A Critical Review: Revisiting Phishing Attacks Classification and Analysis of Techniques Employed in Taxonomies

Riyadh Rahef Nuiaa
College of Education for Pure Sciences, Wasit University, Iraq
riyadh@uowasit.edu.iq
Selvakumar Manickam (✉)
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Malaysia
selva@usm.my

Abstract— People are increasingly sharing their personal information online as internet usage grows. As a result, fraudsters have access to a massive amount of personal information and financial activities. In recent years, phishing assaults have become one of the most common threats faced by internet users, governments, and service providers. The attacker(s) uses falsified emails or bogus websites to obtain the client's sensitive data (i.e., user account login details, credit/debit card numbers, etc.) in a phishing assault. Studies have classed phishing attacks based on fundamental phishing mechanisms and defenses, ignoring the importance of the phishing lifecycle from beginning to conclusion. This study also provides a new thorough taxonomy of phishing assaults, including attack phases, attacker types, vulnerabilities, threats, targets, attack media, and attacking strategies. Furthermore, the proposed anatomy will help readers comprehend the full lifecycle of a phishing attack, which will raise awareness of these phishing attacks and the strategies utilized; it will also aid in the development of a comprehensive anti-phishing system. In addition, various preventative precautions are being investigated.

Keywords—Cybersecurity, Phishing Attacks, Internet security, Information security, Phishing Attack Taxonomy.

1 Introduction

The world of technology continues to grow and develop, as are hackers who have depended on the unlawful use of digital data, especially private data, to cause harm to people. 'Identity theft' is arguably the most dangerous crime for anyone who uses the Internet, as it involves a criminal impersonating a person with the goal to steal and use their private information (i.e., financial data, their social security number, or credit card details, etc.) for the assailant's personal gain as well as for stealing money but also for committing other crimes [1].

Cyber Security refers to the process of defending cyberspace from threats [2]. Cyber security is all about safeguarding, preventing, and recovering all internet-connected resources from cyber-attacks[3]. The complexity of the cybersecurity domain grows by the day, making recognizing, assessing, and controlling important risk events difficult.

Cyberattacks are malicious digital attempts to steal, destroy, or infiltrate personal or corporate secret data[4].

Phishing is a method of fraudulently acquiring sensitive information. Phishing is a combination of social engineering and technical exploitations that is intended to compel a victim to divulge personal information. The majority of phishing attempts are carried out via bogus emails containing an unified resource locator (URL). When activated, such a URL leads to a phony harmful Web site [5][6]. Phishing is currently one of the most severe Internet security problems. In this attack, the user submits sensitive credentials such as credit card information, passwords, etc., on a website that appears to be genuine but is actually fraudulent [7]. Figure 1 presents the growth of phishing attacks during the period from the fourth quarter of 2021 into the third quarter of the year 2022.

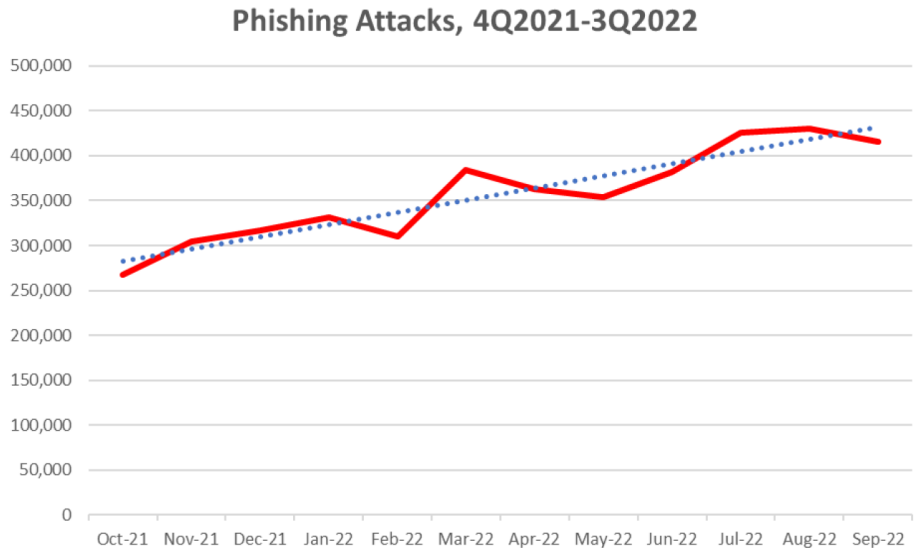

Fig. 1. depicts the increase in phishing attacks through the third quarter of 2022 [8].

The increase in Q3 2022 is due in part to an increase in the number of attacks reported against a variety of specific targets. These targets were subjected to a considerable number of phishing attacks[8].

2 Phishing Life Cycle

When an end user hits the fraudulent webpage and inputs their own private data, the attacker has the ability to access the aforementioned data. Furthermore, the assailants exploit this data for both private and monetary advantage [9][10]. Figure 2 displays the entire life cycle following a phishing attack. A phishing assault consists of the following stages:

Initially, the hacker creates a bogus website that resembles a legitimate one. To deceive users, the scammer attempts to maintain the apparent resemblance between the fake website and the genuine website when constructing the bogus website. Second, the scammer sends the selected victim an email with an URL link to the fraudulent website. Third, when the target reads the sent message as well as interacts with the fraudulent link, he is transported to the fraudulent website, and there he has to give his private data. For example, if the scammer has set up a phishing website that purports to be that of a bank, the person being targeted will be asked to input the details of their bank account. Fourth, the scammer acquires the necessary information promptly when the targeted individual enters their personal details on the fraudulent website. This information may be used for financial or other gains by the phisher.

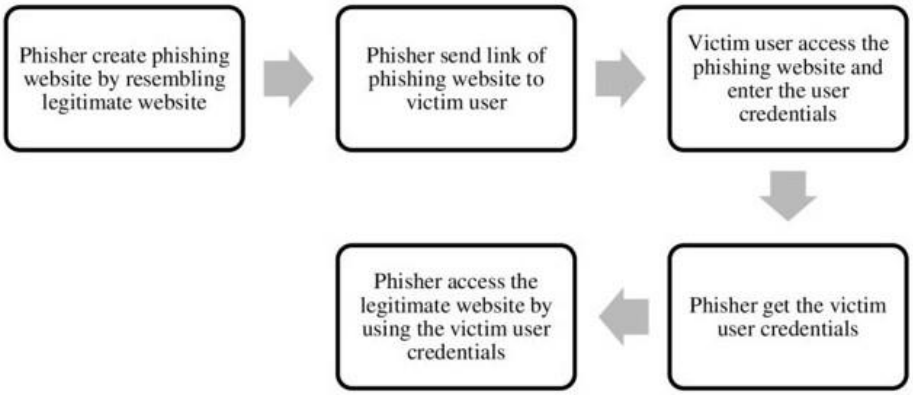

Fig. 2. phishing life cycle cited from [11].

3 Related Works

According to [12], this study provides a novel method to distinguish phishing assaults through the examination of URLs in the HTML coding of a web page. The suggested technique divides hyperlink-specific properties into twelve distinct groups and utilizes these attributes to teaching machine learning techniques. Compared to other methods, the suggested solution has a comparatively high detection rate for phishing websites, as its logistic regression classifier obtained over 98.4% accuracy. This approach uses logistic regression (LR) as a supervised machine learning algorithm.

According to [13],the objective of this project is to construct a machine learning-based phishing detection system that allows users to assess the authenticity and maliciousness of a URL in the shortest time possible. By developing a method capable of extracting feature vectors from the URL every time a user visits that URL. Then, the feature vectors are preprocessed and sent to a number of machine learning algorithms to check if a URL is real.

According to [14], Using binary visualization and machine learning, the authors of this research offer a novel method for preventing phishing assaults. In contrast to prior research in this sector, their method employs a computerized identification procedure

and does not need any additional input from the client. Hence enabling a faster and more accurate detection process. Combining scamming with machine learning and recognition of pictures enables clients to enter previously obscure dubious web pages as well as obtain a deeper grasp of potential menace in a faster manner. The primary aspect of this research is the automatic detection of websites that are phishing automatically. Since the method doesn't require verification from more than one user, the blacklisting process can be done faster, making it easier for potential targets to get to the URL web page.

According to [9], They have suggested a novel method for preventing phishing attempts using an automatically-updated whitelist of authorized sites that the user can view. A whitelist is a collection of authorized domains or URLs. A white list is comprised of the sites that the user intends to access and are legitimate. A black list, on the other hand, provides information about sites that the user does not desire to access since they are fraudulent. In addition, the white-list data is smaller and more accurate than the black-list data. Listed below are the key contributions of their method:

- A viable and real-time solution for protecting users from phishing assaults on client sites is proposed.
- Discovering scams by examining a single significant feature (i.e., links located on the website)
- Discovering zero-hour scamming with no training required.
- DNS assaults are also detected by matching the potential attacker's website's IP address to Google Open DNS.

According to [15], They've suggested a novel ensemble approach for detecting phishing assaults via websites. A scamming web pages dataset containing 30 attributes is used to build the approach, and 10-fold cross-validation is performed to assess efficiency. They employ an innovative ensemble approach to identify phishing assaults on the web page since ensemble approaches have historically demonstrated superior performance. They've utilized a voting model to combine two RFC-based classifiers with ANN, KNN, and C4.5 classification algorithms. All methods are implemented with a maximum number of batches of 100, and 10-fold cross-validation is performed to determine the classifier's efficacy.

According to [16], the article introduces a novel technique for detecting phishing webpages regardless of their language. While many current anti-phishing approaches are limited to identifying fraudulent English-language webpages, this new method uses a search engine-based approach that employs a lightweight and language-independent query to assess the legitimacy of suspicious URLs. The proposed technique also incorporates five heuristics to improve detection accuracy, particularly for newly established legitimate sites that may not yet be indexed by search engines. According to the evaluation results, the proposed method significantly outperforms existing search-based approaches, exhibiting a 98.15% true positive rate and a mere 0.05% false positive rate.
According to [17] This article discusses the problem of phishing attacks on social networks, particularly Twitter, and the limitations of current detection methods that use machine learning. The authors propose a three-step approach to improve the detection

and analysis of phishing attacks on Twitter, which can be extended to other social networks. The first step involves searching a "Blacklist" database for suspicious URLs, followed by a URL analysis step that uses machine learning techniques and introduces new features. Three classifiers (Regression Logistics, SVM, and Random Forest) are used in this step. The third step involves analyzing Twitter accounts using user-related features to detect malicious users responsible for the phishing attacks. The authors test their system on real data and develop an application for end-users.

4 Taxonomy of Phishing Attacks

Phishing schemes can be perpetrated through technical deception and social engineering. "Spoofed" emails are used by social engineering techniques to direct consumers to bogus websites [18]. Phishing URLs can also be disseminated via Internet Relay Chat (IRC), instant messaging (IM), forums, and blogs, among other channels. The scammers send the same email to tens of thousands of people, requesting personal information [9]. Some of the most prevalent phishing attacks designed to deceive Internet users are described in Figure 3:

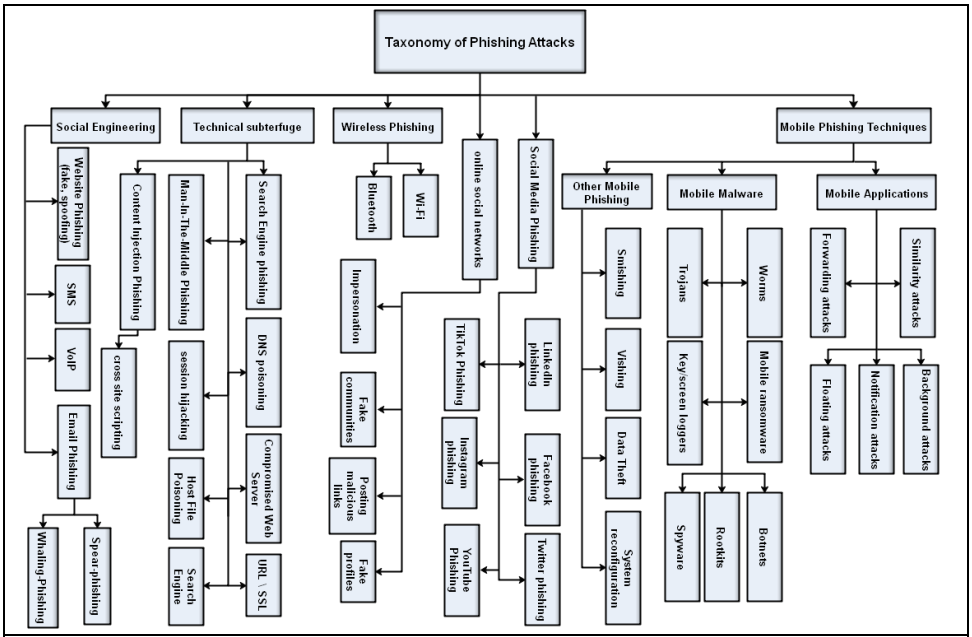

Fig. 3. depicts the increase in phishing attacks through

4.1 Social Engineering Phishing Attack

This type of phishing attack is based on the manipulation of human vulnerabilities to achieve a malicious objective. Therefore, it is complex because they utilize vulnerabilities in people that cannot be readily secured automatically [19]. These types of attacks can be used in a variety of methods to trick individuals into divulging their information. It employs social engineering techniques and cleverly arranged tactics to entice users into providing data. The lure can be sent via text message, phone, or forged email. Phishers post fraudulent emails to millions of internet users in the hopes that at least a few will fall for them. People are the most vulnerable component of an organization, so social engineering is highly effective [20]. There are two famous types of phishing attacks that can be categorized as:

- Website phishing (fake / spoofing): This is also known as websites spoofing, in which phishers create a website that appears authentic and resembles a reputable website[21]. Unsuspecting users are directed to this website after clicking a hyperlink inside a mail message, advertising, or other sources (clickjacking). If the client continues to connect with the counterfeit website, the phisher will divulge and harvest sensitive information[22][23].
- Email phishing: A scam or counterfeit email is a fraudulent email distributed at random to thousands of recipients from an untrustworthy provider. Spear phishing refers to phishing emails that are more coordinated and that target a specific group of individuals inside the same organization. This remains the most prevalent form of phishing to this day [24][25]. This type of phishing attack can be classified into two types:
    - ❖ Spear phishing: Although equivalent to "phishing," spear phishing is a strategy that fraudulently acquires private information by delivering highly personalized emails to a small number of end users[26]. It is the primary distinction between phishing assaults and spear phishing attacks, since spear phishing efforts rely on sending out large quantities of generic emails with the assumption that only a small number of recipients will react. In contrast, spear phishing emails necessitate further research on the part of the attacker in order to "trick" the target[27].
    - ❖ Whaling phishing: Finding for information and data pertaining to senior positions using emails or websites disguised as court notifications, consumer complaints, or other business-related difficulties[28][29].

4.2 Technical Subterfuge Phishing Attack

This type of phishing attack deceives victims into divulging confidential data by installing harmful software inside the target's machine [25]. This type of phishing attack can be categorized into nine types:

- Search engine phishing: at this scamming strategy, the scammer establishes fraudulent websites with enticing offers and uses Search Engine Optimization (SEO) techniques to have them ranked lawfully so that they appear when a user searches for a product[16]. A search through a search engine leads people to these fraudulent websites, where they may provide personal information while assuming they are on a legitimate site[16]. There are black-hat search engine optimization packages available that can rapidly boost the search engine rankings of a fraudulent website. However, due to the time lag between when a website is established and when it is accessed, this is often used to send consumers to harmful websites [30].
- DNS poisoning: In this type of phishing attack, the phisher uses a spoof DNS server to redirect Internet traffic away from the legitimate website and towards malicious sites. As a consequence, the attacker takes control of the DNS server and modifies the DNS cache [31]. When a cache is tainted, the data is transferred to the spoof URL. The phisher lures the client into communicating with it, and once the victim connects, he or she is redirected to malicious websites, or malware may be installed on their systems [32].
- Compromised web server: In this type of phishing attack, the attackers seek weak servers and install a backdoor or secret exit that allows them to gain access to a compromised web server via an encrypted backdoor. The victim downloads phishing websites, which then begin to receive traffic and provide access to malicious content [18].
- URL/SLL: this
- Host file poisoning: This kind of phishing attack involves injecting new entries for webpages into a machine's host file, thereby redirecting the websites to a different location. When an end-user provides a URL, it gets converted into an IP address before sending it through the Internet; fraudsters have falsified addresses transmitted by altering host files and redirecting the end user to a fake web page where private data is required [18][33].
- Session hijacking: this kind of phishing attack is a prevalent and grave issue in WLAN. This is also known as hijacking data. DoS attacks are used to take the session key in order to steal the user's identity and gain unauthorized access to the system's resources. The assailant forces the mobile station to disconnect from a specific access point [34].
- The Man in The Middle phishing attack (MITM): This type of scamming occurs when the scammers introduce communications between both parties (i.e., the client and the legal website) and attempt to intercept the victim's communications in order to obtain information from both parties. In this form of phishing attack, the phishers intervene between the target and the genuine website. The perpetrator receives the data submitted to the legitimate website, which may include credit card information or other personal data. Therefore, the user's transaction is not compromised[35][25].
- Content-Injection phishing: this type of attack, which happens when inserting fraudulent content into a legitimate website, is referred to as phishing. This malicious content might misdirect a client to false websites, resulting

in the disclosure of sensitive information to the hacker, or it could result in the user's device being infected with malware [31][25]. The most famous type of this attack is:

- ❖ Cross site scripting: these types of assaults are a particularly prevalent security flaw in up-to-date web-based applications, constituting a plague for these programs. XSS assaults allow the assailant to initiate scripts that are malicious on the prey's web page browser, leading to a variety of side consequences such as data hack, pilfering of cookies, passwords, credit card information theft, and so on [36].

4.3 Wireless Phishing

Wireless phishing, additionally referred to as an evil twin assault, is a kind of scam that employs wireless networks as an assault mechanism. The scammer places himself among the victim and the genuine entrance point. This is performed through the utilization of a bogus access point with the exact same SSID as well as frequency as the legal network [37]. This type of phishing attack can be categorized into two famous categories:

- Wi-Fi: it has grown to be an integral part of modern life and, as a result, an attractive target for cybercriminals. In general, clients do not verify the access point from which they are currently communicating, and it is simple for an adversary to establish a fake accessing point using a Service Set Identifier (SSID) that resembles the legitimate one. Consequently, Wi-Fi Phishing happens when cybercriminals construct an illegal Wi-Fi access point that resembles or is identical to a legal Wi-Fi access point [35]. An evil twin attack occurs when an attacker creates a bogus Wi-Fi access point in the hopes that clients will join to it instead of the real one. Whenever users interact to this access point, all of the information they share with the network flows through a server under the control of the attacker[38][39].
- Bluetooth: is an additional kind of wireless phishing scam that occurs when the assailant connects via a Bluetooth-enabled device and has the ability to access data on the target's smartphone including contacts and call logs. As a result, mobile phone users should be safeguarded against a variety of phishing attacks. A warning sign must be shown when accessing a dubious website. As a result, Bluetooth-enabled smartphones are considered less authentic due to the assailant obtaining direct access to apps like the contacts database, calendar, to-do list, and call logs. Messages are being sent from the targeted user's smartphone to any other receiver. The assailant has the power to send any type of data to any Bluetooth-enabled device within range [40].

4.4 Social Media (Online social network) Phishing

Social networking is currently one of the most popular digital activities on a global scale. This is why many cybercriminals attempt to exploit social media networks such as Facebook, Instagram, and Twitter[41]. This led to the creation of the idea of "Angler Phishing." This is a new fraud tactic in which cybercriminals pose as customer service personnel on social media sites and accounts. The objective is to deceive disgruntled customers into divulging their personal information[42][43]. Therefore, social media has become the preferred platform for cybercriminals to launch phishing attacks. Due to the possibility of accessing a vast quantity of personal information disclosed by online social network users themselves, online social media can introduce new threats for their users. These threats include account hijacking, impersonation attacks, scams, and malware distribution. Due to the fact that social media resides outside of the network's boundaries, discovering and mitigating these hazards takes longer than conventional detection approaches [25][31]. Nation-state threat actors, for example, undertook an intense series of social media attacks against Microsoft in 2014. These attacks hacked numerous accounts on Twitter, exposing the passwords and email addresses of hundreds of Microsoft employees. Social media has grown into the favored venue for scammers to perpetrate phishing scams. Account takeovers, impersonation attacks, scams, and malware propagation are all examples of social media hazards [44]. According to Kaspersky Lab, over 3.7 million phishing attempts were made to visit fraudulent social network pages in the first quarter of 2018, with 60% of those efforts attempting to reach phony Facebook pages [45]. The most famous types of these phishing attacks can be found below:

- Linkedin: Actually, one of the biggest and most widespread LinkedIn phishing efforts occurs when an individual accepts a connection invitation from a fraudulent user. These demands can take various distinct forms. In rare cases, scammers may claim to be romantically interested in the person being scammed. As an example, LinkedIn-based phishing attempts detected tend to resemble LinkedIn's corporate style,' using headlines that will appear recognizable to any habitual client of the platform [46].
- Facebook: Due to people's lack of security consciousness, regarding the way Facebook is utilized, online phishers have begun conducting phishing assaults on Facebook, posing as friends and using phony or compromised accounts to confuse their targets. Some users of Facebook derive pleasure from social browsing, learning more about other people, and growing their social networks. To discover others and be found, users can customize their privacy settings and profile information to reach a broader audience. Through doing so, these users provide more data to the scamming perpetrators and expose themselves as potential victims [47].
- Twitter: Twitter has grown into a popular platform for phishers to spread infections of phishing because of its large amount of data dissemination and difficulty in being discovered, as opposed to email [48]. Spammers on Twitter tweet for a variety of reasons, including spreading advertisements,

disseminating pornography, spreading viruses, phishing, or simply undermining a system's image. Several reported instances demonstrate the threat posed by spammers on social media platforms online. A number of NatWest bank customers, for example, were the targets of a Twitter-based scamming assault that utilized spam tweets that appeared to be from the official NatWest customer support account[49].

- Tiktok: Due to the popular use of TikTok, the propagation of scamming has grown more diverse, rendering conventional phishing detection techniques, which began with emails, ineffective in preventing phishing. Because the majority of phishing assaults direct victims to fraudulent websites, recognizing fraudulent websites as an entrance point has grown into an increasingly practical method of scamming defense [50]. The scammers take use of TikTok's flaws to automate the contact uploading and synchronization process on a wide scale in order to develop a database for sparse phishing [51].
- Instagram: Instagram has grown to be a particularly common victim for scammers among media-sharing websites, with over 1 billion active users. Similarly, scammers seek to gain the trust of users by impersonating friends or followers in order to distribute harmful content. Criminals impersonating Instagram distribute fraudulent emails to victims, claiming to activate their verified insignia, followed by a phony website asking for the target's Instagram login details, email address, and passwords [52].
- Youtube: YouTube has grown in popularity among users. Because of YouTube's popularity, it has become a venue for spammers to transmit spam via YouTube comments. This is an issue since spam can lead to a phishing assault, with the target being any person who clicks on a bad link. Spam causes numerous issues, including squandering the user's time and memory, as well as utilizing network bandwidth. Because of the threat of spam, organizations, and clients may suffer financial losses. Some scammers utilize the YouTube comment section for advertising purposes, whereas other individuals are responsible for delivering computer viruses, and other spam messages meant to steal personal data and financial identity. The most worrisome spam risks include harmful spam that directs consumers to phish websites once they click the link and malware spreading [53].
- Impersonation: Users enjoy following renowned people on social media platforms and joining their interest-based groups. There currently exists no technique for validating the legitimacy of a virtual profile. The phisher takes advantage of this by posing as a renowned person and posting malicious links to sales or offers that, when clicked, request personal information or download malware [54].
- fake communities: To carry out the scam, the scammer may establish a phony group with an alias of a well-known organization and join some individuals who are actually members of the real organization but in fact, they are phishers attached to the fake group. They send group requests to other

participants in the organization, who join the group after seeing that their coworkers are also members. The phisher then obtains private data from their conversations and uses it for his personal benefit [35].

- Posting malicious links: Assailants employ harmful links to reroute the client to an outside malicious webpage controlled by the assailant. It is possible for fake accounts to publish the links. Within 24 hours of an attacker posting a malicious URL, nearly 90 % of visits occur. When a link looks to be a promising link, the redirection can be accomplished using social engineering. The rerouted website could include deceptive information, such as malicious software, a sham registration page, or advertisements for counterfeit goods [31].
- fake profiles: The assailant is able to distribute friend invitations to clients while posing as an old acquaintance. The phisher gains access to the user's confidential information that he shares with acquaintances, relatives, and coworkers after being added to the friend list. For more details, the scammer may contact the user via email or phone [55].

4.5 Mobile Phishing Techniques

Phishing attacks based on mobile are often categorized according to mobile applications, mobile malware, and other phishing attacks based on mobile. Some varieties of mobile phone phishing attacks will be discussed below.

- Mobile applications: On mobile devices, app-based phishing assaults are a significant issue. an internet user could become a victim of phishing attempts while browsing or downloading an application. When malicious apps infiltrate the mobile, they gather private data from the end-user, such as login ids and passwords, and send it to the assailant. The assailant might set up a backdoor as well as other applications that breach the user's privacy [56]. The following section discusses various phishing attack tactics on mobile applications:
    - ❖ Similarity attack: The phishing application attempts to convince legitimate users that a phishing website is legitimate by using a website or registration interface with the identical name, User interface (UI), and icon as the legitimate website. The phishing perpetrators create websites with a high degree of similarity to the content of their intended pages, which is essentially manifested by the logo, Favicon, CSS architecture, page layout, and overall visuals. As a result, the phisher prompts the user to install a phishing application and enter credentials in a phishing Login User Interface (LUI) rather than a legitimate one [57].
    - ❖ Forwarding attacks: In this phishing assault, an assailant's website invites clients to share their activities on social networking sites, such as their high score in a game, and asks that a social media application be launched. Whenever the client clicks the link to start the social media appl, a scamming login page is displayed

instead. To gain entry to the account, the phishing page requests login information. Forwarding attacks of this nature are challenging to detect [35].

- ❖ Background attacks: Occasionally phishing applications operate in the backend and utilize Android's Activity Manager to maintain track of various apps operating on the mobile phone. When the client launches a legitimate target app, the scamming application appears in the forefront and displays the phishing screen [58].
- ❖ Notification attacks: The phisher may display an erroneous notification requesting the client for confidential information. The phisher can modify the notification window to appear identically to an authentic notification window [59].
- ❖ Floating attacks: The phisher takes advantage of an Android device feature that allows an app to draw a certain action on the surface of another app in the forefront. A phishing app with the SYSTEM ALERT WINDOW privilege can display a transparent input area on top of the authentic application's login id and password input fields. The legitimate application's Login User Interface is visible to the end user, however, the covered input area is not. The phishing application receives credentials whenever the user enters them in the input area [60].

- Mobile malware: Lack of awareness and security culture among users, as well as weaknesses in some applications that can be controlled through continuous updates. below are the famous types of this phishing attacks but not limited to:
  - ❖ Trojans: is a type of malware that disguises itself as a benign application in order to entice users to acquire and install malware. With such kinds of malicious software, attackers get the ability to remotely access for stealing information as well as finances, remove and alter files, generate malicious versions, monitor user activities such as monitoring screens and logs, and so on [58].
  - ❖ Worms: is a piece of code that can replicate and spread across networks of computers from machine to machine without the need for human involvement. Worms are capable of carrying "payloads" to harm devices that host them as well as hosting networks via consuming traffic and generating website congestion. Payloads typically pilfer client information, erase system files, and establish botnets. Opening an infected email attachment can propagate worms [58].
  - ❖ Mobile ransomware: is a form of malware that does not allow hardware and software to be released until the target pays a ransom. Ransomware locks the computer, restricting access, encrypts data, and displays messages requiring users to pay money. Following payment, ransomware software will be removed from the system [61].

- ❖ Key / screen loggers: Loggers are a type of malicious software used by phishers that are downloaded and installed on the victim's computer via Trojan horse email attachments or direct download. Before transmitting the information to the phisher, this program checks data and logs user keystrokes [62]. The Phisher uses keyloggers to gather private data about the clients, including their names, addresses, passwords, as well as other confidential information. Key loggers are additionally useful for non-phishing purposes, such as monitoring a child's Internet usage [40]. Key loggers may additionally be employed in various ways, including recognizing changes in URLs and logging information as a Browser Helper Object (BHO) which permits the hacker to influence the attributes of all Internet Explorers, observing keyboard and mouse input as a driver for the device, and observing client's input and show as a screen logger [18][63].
- ❖ Botnets: A mobile botnet is a collection of smartphone and tablet computers corrupted by a malicious program. An attacker known as the Botmaster commands a mobile botnet to conduct illegal operations such as eavesdropping, transmitting malicious codes via SMS, DDoS attacks, and stealing sensitive information [64].
- ❖ Spyware: The attacker uses freely available online spyware to gain control of the victim's mobile phone, allowing them to control SMS, emails, listen to phone conversations, and monitor the victim's location using GPS. Spyware utilizes hidden channels in the smartphone to provide the information for the assailant. When an app requires sending information to outside parties for reasons that are legitimate, the settings of permissions existing on smartphones are not sufficient to prevent similar approval from being misused for any other purpose [35].
- ❖ Rootkits: is a form of malware that gains remote access and control of a device in order to exploit users. To perform harmful actions, rootkits include a dropper, a loader, and the rootkit itself. It gets administrative access in order to install various malicious activities such as stealing information, disrupting system routines, making changes in the system, causing system configuration to be altered, and so on. When a rootkit is installed on a computer, it starts at boot time. The rootkit can be challenging to identify and eliminate from the system due to its covert operations. Because the rootkit employed obfuscation to conceal its existence, it remains on the system for a long time [58].

- Other mobile phishing: this type
  - ❖ Smishing (SMS): is a type of phishing attack that focuses on sending SMS messages. Smishing functions almost identically to email phishing attempts. Using SMS to phone numbers that are randomly accessible to the public, hackers send messages to victims

holding crucial information or instructions that must be executed promptly[65]. This Smishing attack is dangerous since it is more personalized and so renders the victim less vigilant[66][67]. The objective of a social engineering attack is to obtain sensitive information using a variety of human interaction techniques. Certain tactics involve sending a victim a malicious SMS and convincing the victim to make a security error by clicking a malicious link or providing confidential information. Due to the lack of cyber security awareness among users, the number of SMS spam messages continues to rise over time [68].

- Vishing (VoIP): is a kind of phishing that targets telephone communication channels. Without the user's knowledge, hackers employ Vishing to fool clients into divulging confidential data that involves PINs, One-Time Passwords, and so on. Hackers employ a variety of psychological strategies, such as threats, worry, and good news, to prevent victims from recognizing they are not being scammed[29][69].
- Data theft: is the unauthorized accessing and obtaining of confidential information belonging to an organization or an individual. An email that is phishing and that leads to the download of malicious software onto a user's computer and then directly captures confidential information stored on that computer can be used to commit data theft [70]. Phishers could directly or indirectly sell information that was stolen such as usernames and passwords social security numbers, credit card numbers, confidential emails, and other personally identifiable data [25].
- System reconfiguration: In a system reconfiguration attack, the attacker sends a message to the user requesting them to reconfigure their computer settings. That message could originate from a web address that looks to be trustworthy[71]. As a result, the phisher modifies the settings on a user's computer for malevolent purposes, compromising the data on this PC. Reconfiguring the operating system and changing the user's DNS server address are two ways for changing system configurations. The wireless evil twin assault is an instance of a network reconfiguring assault whereby a hostile wireless Access Point monitors the entire user network traffic [18].

5 Conclusion

Phishing attacks continue to pose a serious threat to both individuals and businesses. This is largely due to the fact that these attacks exploit human vulnerabilities and weaknesses, alongside technological weaknesses. This review paper examines various strategies, challenges, and trends in detecting phishing attacks, providing valuable insights

for researchers in this field. Unfortunately, preventing phishing attacks remains a complex task in the realm of system security. Effective detection systems must be able to identify these attacks with few false positives. Moreover, phishing attempts have evolved from traditional email scams to social media-based attacks, which require updated detection methods. As attackers constantly refine their tactics, there is often a time lag between new phishing schemes and available defensive measures. Therefore, future defense strategies should be comprehensive, addressing both the technical and human factors involved in these attacks. Overall, this article offers a wealth of information on current phishing threats and countermeasures, with a precise classification system that illuminates the entire phishing life cycle.

6 References

[1] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Comput. Human Behav.*, vol. 38, pp. 304–312, 2014.

[2] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respício, "Cybersecurity education: Evolution of the discipline and analysis of master programs," *Comput. Secur.*, vol. 75, pp. 24–35, 2018.

[3] W. A. Conklin, R. E. Cline, and T. Roosa, "Re-engineering cybersecurity education in the US: an analysis of the critical factors," in *2014 47th Hawaii international conference on system sciences*, 2014, pp. 2006–2014.

[4] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, 2021.

[5] E. Benavides, W. Fuertes, S. Sanchez, and M. Sanchez, "Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review," *Dev. Adv. Def. Secur.*, pp. 51–64, 2020.

[6] S. Marchal, G. Armano, T. Gröndahl, K. Saari, N. Singh, and N. Asokan, "Off-the-hook: An efficient and usable client-side phishing prevention application," *IEEE Trans. Comput.*, vol. 66, no. 10, pp. 1717–1733, 2017.

[7] A. K. Jain and B. B. Gupta, "Phishing detection: analysis of visual similarity based approaches," *Secur. Commun. Networks*, vol. 2017, 2017.

[8] APWG, "Phishing E-mail Reports and Phishing Site Trends 4 Brand-Domain Pairs Measurement 5 Brands & Legitimate Entities Hijacked by E-mail Phishing Attacks 6 Use of Domain Names for Phishing 7-9 Phishing and Identity Theft in Brazil 10-11 Most Targeted Industry," *APWG Phishing Act. Trends Rep. 1st Quart. 2022*, vol. 1, no. 1, p. 13, 2022, Accessed: Dec. 16, 2022. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf

[9] A. K. Jain and B. B. Gupta, "A novel approach to protect against phishing attacks at client side using auto-updated white-list," *EURASIP J. Inf. Secur.*, vol. 2016, no. 1, p. 9, 2016.

[10] D. Patel, "Test utility for live and online testing of an anti-phishing message security system," 2018.

[11] S. H. Apandi, J. Sallim, and R. M. Sidek, "Types of anti-phishing solutions for phishing

attack," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 769, no. 1, p. 12072.

[12] A. K. Jain and B. B. Gupta, "A machine learning based approach for phishing detection using hyperlinks information," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 5, pp. 2015–2028, 2019.

[13] B. B. Gupta, K. Yadav, I. Razzak, K. Psannis, A. Castiglione, and X. Chang, "A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment," *Comput. Commun.*, vol. 175, pp. 47–57, 2021.

[14] L. Barlow, G. Bendiab, S. Shiaeles, and N. Savage, "A novel approach to detect phishing attacks using binary visualisation and machine learning," in *2020 IEEE World Congress on Services (SERVICES)*, 2020, pp. 177–182.

[15] A. Basit, M. Zafar, A. R. Javed, and Z. Jalil, "A novel ensemble machine learning method to detect phishing attack," in *2020 IEEE 23rd International Multitopic Conference (INMIC)*, 2020, pp. 1–5.

[16] B. B. Gupta and A. K. Jain, "Phishing attack detection using a search engine and heuristics-based technique," *J. Inf. Technol. Res.*, vol. 13, no. 2, pp. 94–109, 2020.

[17] K. A. Djaballah, K. Boukhalfa, Z. Ghalem, and O. Boukerma, "A new approach for the detection and analysis of phishing in social networks: the case of Twitter," in *2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS)*, 2020, pp. 1–8.

[18] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, 2017.

[19] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A literature review," in *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*, 2018, pp. 62–68.

[20] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *2016 international conference on computing, communication and automation (ICCCA)*, 2016, pp. 537–540.

[21] A. S. Sengar, A. Bhola, R. K. Shukla, and A. Gupta, "A Review on Phishing Websites Revealing through Machine Learning," in *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2021, pp. 330–335.

[22] E. Gandotra and D. Gupta, "Improving spoofed website detection using machine learning," *Cybern. Syst.*, vol. 52, no. 2, pp. 169–190, 2021.

[23] L. Tang and Q. H. Mahmoud, "A survey of machine learning-based solutions for phishing website detection," *Mach. Learn. Knowl. Extr.*, vol. 3, no. 3, pp. 672–694, 2021.

[24] K. Krawchenko, "The phishing email that hacked the account of john podesta," *CBS NEWS, Oct.*, 2016.

[25] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Front. Comput. Sci.*, vol. 3, p. 563060, 2021.

[26] A. Bhadane and S. B. Mane, "Detecting lateral spear phishing attacks in organisations," *IET Inf. Secur.*, vol. 13, no. 2, pp. 133–140, 2019.

[27] L. Allodi, T. Chotza, E. Panina, and N. Zannone, "The need for new antiphishing measures against spear-phishing attacks," *IEEE Secur. Priv.*, vol. 18, no. 2, pp. 23–34,

2019.

[28] G. Wangen, "Quantifying and analyzing information security risk from incident data," in *International Workshop on Graphical Models for Security*, 2019, pp. 129–154.

[29] V. Gomes, J. Reis, and B. Alturas, "Social engineering and the dangers of phishing," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 2020, pp. 1–7.

[30] R. S. Rao and A. R. Pais, "Jail-Phish: An improved search engine based phishing detection system," *Comput. Secur.*, vol. 83, pp. 246–267, 2019.

[31] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterp. Inf. Syst.*, vol. 16, no. 4, pp. 527–565, 2022.

[32] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, pp. 247–267, 2018.

[33] M. N. Alam, D. Sarma, F. F. Lima, I. Saha, and S. Hossain, "Phishing attacks detection using machine learning approach," in *2020 third international conference on smart systems and inventive technology (ICSSIT)*, 2020, pp. 1173–1179.

[34] A. Sadiq *et al.*, "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0," *Hum. Behav. Emerg. Technol.*, vol. 3, no. 5, pp. 854–864, 2021.

[35] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Comput. Secur.*, vol. 73, pp. 519–544, 2018.

[36] S. Gupta and B. B. Gupta, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art," *Int. J. Syst. Assur. Eng. Manag.*, vol. 8, pp. 512–530, 2017.

[37] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Futur. internet*, vol. 12, no. 10, p. 168, 2020.

[38] Kasperky, "What is an Evil Twin Attack? Evil Twin Wi-Fi Explained," 2022. https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks (accessed Dec. 16, 2022).

[39] S. Kitisriworapan, A. Jansang, and A. Phonphoem, "Evil-twin detection on client-side," in *2019 16th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, 2019, pp. 697–700.

[40] J. Khalid, R. Jalil, M. Khalid, M. Maryam, M. A. Shafique, and W. Rasheed, "Anti-phishing models for mobile application development: a review paper," in *International Conference on Intelligent Technologies and Applications*, 2018, pp. 168–181.

[41] G. Sonowal, "Communication Channels," in *Phishing and Communication Channels*, Springer, 2022, pp. 51–75.

[42] P. P. Kumar, T. Jaya, and V. Rajendran, "SI-BBA–a novel phishing website detection based on Swarm intelligence with deep learning," *Mater. Today Proc.*, 2021.

[43] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," *IEEE Access*, 2022.

[44] R. S. Kunwar and P. Sharma, "Social media: A new vector for cyber attack," in *2016 International Conference on Advances in Computing, Communication, & Automation*

(ICACCA)(Spring), 2016, pp. 1–5.

[45] M. Raggo, "Anatomy Of A Social Media Attack," *Dark Reading*, 2016. https://www.darkreading.com/analytics/anatomy-of-a-social-media-attack (accessed Dec. 14, 2022).

[46] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *Int. J. Hum. Comput. Stud.*, vol. 82, pp. 69–82, 2015.

[47] S. Seng, M. N. Al-Ameen, and M. Wright, "Understanding users' decision of clicking on posts in facebook with implications for phishing," 2018.

[48] S. W. Liew, N. F. M. Sani, M. T. Abdullah, R. Yaakob, and M. Y. Sharum, "An effective security alert mechanism for real-time phishing tweet detection on Twitter," *Comput. Secur.*, vol. 83, pp. 201–207, 2019.

[49] N. H. Imam and V. G. Vassilakis, "A survey of attacks against twitter spam detectors in an adversarial environment," *Robotics*, vol. 8, no. 3, p. 50, 2019.

[50] D.-J. Liu, G.-G. Geng, and X.-C. Zhang, "Multi-scale semantic deep fusion models for phishing website detection," *Expert Syst. Appl.*, vol. 209, p. 118305, 2022.

[51] C. JANG, O. O. K. LEE, C. MUN, and H. HA, "AN ANALYSIS OF PHISHING CASES USING TEXT MINING," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 22, 2022.

[52] J. Chung, J.-Z. Koay, and Y.-B. Leau, "A Review on Social Media Phishing: Factors and Countermeasures," in *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*, 2021, pp. 657–673.

[53] N. F. Othman and W. Din, "Youtube spam detection framework using naïve bayes and logistic regression," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 14, no. 3, pp. 1508–1517, 2019.

[54] A. Bhardwaj, F. Al-Turjman, V. Sapra, M. Kumar, and T. Stephan, "Privacy-aware detection framework to mitigate new-age phishing attacks," *Comput. Electr. Eng.*, vol. 96, p. 107546, 2021.

[55] A. Alharbi, A. Alotaibi, L. Alghofaili, M. Alsalamah, N. Alwasil, and S. Elkhediri, "Security in social-media: Awareness of Phishing attacks techniques and countermeasures," in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, 2022, pp. 10–16.

[56] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, 2018.

[57] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, "Phishing website detection based on deep convolutional neural network and random forest ensemble learning," *Sensors*, vol. 21, no. 24, p. 8281, 2021.

[58] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks: Review, taxonomy & future directions," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 887–909, 2019.

[59] D. Wu, G. D. Moody, J. Zhang, and P. B. Lowry, "Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention," *Inf. Manag.*, vol. 57, no. 5, p. 103235, 2020.

[60] S. Baadel, F. Thabtah, and A. Majeed, "Avoiding the Phishing Bait: The Need for Conventional Countermeasures for Mobile Users," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018, pp. 421–425.

[61] S. Kalpana and S. Karthikeyan, "A survey on rise of mobile malware and detection methods," in *2017 international conference on innovations in information, embedded and communication systems (ICIIECS)*, 2017, pp. 1–5.

[62] G. Varshney, M. Misra, and P. Atrey, "Browshing a new way of phishing using a malicious browser extension," in *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*, 2017, pp. 1–5.

[63] T. L. Shan, G. N. Samy, B. Shanmugam, S. Azam, K. C. Yeo, and K. Kannoorpatti, "Heuristic systematic model based guidelines for phishing victims," in *2016 IEEE Annual India Conference (INDICON)*, 2016, pp. 1–6.

[64] S. Hamzenejadi, M. Ghazvini, and S. Hosseini, "Mobile botnet detection: a comprehensive survey," *Int. J. Inf. Secur.*, vol. 22, no. 1, pp. 137–175, 2023.

[65] J. W. Joo, S. Y. Moon, S. Singh, and J. H. Park, "S-Detector: an enhanced security model for detecting Smishing attack for mobile computing," *Telecommun. Syst.*, vol. 66, no. 1, pp. 29–38, 2017.

[66] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, SMiShing & Vishing: an assessment of threats against mobile devices," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 5, no. 4, pp. 297–307, 2014.

[67] R. E. Ulfath, I. H. Sarker, M. J. M. Chowdhury, and M. Hammoudeh, "Detecting Smishing Attacks Using Feature Extraction and Classification Techniques," in *Proceedings of the International Conference on Big Data, IoT, and Machine Learning*, 2022, pp. 677–689.

[68] N. Rifat, M. Ahsan, M. Chowdhury, and R. Gomes, "BERT Against Social Engineering Attack: Phishing Text Detection," in *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022, pp. 1–6.

[69] Q. Yuan, B. Huang, J. Zhang, J. Wu, H. Zhang, and X. Zhang, "Detecting phishing scams on ethereum based on transaction records," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2020, pp. 1–5.

[70] G. Sonowal and G. Sonowal, "Introduction to Phishing," *Phishing Commun. Channels A Guid. to Identifying Mitigating Phishing Attacks*, pp. 1–24, 2022.

[71] J. A. Chaudhry and R. G. Rittenhouse, "Phishing: Classification and countermeasures," in *2015 7th International Conference on Multimedia, Computer Graphics and Broadcasting (MulGraB)*, 2015, pp. 28–31.

Article submitted 1 March 2023. Accepted at 11 May. Published at 30 Jun 2023.