles the legitimate one, or it may have an attachment that appears harmless but is actually malware. When the target clicks the link, they are automatically redirected to a fraudulent website that closely mimics the appearance of a legitimate site. The purpose of this fake website is to collect login credentials or personal information when the target enters it.
8) Attacker Collects target information: When the target interacts with the fake website, the phisher captures the entered information, such as login credentials or credit card details.
9) Attacker uses the target credentials: After gathering the desired information, the phisher will use the target credentials to access the real websites.

In addition to the above steps, the attacker will try to cover their tracks and make it difficult for security teams to trace back to them. Sometimes, phishers may use the obtained information for further attacks or sell it on the dark web for financial gain.

Phishing attacks can be simple but also can be highly sophisticated, and phishers continuously evolve their tactics to bypass security measures and exploit human vulnerabilities.

3. TYPES OF PHISHING

Phishing has extended its reach from email to encompass VOIP, SMS, instant messaging, social networking platforms, and even multiplayer games. The following are key phishing categories.

3.1 Clone Phishing

In this type, the phisher starts by creating a cloned email. Then, the attacker sent the same email by getting information such as the content and the recipient's address from a previously sent legitimate email and then replacing the link with a malicious one. The email could include clicking on a link, downloading an attachment, or providing sensitive information like usernames, passwords, or credit card details. Furthermore, email often contains a sense of urgency or a compelling reason to trick the recipient into complying without much suspicion. The attacker also uses address fraud to make recipients feel like they are being sent from the original user. The malicious version is designed to mimic a resend of the original message or an updated version of the original. This technique gains the user's trust by exploiting the social trust associated with inferring the connection as both parties receive the original email. Hence, when users provide sensitive information, they are actually contacting the phishing artists and not the legitimate email sender (Aracindhan,2016). Clone phishing attacks exploit the trust users have in familiar brands or legitimate communication channels, making it difficult for recipients to distinguish between genuine and fraudulent messages or websites (Aracindhan,2016;Cisco Umbrella, 2021).

3.2 Spear Phishing

Spear phishing is a kind of Phishing aimed at a specific group. Therefore, Spear phishing targets specific groups of people who have something in common, such as a group of people from the same organization. Attackers research their victims and craft customized messages to make them appear authentic. The success of spear phishing attacks often relies on social engineering techniques, which exploit human psychology and emotions. The emails may use urgency, fear, or familiarity to manipulate the recipient into bypassing their usual caution and following the attacker's instructions.

Spear phishing attacks can have various objectives, including gaining unauthorized access to systems or networks, stealing sensitive information, conducting financial fraud, or planting malware. The ultimate goal is to compromise the target's security and extract valuable data or exploit their resources. They may use information gathered from social media or other sources to create a sense of familiarity and credibility, increasing the likelihood of success. There are many examples of Spear phishing. For example, in 2016, the Fancy Bear used spear phishing to attack nearly 1,800 Google users linked to Hillary Clinton (Cisco Umbrella, 2021), (The Annual Data Exposure Report, n.d.), (Threat Group-4127, 2016).

3.3 Phone Phishing

Phone phishing is sometimes called “vishing,” Voice phishing. Phone phishing is a form of social engineering attack where an attacker uses phone calls to deceive and manipulate individuals into divulging sensitive information or performing certain actions. It is a method that exploits human trust and relies on persuasive techniques to trick victims.

In a phone phishing attack, the attacker typically poses as a trustworthy entity, such as a representative from a bank, a government agency, a tech support team, or a well-known organization. They may use various tactics to gain the victim's confidence, such as providing false information, creating a sense of urgency, or using intimidation to pressure the victim into complying. The attacker may request sensitive information like usernames, passwords, social security numbers, credit card details, or other personally identifiable information (PII). They try to urge the victim to perform certain actions, such as downloading malicious software, granting remote access to their computer, or making financial transactions.

Attackers use caller ID spoofing during the attacks to enhance their credibility by making it seem like the call originates from a genuine and trusted source. This manipulation of caller ID information makes the attacker appear more convincing and increases the likelihood of their victim falling for deception. They may also have access to some basic information about the victim, making the call seem more credible.

Scammers use a variety of free and open-source tools to “spoof” the number displayed as the caller ID, which makes the phone look legitimate. Also, scammers collect personal data suchas SSNs, dates of birth, addresses, and other information to enhance the caller's legitimacy. Underground sites generally sell such information (Cisco Umbrella, 2021),(The Annual Data Exposure Report, n.d.), (Threat Group-4127, 2016).

4. PHISHING TECHNIQUES

Phishing techniques encompass various methods malicious actors employ to deceive individuals and acquire sensitive information. In this section, we will introduce some of the most common phishing techniques:

4.1 Email/Span

This is a very common phishing technique. Some of the attacks resulted in significant financial losses and reputational damage (The Annual Data Exposure Report, n.d.),(Threat Group-4127, 2016), (Gupta et al.,2020). They send the same emails to millions of users and ask for personal information. Most are disguised as emergency notification emails, asking users to enter information about their accounts to verify or update them. Sometimes, it is the link in the mail that leads the user to the new interface to do this. The fake site is made similar to the original site (Threat Group-4127, 2016). Such fraudulent information often ends up being used to do many illegal things.

4.2 Web-Based Delivery

Web-based delivery is one of the most complex phishing techniques. Phishers track the details of transactions between legitimate websites and users. When a user communicates with a website, the phisher can access information about a user's account through some network technology without the user's knowledge. In a Web-based phishing attack, the attacker creates fraudulent web pages that mimic important websites, such as social network portals, with the intention of deceiving users into divulging their private information, including passwords, social security numbers (SSN), credit card numbers, and other sensitive data(Threat Group-4127, 2016; Gupta et al.,2020).

4.3 Link Manipulation

Manipulation is a technique in which a phisher sends a link to a malicious website. What users see may be a normal site, but if they do click on it, they get the phisher's fake site. The best way to prevent this phishing technique is to let the mouse hover over the link for a while before clicking. If it is a fake website, you can notice some differences before clicking (A. D. Kulkarni et al., 2019; Lyashenko,2019).

4.4 Key loggers

Key-logger combines spyware, a Trojan horse, and a key-logger script (Mao et al., n.d.). The technology works by recording your keystrokes and analyzing them by hackers. Many of today's more formal websites prevent this phishing behavior by adding a soft keypad for mouse clicks (Cisco Umbrella, 2021), (The Annual Data Exposure Report, n.d.), (Threat Group-4127, 2016), (Gupta et al.,2020).

4.5 Trojan

A Trojan horse is malicious software designed to mislead a user through what appears to be a legitimate operation. In practice, however, the software allows unauthorized access to user accounts and collects credentials through the local computer. In the end, the obtained information

is transmitted to the cybercriminals. In spite of the recent anti-virus software, Android still remains vulnerable to attacks by Trojan (Mao et al., n.d.), (Bahjet & Wahab, 2020).

4.6 Malvertising

Malvertising, short for "malicious advertising," refers to the practice of delivering malware through online advertisements. Malvertisements are typically displayed on legitimate websites and can havemany forms, such as banners, pop-ups, or embedded content. The goal of malvertising is to deceive users into clicking on the ads, which then installs the malware on their devices. Malvertisements often exploit web browsers, plugins, or operating systems vulnerabilities to deliver their payload. Once clicked, the ad may redirect users to a malicious website that initiates a drive-by download, automatically installing malware without the user's knowledge or consent. Alternatively, the ad may contain malicious code that directly infects the user's device.

4.7 Session Hijacking

Session hijacking, also known as session stealing or session side jacking, is a type of cyber-attack where an attacker intercepts and takes control of a user's active session on a computer system or a network. This attack typically targets web-based applications or services that rely on session cookies or tokens to maintain user authentication and authorization. During a session hijacking attack, the attacker monitors the network traffic or employs various techniques to capture the victim's session identifier or authentication credentials. This can be achieved through methods such as packet sniffing, man-in-the-middle attacks, or exploiting vulnerabilities in the target system. Once the attacker obtains the session identifier or authentication credentials, they can impersonate the victim and gain unauthorized access to the targeted application or service. This allows them to perform actions on behalf of the victim, potentially including accessing sensitive information, conducting fraudulent transactions, or modifying user settings (Yuan et al.,2018). There are different types of session hijacking attacks, including:

1. Session sniffing: The attacker captures and analyzes network traffic to obtain session information or authentication credentials.
2. Session replay: The attacker intercepts and records a valid session, which they later replay to gain unauthorized access.
3. Session fixation: The attacker tricks the victim into using a session identifier controlled by the attacker, allowing them to hijack the session.
4. Cross-site scripting (XSS): The attacker injects malicious code into a web page, which then steals the victim's session information.
8. Content Injection

Content injection, also known as website defacement or page defacement, is a type of cyber-attack where the attacker gains unauthorized access to a website or web application and modifies its content. The attacker typically replaces or modifies the original content with their own messages, images, or code. The purpose of content injection attacks can vary. Some attackers deface websites to spread their message, promote a political or ideological agenda, or simply vandalize and disrupt the targeted site. Other attackers may inject malicious code or links to redirect users to malicious websites, distribute malware, or steal sensitive information. Content injection attacks can occur due to various vulnerabilities in the targeted website or application, such as unpatched software, weak passwords, insecure file upload mechanisms, or cross-site scripting (XSS) vulnerabilities. The attackers'intent is to exploit these vulnerabilities to gain unauthorized access and manipulate the content.There are different techniques attackers may use for content injection, including:

1. Code injection: The attacker injects malicious code, such as JavaScript or SQL queries, into the website or application to execute their own commands.
2. File inclusion: The attacker exploits insecure file inclusion mechanisms to include external files containing their own content or code.
3. Template manipulation: The attacker alters the website's templates or themes to modify the appearance or content of the site.

4.8 Phishing through Search Engines

Phishing scams through search engines involve search engines. Phishing scams through search engines involve cybercriminals tricking users into visiting malicious websites or disclosing sensitive information by manipulating search engine results. Users are directed to product sites that offer low-cost products or services. When a user tries to purchase the product by entering the credit card information, it is collected by the phishing site (Gupta et al.,2020),(Lyashenko,2019). Phishing through Search Engines typically works as follows:

1. Fake Websites: Scammers create fake websites that resemble legitimate ones, such as popular online banking platforms, e-commerce sites, or social media platforms. These websites are designed to collect users' login credentials or to collect sensitive information such as credit card information.
2. Manipulated Search Results: Scammers use various techniques to manipulate search engine algorithms and push their malicious websites to the top of the search results for specific keywords. They may exploit search engine optimization (SEO) techniques, use compromised websites to redirect traffic or utilize paid advertising campaigns.
3. Deceptive Ads: Phishers may also use deceptive ads or sponsored links that appear alongside legitimate search results. These ads often mimic genuine websites and entice users to click on them, leading to phishing websites or malware downloads.
4. Email Spoofing: Another tactic is to send phishing emails that appear to be legitimate and comingfrom well-known companies or organizations, containing links that direct users to phishing websites. These emails are designed to deceive recipients into revealing sensitive information or downloading malicious attachments.
5. URL Manipulation: Phishers may use URL manipulation techniques to make their malicious websites appear legitimate. They can include common misspellings, subdomains, or additional characters in the URL to trick users into believing they are on a legitimate website.

5. PREVENTION METHODS

Phishing is a prevalent cyber threat that targets individuals and organizations through deceptive tactics aimed at stealing sensitive information. To safeguard against these malicious schemes, it's crucial to implement effective prevention methods. In this section, we will explore various strategies and best practices to help protect individuals and organizations from falling victim to phishing attacks. By understanding and implementing these prevention methods, we can significantly reduce the risk of falling prey to fraudulent schemes and keep your valuable data secure.

5.1 Personal Precautions

This is a way to educate users about the risks and precautions of such attacks. It can enhance users' awareness of prevention (Chorghe et al., 2016). Humans representthe weakest link in the phishing attack. It is critical to educate users to detect and avoid phishing attacks (Rodríguez et al.,2020; KernerS, 2019). According to the study by Tyagi,(2014), weknow that users have a limited understanding of network security terms and their associated risks. For example, in the United States, only 65% of users could correctly explain Phishing. Therefore, instead of telling users the serious consequences of being attacked, it is better to educate users on how to avoid phishing attacks (Rodríguez et al.,2020).

5.2 Enhance Safety Awareness

In the digital world, the urgency and behavior of many people do not reflect a high level of awareness of cyber security (Chou,2004). There are many ways to attract users to phishing websites. The common ones are Browser Based System (BBS), social networking sites, and blogs, which send many tempting information, such as promotions, discounts, lucky draws, and lottery tickets, to lure victims into submitting personal information. Most victims still fill in their personal information online for free services, products or to meet more friends, despite concerns about information security. It shows that users do not pay enough attention to protecting personal information and have a weak sense of security, which provides convenient conditions for illegal

websites. For Phishing, the most effective way to fight is to strengthen personal awareness of prevention, for the first time to reduce the possibility of being cheated. For example, some researchers have developed phishing games to improve safety awareness. Well-designed end-user security education contributes to thwarting phishing threats (Chou,2004), (Butler,2007), (Baral et al.,2019), (de Bruijn&Janssen,2017), (Aloul,2012), (Dodge,2011), (Kumaraguru et al.,2010).

5.3 Distinguish Real and Fake

Phishers disguise themselves as legitimate messages or announcements to confuse users. Fishermen, for example, when they send emails to the victim's email address to do a certain amount of camouflage, especially if some user's email or instant messaging tool is being invaded, fishermen will directly send information to users through the address book or phishing buddy list, so that the recipient will not doubt the security of the source and contents. The most common way is to disguise the URL, which is confusing enough. Without enough knowledge about the structure and the rules for a legitimate URL, it will be difficult to distinguish the fake from the real URL. Of course, there are many ways to identify and review incoming emails. One way is to search for the email address or the message's contents to check for the history of phishing attacks. Another one is noticing the domain name. No matter how realistic fake web pages are, there is a difference between them and real ones. Once found that the domain name has more "suffix" or tampers with "letters," we must be vigilant.

5.4 Manually Enter the URL

The title of a hyperlink could be completely different from the URL it actually points to. Attackers often use this difference by displaying a URL in the link title and a completely different URL behind it. Therefore, to judge the destination address of a hyperlink, the easiest way is to place the mouse over the hyperlink and check the URL displayed in the status bar (Higashino et al.,2019). Or right-click the link andselect the properties. The full Web address will be displayed. However, it is essential to mention that an attacker can also change what is displayed through JavaScript. In this case, the best approach is manually entering the destination URL to ensure you are visiting a legitimate site. As long as the users think they have received a legitimate request (Arachchilage et al.,2014).

5.5 Check the HTTPS:// and Padlock

When a user opens a website, it is necessary to check the URL bar to ensure a secure connection is established through the HTTPS protocol. Move the mouse over the link, do not click, and check if the link starts with HTTPS instead of HTTP. Also, notice that if the padlock icon appears, this indicates that the site has been verified by a third-party security company (A. D. Kulkarni et al., 2019; Higashino et al.,2019).

5.6 Keep software Up To Date

Phishing attacks that use malware usually rely on software errors to place the malware on the user's computer. Once an error is found, the software manufacturer will issue an update to fix it. However, it also means that older software has more open and known bugs, making it possible for more malware to access users' private information through older versions. So, update the systems and install security patches to reduce the risk of malware.

5.7 Real-time Web Protection

Advanced web page protection technology can make an intelligent judgment on the objects accessed by users. The browser can be parsed into specific CSS, JavaScript, and other program code for any web content. Therefore, when the browser parses the target URL, it can judge whether there is phishing harm by verifying whether the code of the target URL and generally phishing websites have something in common. Most web browsers have built-in security features that can help detect and block phishing websites. These features include warnings or alerts when visiting suspicious websites or sites with known phishing activity. Ensure that your browser's security settings are enabled and up to date.

5.8 Anti-spam Technology

Many web-based email providers, such as Yahoo, Hotmail, and Gmail, have their own anti-spam technology (Gupta et al.,2020; Kulkarni et al., 2019; Fatima et al.,2019). They offer anti-phishing extensions or add-ons that provide an extra layer of protection. However, if users don't know how to use this technology, or find that the solution provided by the E-mail provider is ineffective, they can purchase anti-spam software to support their protection. Most antivirus and security suite products have their own professional protection against Phishing (Barracuda,2019; Khonji et al.,2011).

5.9 Password Manager

For most password managers, users can access the safe site using a single click to log in. If the user somehow arrives at a fraudulent site, the password manager will not automatically fill in the saved login information, which is a big red flag. Because the password manager will keep track of the sites to which these passwords belong to. Although fake login pages are deceptive, password managers are not easily tricked. Password managers can generate and securely store unique passwords for each website you use, reducing the risk of falling victim to credential theft.

5.10 Warning Against Attacks

Warnings are generally divided into two methods. (1) Active warnings. The browser will prevent users from viewing malicious content. (2) Passive warning. The browser displays a popup to alert the user, but the content can still be viewed. Studies conducted byMacAfee have shownthat active warnings are more effective because passive warnings are easily ignored most of the time (MacAfee Knowledge Center, n.d., 2022). According to this study, only 13% of participants were able to notice the passive warnings, but 79% of participants were able to pay attention to active warnings. This is the main reason why most security toolbars are ineffective at blocking attacks. However, further studies proposed a new attack to bypass security toolbars and phishing filters via DNS poisoning. Fake DNS cache entries are employed to manipulate the outcomes presented to security toolbars, thereby causing the victim to be presented with deceptive information (Montazer et al.,2015; Moore et al.,2012; Wu et al.,2006; M. Ester et al.,2012).

5.11 Data Mining and Machine Learning

Since Phishing represents a common classification challenge, leveraging Machine Learning (ML) and Data Mining (DM) techniques to analyze website features can effectively help combat the issue (Tran, T., et al., 2022). The process involves comparing phishing websites to similar ones and extracting relevant characteristics from URLs and keywords. By employing data mining methods, it becomes possible to scrutinize vast amounts of web data and discover patterns associated with phishing websites(Peng &Sawa, (2018).

Data mining algorithms focus on various aspects, including URL structure, content, HTML tags, and website behavior, enabling them to discern between legitimate and malicious sites. For instance, the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm was utilized to detect similarity between phishing websites and target websites, effectively identifying those at high risk. DB-SCAN uses density (e.g., Euclidean distance) to partition data without requiring the number of clusters in advance(Ester, et al.,2012).Altaher et al., (2017) proposed a hybrid approach for classifying websites as Phishing, Legitimate or Suspicious. The proposed approach combined the K-nearest neighbors (KNN) algorithm with the support vector machine algorithm (SVM). The proposed approach fuses the effectiveness and simplicity of KNN with the power of SVM. In 2011, Radha & Valarmathi used Particle Swarm Optimization (PSO) for Phishing Website Detection (Radha & Valarmathi, (2011).The Particle Swarm Optimization (PSO) method is employed in conjunction with an associative classification algorithm to detect phishing websites in the e-banking sector. This combination has demonstrated superior performance compared to current classification algorithms, exhibiting improved prediction accuracy and a reduced error rate (Radha & Valarmathi, (2011).

In addition, the k-nearest neighbors (k-NN) algorithm utilizes multi-dimensional vectors to store training instances, with each vector component representing a specific feature value (e.g., the

number of URLs in an email). During classification, testing instances are processed similarly, and their distances (e.g., Euclidean distance) to the training instances are calculated. When k equals 3, the classes of the three nearest neighbors from the training phase are considered, and majority voting determines the testing instance's class. In contrast, algorithms like C4.5 and SVM generalize classification models. C4.5 constructs decision trees to accurately classify unseen instances, optimizing Information Gain for splitting. SVM finds a generic separation plane in a vector space for both training and unseen data. Clustering algorithms like k-means and DB-SCAN partition data without class labels. K-means form partitions iteratively by selecting initial centers and assigning instances to the nearest center, updating centers until convergence (Kunju et al., 2019).

Finally, data mining proves helpful in analyzing email headers, content, and attachments to uncover phishing indicators like suspicious URLs, email spoofing, or phishing email templates.This comprehensive approach strengthens defenses against phishing attempts and enhances overall cybersecurity measures. These techniques can help in building email filters or warning systems to detect and flag potential phishing emails (Sahoo,2018; Aburrous et al.,2009; Sahingoz et al., 2019).

6. ANTI-PHISHING POPULAR TOOLS

The following is a brief discussion of a few of the popular anti-phishing tools:

6.1 Google SafeBrowsing

Safe browsing was introduced in 2007 to protect users on the Web from phishing attacks (Aburrous et al.,2009). The goal is to protect users from malware and web-based threats that rely on desktop and mobile platforms. When users try to navigate to a dangerous website or download a dangerous file, a warning will be displayed to remind users.Web browsers like Google Chrome, Safari, and Firefox integrate Google Safe Browsing technology to warn users about potentially harmful sites before they click on them in search results or visit them directly.

6.2 McAfee SiteAdvisor

McAfee SiteAdvisor is a browser extension developed by cybersecurity firm McAfee to help users navigate the internet safely. The tool aids in identifying and avoiding potentially harmful websites that may harbor malware or engage in phishing scams. It provides safety ratings for websites, distinguishing them with green checkmarks for safe sites and red marks for dangerous ones, directly in the search results. Additionally, it offers real-time scanning of websites to prevent interaction with hazardous content, and scrutinizes downloads for malware, alerting users to any detected threats. This combination of features works to protect users from a variety of online threats, fostering a more secure browsing experience.(Vanita McAfee® WebAdvisor, n.d.).

6.3 Cloudmark

Cloudmark Security Platform is a high-performance mail security solution (Cloudmark et al. for Email, n.d., 2023). Cloudmark Security Platform is a comprehensive email security solution provided by Cloudmark, a company specializing in messaging security. The new platform was designed to protect organizations from various email-based threats, including phishing attacks, spam, malware, and other forms of abuse.

6.4 PhishGuard

When the tool detects that the user will submit the ID and password, it triggers the action. PhishGuard always repeats some bad passwords first and judges that if there is no phishing attack, it will forward the real user ID to the page. The page may be legitimate if there are no phishing attacks, and the HTTP status code is 401. Otherwise, when the HTTP status code is 200, the page is considered a phishing site (PishGuard, n.d., 2016).

6.5 Phishwish

Phishwish is an anti-phishing filter that works without the need for training (Likarish et al.,2008). It also uses a white or blacklists to decide whether an email is suspect. By analyzing the email

headers and URLs in emails, Phishwish can determine the email's legitimacy according to 11 rules. There is a score calculated based on a weighted average of 11 rules. If the score exceeds 50%, then this email is considered phishing (Likarish et al.,2008).

7. DISCUSSION AND THE COST OF PHISHING

As per the IBM Security 2022 report (IBM Security, 2022)on the Cost of a Data Breach, the leading cause of data breaches is the utilization of stolen or compromised credentials. In the 2022 study, stolen or compromised credentials accounted for 19% of breaches, making it the primary attack method. This trend was consistent with the 2021 study, where it caused 20% of breaches, holding the top position. On average, breaches resulting from stolen or compromised credentials cost $4.50 million. These breaches also had the longest duration, taking approximately 243 days to identify the breach and an additional 84 days to contain it. Phishing emerged as the second most common cause of breaches, contributing to 16% of incidents. Furthermore, it had the highest average cost of $4.91 million in breach-related expenses, as reported by many sources (Gupta et al.,2016; Alsharnouby,2015; IBM Security, 2023).

Phishing attacks have surged to unprecedented levels, particularly with the emergence of technologies such as mobile devices and social media (Marforio et al., 2015). For example, between 2017 and 2020, there was a substantial increase in phishing attacks, rising from 72% to 86% among businesses in the United Kingdom. Notably, many of these attacks originated from social media platforms (GOV.UK, 2020).

Furthermore, In 2022, the frequency of phishing attacks escalated dramatically, setting new records with the APWG reporting over 4.7 million incidents, reflecting an annual increase of more than 150% since 2019. In October of that year, an all-time high was reached, with 101,104 unique phishing email subjects being identified, illustrating the peak of this trend. The last quarter saw a slight uptick from the previous record quarter, tallying 1,350,037 cases. Notably, the financial sector became a prominent target, encompassing about 28% of all attacks, while enterprises continued to grapple with Business Email Compromise (BEC) attacks that, on average, sought to siphon off $132,559 in each attempt(APWG, 2022).

In addition, APWG reported a persistent focus on phishing attacks in the financial sector. For example, phishing campaigns targeting banks,constitute 27.7% of all attacks, a rise from 23.2% in the third quarter of 2022. Following in frequency were attacks against webmail and Software-as-a-Service (SaaS) providers at 17.7%, albeit showing a slight decrease from the previous quarter. Payment processors like PayPal, Venmo, and VISA were targeted in 6% of the attacks. Meanwhile, the rate of phishing against social media platforms varied, peaking at 15.5% in the second quarter of 2022 before decreasing, while attacks on cryptocurrency entities, such as exchanges and wallet providers, reduced to 2.3% by the end of the year amid a decline in market values. Matthew Harris, the Senior Product Manager of Fraud at OpSec Security, highlighted a significant uptick in fraud within the logistics and shipping industry, particularly targeting the U.S. Postal Service, and noted a surge of over 40% in vishing incidents detected via mobile phones in the fourth quarter compared to the third APWG, 2022).

In addition, cybercriminals consistently exploit disasters and major events for their own gain. With the onset of the COVID-19 crisis, a wide array of phishing and malware attacks with themes related to the pandemic were launched by malicious actors, targeting not only workers but also healthcare facilities and the general public. According to a report by Microsoft (Microsoft, 2020), cyberattacks linked to COVID-19 reached an unprecedented peak in March, with the majority of these scams involving fake COVID-19 websites, as reported by the security company RiskIQ (RISKIQ, 2020).

People rely more on technology as more online services and more personal data are stored digitally. However, at the same time, such safety incidents are becoming more frequent and intractable (Likarish et al.,2008; Cook et al.,2008; Gupta et al.,2016). However, whenever the researchers devised a new strategy, the phishers used the holes in the strategy to change their

attack ways (Cook et al.,2008; Alsharnouby,2015). So how to identify and defend against phishing attacks continues to be the most challenging facing network security. An eye-tracking experiment shows that when judging whether a website is legal, users only spend 6% of the time looking at the security index and 85% of the time looking at the webpage content (Jansen et al.,2019).Therefore, in many cases, technology alone is not enough to avoid phishing attacks. For users, the simplest and most effective way is to enhance their awareness of prevention and understand the basic technical means of prevention to reduce the possibility of being cheated from the root.

There are several studies on the effectiveness of anti-phishing tools currently used. For example, in 2021, Wosah and Win conducted a survey in which they examined various existing tools used to mitigate email and website Phishing for the purpose of detection. Their findings ultimately revealed that current solutions have limited success in aiding email users in distinguishing phishing emails from legitimate ones, (Wosah, N. P.;& Win, T., 2021).In 2021, Jain AK and Gupta BB conducted a study that highlighted the performance difficulties encountered by developers when addressing this critical attack. Furthermore, their research delved into the repercussions of phishing attacks in emerging domains such as mobile and online social networks (Jain et al., 2021).

The majority of the conducted studies reviewed concluded that, while these tools are generally useful, they are also limited in scope, and all have weaknesses. The security indicators generated by these tools are within the context of specific types of Phishing. Furthermore, phishing attacks continue to evolve, and targeted attacks are more widespread. The need for more active and visual indicators and cues needs to be provided to users. Indicators and cues should be clear and easy to understand by users.

8. CONCLUSION & FUTURE WORK

Phishing continues to be a challenging and evolving problem. Many solutions are being deployed, but the fact is that, with every solution introduced to overcome these attacks, phishers are always ready to find new vulnerabilities and devise new attacks.Based on our literature review, it's clear that the existing solutions have not successfully reduced phishing attacks as anticipated. This failure can be attributed to the fact that the human security vulnerabilities exploited by phishers have not been adequately addressed with user-friendly methods to identify phishing emails. Regular internet users often lack awareness about the initiation of phishing attacks and struggle to visually distinguish between illegitimate and legitimate websites, resulting in their susceptibility to such attacks.

We need to devise and design tools and countermeasures to enhance user awareness of prevention. We also need to help users understand the necessary technical means of prevention to reduce the possibility of being cheated from the root. The research community accepted that the first line of defense in protecting people from phishing attacks is understanding the dynamics of Phishingand the psychology of both the phisher and the victim, and analyzing users' decision-making strategies in reaction to phishing attacks. We also found that studying the variance in vulnerability to Phishing and the reasons behind it is a much under-researched area. Our research is currently focusing on understanding people's online behavior. The answer to the question, "Whydo some people fall for phishing while others do not?" continues evolving. We believe this issue is as critical as deploying new tools, and more research needs to be directed toward this issue.

Furthermore, a holistic approach to combat Phishing requires a deep understanding of the human factor, technology factor, and organizational factor. In cybersecurity, humans are considered the "weakest link" when it comes to protecting information. It is imperative to streamline the procedures for recognizing and uncovering phishing attacks, making them accessible to all users irrespective of their technical proficiency.

Finally, to combat the dangers of Phishing, it is crucial to educate individuals about phishing

techniques, promote awareness of safe online practices, and employ robust technical solutions, including email filters, anti-phishing software, and multi-factor authentication, to mitigate the risks associated with these attacks.

9. REFERENCES

APWG (2022). APWG Phishing Activity Trends Reports (2022) anti-phishing work Group, IncAvailable at: https://apwg.org/trendsreports/ (Accessed Aug.. 20, 2023).

Arun Kulkarni and Leonard L. Brown III, (2019).“Phishing Websites Detection using Machine Learning”*International Journal of Advanced Computer Science and Applications (IJACSA),* 10(7).

Abu-Nimeh, S., & Nair, S. (2008). Bypassing security toolbars and phishing filters via dns poisoning. *In IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference* (pp. 1-6).

Aburrous, M. R., Hossain, A., Dahal, K., & Thabatah, F. (2009). Modelling intelligent phishing detection system for e-banking using fuzzy data mining*. In 2009 International Conference on CyberWorlds (pp. 265-272).*

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology,* 3(3), 176-183.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why Phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*,82, 69- 82. doi:10.1016/j.ijhcs.2015.05.005

Altaher, A. (2017). Phishing Websites Classification using Hybrid SVM and KNN Approach. *International Journal of Advanced Computer Science and Applications(IJACSA),* 8(6), 2017.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.

Bahjet, H., & Wahab, A. (2020). Detect and prevent Phishing based on hybrid approach. *AL-Mansour Journal,* 33, 1– 25..

Baral, G., & Arachchilage, N. A. G. (2019). Building confidence not to be phished through a gamified approach: conceptualizing user's self-efficacy in phishing threat avoidance behavior*. In 2019*
*cybersecurity and cyber forensics conference (CC*C), (pp. 102-110).

Binks, A. (2019). The art of Phishing: past, present and future. *Computer Fraud & Security*, 2019(4), 9-11.

Butler, R. (2007). A framework of anti□phishing measures aimed at protecting the online consumer's identity. *The Electronic Librar*y, Volume 25, Number 5, 2007, pp. 517-533(17). Emerald Group Publishing Limited. DOI: https://doi.org/10.1108/02640470710829514

Barracuda Enterprise Email Security Q2 (2019). Staying Safe from Phishing Attacks. https://blog.lastpass.com/2016/01/staying-safe-from-phishing-attacks.html/

Code42: The Annual Data Exposure Report: 2023 (2023). https://www.code42.com/resources/reports/2023-data-exposure? (Accessed, May 2023).
Chorghe, S.P., Shekokar, N. (2016). A survey on anti-phishing techniques in mobile phones. *In: 2016 International Conference on Inventive Computation Technologies (ICICT*), pp. 1–5.

Chou, N., Ledesma, R., Teraguchi, Y., & Mitchell, J.C. (2004). Client-Side Defense Against Web-

Based Identity Theft. *Network and Distributed System Security Symposium*.

Cisco Umbrella. (2021). "Cybersecurity threat trends: phishing, crypto top the list," https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.

Cloudmark Security Platform for Email, (2023). https://www.cloudmark.com/en/products/email-messaging-security/cloudmark-platform-for-email

Cook DL, Gurbani VK, Daniluk M. (2008). Phishwish: a stateless phishing filter using minimal rules. In: Tsudik G (ed) Financial cryptography and data security. Springer, Berlin, pp 182–186.

Danuvasin, C. (2011). Phishing: A field experiment. *International Journal of Computer Science and Security* (IJCSS),5(2), 277–286.

Debra L. Cook, Vijay K. Gurbani, Michael Daniluk. (2008). Phishwish: A Stateless Phishing Filter Using Minimal Rules Financial Cryptography and Data Security, 2008, Volume 5143 ISBN: 978-3-540-85229-2.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1-7.

Dodge, R., Rovira, E., Zachary, R., & Joseph, S. (2011). Phishing awareness exercises. *In Proc. of the 15th colloquium for Information Systems Security Education* (pp. 13–15).

Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security*, 27(6), 581-612.

G. Tyagi, K. Ahmad and M. N. Doja (2014). "A novel framework for password securing system from key-logger spyware," *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Ghaziabad, India, 2014, pp. 70-74, doi: 10.1109/ICICICT.2014.6781255.

GOV.UK (2020). Cyber security breaches survey 2020. Available at: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020 (Accessed June13, 2022).

Gupta, B. B., & Jain, A. K. (2020). Phishing attack detection using a search engine and heuristics-based technique. *Journal of Information Technology Research (JITR),* 13(2), 94– 109.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*,28(12), 3629- 3654. doi:10.1007/s00521-016-2275-y.

H. Yuan, X. Chen, Y. Li, Z. Yang and W. Liu.(2018). "Detecting Phishing Websites and Targets Based on URLs and Webpage Links," *2018 24th International Conference on Pattern Recognition (ICPR)*, Beijing, China, 2018, pp. 3669-3674, doi: 10.1109/ICPR.2018.8546262.

Higashino, M., Kawato, T., Ohmori, M., & Kawamura, T. (2019). An anti-phishing training system for security awareness and education considering prevention of information leakage. In 2019 5th international conference on information management (ICIM) (pp. 82-86).

IBM Security Report, (2022). Cost of a data breach 2022 A million-dollar race to detect and respond (2023). Retrieved from https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268688&p5=p&gclid=Cj0KCQjwyLGjBhDKARIsAFRNgW_W00uTBdSfBw-sB_2DeqQU-gM80Pld30mzor2HfXNRCZszDLyiYBgaAuW8EALw_wcB&gclsrc=aw.ds.

Jain AK, Gupta BB, (2021). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterp Inf Syst.* 2022;16(4):527–565.

J. Mao, W. Tian, P. Li, T. Wei and Z. Liang.(n.d.). "Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity," *in IEEE Access,* vol. 5, pp. 17020-17030, 2017, doi: 10.1109/ACCESS.2017.2743528.

Jansen, J., & Schaik, P. V. (2019). The design and evaluation of a theory-based intervention to promote security behavior against Phishing. *International Journal of Human-Computer Studies*,123, 40-55.

Kerner, S. M. (2019). Phishing Attacks Continue to Rise, Proofpoint Reports. *EWeek, N.PAG.*

Khonji, M., Jones, A., & Iraqi, Y. (2011). A novel phishing classification based on url features. *In 2011 IEEE GCC conference and exhibition (GCC)* (pp. 221-224).

Kirda, E., & Kruegel, C. (2006). Protecting users against phishing attacks. *The Computer Journal*, 49(5), 554-561.

Kunju M.V., Esther D., Anthony H. C. &BhelwaS. (2019). "Evaluation of Phishing Techniques Based on Machine Learning," *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, Madurai, India, 2019, pp. 963-968, doi: 10.1109/ICCS45141.2019.9065639.

MacAfee Knowledge Center. (2022). How to recognize and protect yourself from Phishing. https://service.mcafee.com/webcenter/portal/cp/home/articleview?locale=en-US&articleId=TS101810

Marforio, C., Masti, R. J., Soriente, C., Kostiainen, K., and Capkun, S. (2015). Personalized security indicators to detect application phishing attacks in mobile platforms. Available at: http://arxiv.org/abs/1502.06824.

Microsoft (2020). Exploiting a crisis: how cybercriminals behaved during the outbreak. Available at: https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/ (Accessed May 21, 2022).

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT),* 10(2), 1-31.

Likarish P, Dunbar D, Hansen TE. (2008). Phishguard: a browser plug-in for protection from Phishing. *In: 2nd International Conference on Internet multimedia services architecture and applications*, IMSAA, Bangalore, India, pp 1– 6.

Liu G, Qiu B, Wenyin L. (2010). Automatic detection of phishing target from phishing webpage. *In: Pattern recognition (ICPR), 2010 20th international conference*, Istanbul, Turkey, Aug 2010, pp 4153–4156

M. Khonji, Y. Iraqi and A. Jones, (2023). "Phishing Detection: A Literature Survey," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091-2121, Fourth Quarter 2013, doi: 10.1109/SURV.2013.032213.00009.

M. Ester, et al.(2012). "A density-based algorithm for discovering clusters in large spatial databases with noise," in Kdd, 1996, pp. 226-231. Purkait, S. Phishing countermeasures and their effectiveness–literature review. *Information Management & Computer Security*, 20(5), 382-420.

Montazer, G. A., & ArabYarmohammadi, S. (2015). Detection of phishing attacks in Iranian e-banking using a fuzzy–rough hybrid system. *Applied Soft Computing*, 35, 482-492.

Moore, T., & Clayton, R. (2012). Discovering phishing dropboxes using email metadata. *In 2012 eCrime Researchers Summit (pp. 1-9)*.

Peng T., Harris I., &Sawa Y. (2018). "Detecting Phishing Attacks Using Natural Language Processing and Machine Learning*," 2018 IEEE 12th International Conference on Semantic Computing (ICSC)*, Laguna Hills, CA, USA, 2018, pp. 300-301, doi: 10.1109/ICSC.2018.00056.

PishGuard.A comprehensive phishing simulation solution(n.d.). https://cerebra.sa/products/phishguard/.

Radha Damodaram,M.L.Valarmathi, (2011). Phishing Website Detection Using Particle Swarm Optimization Technique. *International Journal of Computer Science and Security (IJCSS),* 5(5), PP 477 - 490

R. Aravindhan, R. Shanmugalakshmi, K. Ramya and Selvan C., "Certain investigation on web application security: Phishing detection and phishing target discovery," (2016). *3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2016, pp. 1-10, doi: 10.1109/ICACCS.2016.7586405.

RISKIQ (2020). InvestigateCOVID-19 cybercrime weekly update. Available at: https://www.riskiq.com/blog/analyst/covid19-cybercrime-update/%0D (Accessed Feb6, 2023).

Rodríguez, G., Torres, J., Flores, P., Benavides, E., & Proaño, P. (2020). Trusted Phishing: A Model to Teach Computer Security Through the Theft of Cookies. *In Advances in Emerging Trends and Technologies: Volume 2 (pp. 390-401).* Springer International Publishing.

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning-based phishing detection from URLs. *Expert Systems with Applications*, 117, 345-357.

Sahoo, P. K. (2018). Data mining a way to solve Phishing Attacks. *In 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)* (pp. 1-5).

Threat Group-4127 Targets Google Accounts(2016). https://www.secureworks.com/research/threat-group-4127-targets-google-accountsIBM security.

Vanita McAfee® WebAdvisor. (n.d.). https://www.mcafee.com/consumer/en-us/store/m0/catalog/mwad_528/mcafee-web-advisor.html (Accessed, May 2023).

V. Lyashenko, O. Kobylin and M. Minenko, "Tools for Investigating the Phishing Attacks Dynamics," (2018).*International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T*), Kharkiv, Ukraine, 2018, pp. 43-46, doi: 10.1109/INFOCOMMST.2018.8632100.

Wosah, N. P., & Win, T. (2021). Phishing mitigation techniques: A literature survey. *International Journal of Network Security & Its Applications (IJNSA)* Vol.13, No.2, March 2021

Wu M, Miller RC, Garfinkel SL.(2006). Do security toolbars actually prevent phishing attacks? *In: Proceedings of the SIGCHI conference on human factors in computing systems*, ser. CHI'06, New York, NY, USA, pp 601–610.