Societal Transformation: AI and Big Data Journal
Vol: 2(1): 94-115, 2024
DOI: 10.20547/aibd.242105

A Systematic Literature Review on Phishing Attacks and Countermeasures

Tariq Saeed[1], Muhammad Nafees[2]

Abstract: During the past few years, cybersecurity has gained a lot of prominence. In this paper, phishing attacks are discussed in detail. In a phishing attack, an attacker disguises itself as a genuine user and deceives the end-user to gains its personal information such as credit card, usernames/ passwords etc. There are a number of ways to perform phishing attacks such as via email, spear phishing, clone phishing, whaling etc. This paper talks about phishing attacks in detail along with its techniques, counter-measures and recent trends directions for research. Phishing is a significant threat to every individual, organization, and in general the global landscape. The paper starts with a comprehensive study on phishing attacks and countermeasures. It provides an overview of the techniques employed by attackers for compromising security. It also presents the evolving trends in phishing attacks. Finally, the paper delves on the current countermeasures proposed in literature to mitigate such threats.

Keywords: *phishing attacks, counter measures, cyber security*

1. Introduction

Phishing attacks have emerged as one of the most prevalent and destructive cyber threats. With the increasing reliance on digital platforms for communication, commerce, and data sharing, phishing attacks have become more sophisticated, deceptive, and difficult to detect. Specifically, after the emergence of recent technologies such as Internet of Things (IoT), generative AI and 5G networks, there have been growing discussion on phishing attacks [27]. For this reason, understanding the techniques employed by attackers, staying updated on evolving trends, and implementing effective countermeasures have become very essential for protecting the sensitive information as well as keeping the security of digital systems. Normally, the intent of the attacker in a phishing attack is to access financial details, steal system credentials or other sensitive information [14]. In addition, a phishing attack is generally followed by other forms of sophisticated attacks such as ransomware attacks. According to Anti-Phishing Working Group, phishing attacks increased by 250,000 per day in Jan 2021[17].

[1] Karachi Institute of Economics and Technology, Karachi *tariq@kiet.edu.pk*
[2] Karachi Institute of Economics and Technology, Karachi *safdarabad@gmail.com*

In literature, various techniques to phishing have been presented. The attacker masquerade as a legitimated person and then launches the attack in almost all form of phishing attack[17]. Primarily, phishing is performed over three types of mediums i.e. internet, SMS and voice [14]. For instance, fraudulent emails, sometimes called phishing emails, can be used to do phishing. The email seems to be from reliable and trustworthy sources. False websites are another kind of phishing tactic that are designed to trick users into giving up personal information. Finally, social engineering in the form of phone calls/ SMS can be done to perform phishing. All of these techniques employee (one form of or other) psychological techniques that are used to incite individuals into disclosing private information.

Spear phishing, for example, has emerged as a highly targeted form of phishing, wherein attackers personalize their messages to specific individuals or organizations, increasing the probability of success. Moreover, mobile phishing and voice-based phishing have gained prominence due to the widespread use of smartphones and voice-enabled devices, offering new avenues for attackers to exploit.

In literature, a number of techniques have emerged to mitigate phishing. Amongst them, blanket measures like SPAM filters, black lists, and domain reputation among others are popular approaches. In addition, a number of novel approaches such as those based on machine learning and deep learning have also been proposed. Machine learning is a branch of artificial intelligence that learns patterns from the data and then classifies/ make prediction for unseen data. Finally, novel measure to enhance end-users' awareness about the threats of phishing attacks are also needed. In addition, involvement of multi-factor reliable authentication methods are also an essential component to eliminate vulnerability.

In view of the discussions outlined above, this paper presents a systematic literature review of phishing attacks and countermeasures. The paper aims to provide a comprehensive overview. Specifically, the major questions addressed in this paper are as follows:

- What is a phishing attack? What are its various definitions?
- What are the objectives of phishing? To identify a novel multi-phased approach to the launch of a phishing attack
- What are the psychological techniques that are exploited to launch a phishing attack?
- Can we analyze the tactics employed by attackers so that readers can gain significant insight into the nature of phishing? Can we identify the factors that contribute to successful execution of a phishing attack
- What are the counter-measures employed to mitigate phishing attacks?
- What are the future directions for research in phishing attack prevention and detection.
- What are potential challenges of emerging technologies, such as blockchain, generative AI in the context of phishing

Rest of the sections are organize as follows. The next section presents related work in this direction. This is followed with the methodology adopted for systematic literature review. Then, various phishing definitions of phishing, popular phishing attacks, phishing techniques and then counter measures are presented. The paper also presents the human factors involved in phishing. Finally, the paper concludes with directions for future research.

2. Related work

Before proceeding towards the systematic literature review performed in this paper, it is essential to highlight the current SLR performed and reported in literature. In [14], a systematic literature review was performed on mitigation strategies for phishing attacks. The authors considered only web-of-science and Scopus journals. They attempted to answer various questions related to mitigation strategies, guidelines for anti-phishing and open research challenges. In [17], a state-of-the-art survey on phishing detection was performed. The authors targeted only phishing techniques based on URL and they discussed various conventional and machine/ deep learning solutions proposed for detection of phishing attacks. A systematic literature review on phishing and anti-phishing techniques have been presented in [27]. Similarly, a study on phishing techniques, environments and counter-measures have been done in [28]. A review on phishing techniques, counter-measures and phishing prevention techniques have been provided in [29]. Perspectives on Nigerian environment has been provided in [30].

Despite the availability of existing reviews, it is essential to provided an updated account on the subject, as the phishing attacks are on the rise and every day, new forms of attacks are emerging.

3. Methodology

The paper has performed a systematic literature review of 25 research papers on phishing attacks. Figure 1 shows the methodology adopted for research. The guidelines provided in [15] have been followed for the systematic literature review.

3.1 Inclusion / exclusion criteria

For the systematic literature review, some inclusion and exclusion criteria were formulated to obtain the papers that align with the goals of the study. Following are the criteria for the selection of the paper:

- IC1: The language of the publication is English
- IC2: The subject/ title of the paper is about phishing
- IC3: The paper has been published in a journal
- IC4: The paper has been published in last 5 years

Following are the exclusion criteria:

- EC1: The paper has not been published in English
- EC2: The full text of the paper is not available
- EC3: The publication is not a peer-reviewed journal

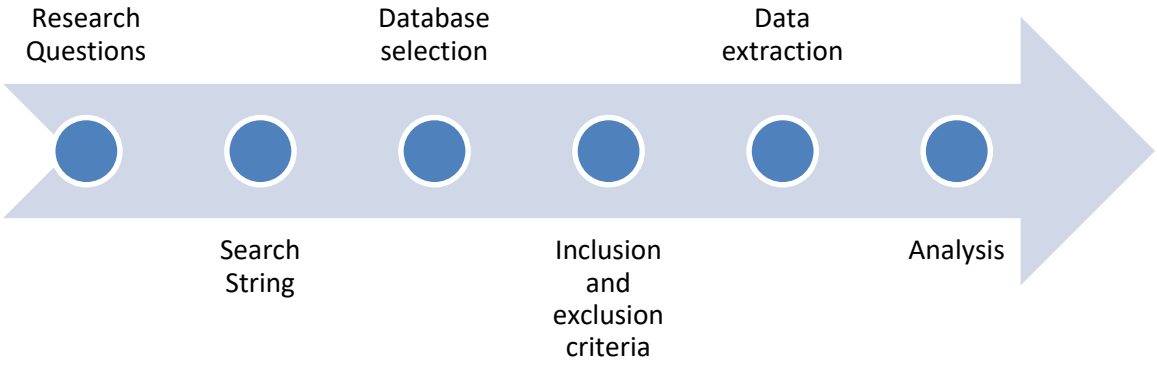

Figure 1: The methodology for systematic literature review

3.2 Search string

In order to select papers, various key words were used to perform search such as phishing, phishing attack, mitigating phishing attacks, counter measures for phishing attack, phishing definitions. The search string can be formulated as follows:

Phishing OR mitigating phishing attacks OR phishing definitions OR phishing guidelines OR prevention techniques OR solutions

3.3 Publication sources

For systematic literature review, existing papers have considered various data sources. Based on the study, we have identified the most important data sources. Following are the dataset / avenues from which research papers been collected: IEEE, ACM, Springer, Elseveir, Web of science, Scopus, Emerald, MDPI. Google scholar has been used as the primary search engine. Table 1 presents a summary of some of the selected papers.

Table 1: A summary of research literature on phishing attacks

S No	Title	Year/Journal	Journal	Discussed Area
1.	Types of Anti-Phishing Solutions for Phishing Attack [1]	2020	IOP Conference Series: Materials Science and Engineering	1. Phishing Attack in details 2. Anti-phishing solution i. Phishing Prevention ii. Phishing Detection
2.	A Study of Phishing Attack towards Online Banking [2]	2023	Borneo International Journal	1. Introduction 2. Types of phishing attacks 3. Phishing Attack Countermeasures
3.	Detection of Phishing Attack [3]	2022	International Journal of Research Publication and Reviews	1. Introduction 2. Anti-Phishing Solution
4.	Prevention of Phishing Attacks Using AI-Based Cyber security Awareness Training [4]	2022	International Journal of Smart Sensor and Adhoc Network	1. Background on Phishing Attacks 2. How Phishing works 3. Phishing Techniques 4. National Initiative for Cyber security Education (NICE) framework and viCyber Model
5.	A Literature Survey of Phishing and Its Countermeasures [5]	2022	Conference: Second Annual Computer Science Conference for CSU Undergraduates	1. An overview of phishing 2. Phishing Motives 3. Phishing attacks and countermeasures
6.	A Review on Phishing Attacks[6]	2019	International Journal of Applied Engineering Research	1. Introduction 2. Phishing Mechanism: Plan, Compose email,

				Attack, Gather data and Fraud 3. Types of Phishing Attacks 4. Anti-Phishing Techniques
7.	Enterprise Credential Spear-phishing attack detection [7]	2021	Computers & Electrical Engineering	1. Introduction. 2. "Steps Enterprise Credential Spear-phishing". 3. Attack Taxonomy and Anti-Phishing Algorithm
8.	Cyber Security Threats, Vulnerability, Challenges with Proposed Solution [8]	2022	Applied Computing Journal	1. Cyber Security Fields: (NACO) 2. Benefits of Cyber-Security 3. Common Cyber Security Measures
9.	Social Engineering Attack Detection Using Machine Learning: Text Phishing Attack[9]	2021	Indian Journal of Computer Science and Engineering (IJCSE)	1. Social Engineering (SE) attacks 2, Mitigation Techniques 3. Comparison between Mitigation Techniques
10.	Social Engineering Attacks: A Survey [10]	2019	Future Internet	1, Introduction 2. Types 3. Prevention Techniques
11.	Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms [11]	2022	International Journal of Advanced Research in Computer and Communication Engineering	1. Phishing attacks in details 2. Detecting via anti-phishing through deferent ways.

Definitions of phishing

There has been several definitions of phishing proposed in literature. However, based on the studies, it has been find that there doesn't exist a single definition of the term [28]. According to [13], phishing is a fraudulent activity and the objective is to deceive an end-user or a trusted third party to obtain sensitive information. [17] defines phishing as a social engineering attack. The attacker deceives end-user via sending fake messages using social media platforms or emails. According to [20], the attacker impersonates via taking the advantage of resemblance with a legitimate entity to gain credentials of a user or other sensitive information. According to [21], a phishing attack comprises three steps: lure, hook and catch. The victim first receives a lure message. The message may contain some curiosity, fear, or empathy. The hook is the attachment or the link that user clicks. The catch is when the attacker gains access to user's personal / sensitive information. According to [24], phishing attacks are multi-faceted, employing various techniques to gain access to servers, domain names and stealing credentials. It is also regarded as an approach to gain access to sensitive data of end-user using social engineering and technology [27]. The authors in [22] provided the definition of phishing in the context of blockchain as the technique of tricking a miner to add a malicious block to the chain. According to [28], phishing involves tricking the end-user to let them perform the intent of the attacker.

Popular phishing attacks

In this section, we highlight some of the popular phishing attacks in literature. Figure 2 provides the summary.

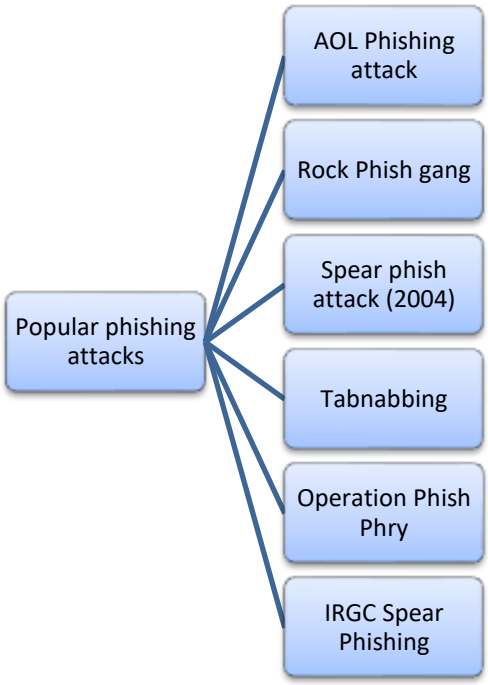

Figure 2: Popular Phishing attacks in literature

1.1. AOL Phishing attack in 1996

The roots of phishing can be traced back to 1996. A group of hackers utilized email and instant messaging service. The attackers pretending them to be AOL workers to obtain passwords from customers and take over their accounts. Since then, a rise in phishing assaults has been observed around 57.53% on average every month [5].

1.2. Rock Phish Gang

Rock Phish Gang has also been cited in studies as involved in phishing. Being one of the most prominent phishing organizations (formed in mid 2003), it has been a significant danger since then. The gang employed various analytical techniques such as creating fake Internet sites which are similar to real sites. The authors tricked consumers into surrendering their private details.

1.3. Spear Phishing attack on banking

Similarly, in another type of phishing called spear phishing, attackers tailor their communications to certain people or organizations. A spear phishing attempt on the banking sector was launched in 2004. The attack targeted executives with phone calls, emails and websites.

1.4. Tabnabbing

Tabnabbing in 2005 was launched by a security researcher Aza Raskin. One of the socio-technical vulnerabilities would be that a malicious site could inject a new page taking the place of the genuine content with this fake login page thus capitalizing on the browser tabs.

1.5. Operation Phish Phry

In another phishing attack called Operation Phish Phry, hundreds of people took part in the massive multinational phishing. This resulted in loss of millions of dollars. The group was involved in targeting of banks and other financial institutions. Overall, this operation was one of the phishing attempts on a worldwide scale.

1.6. Iranian Revolutionary Guard Corps (IRGC) Spear Phishing

A group of hackers from Iran were involved in spear fishing attacks recently in Air Force. Emails were sent specifically with the information that were collected from an insider with a reconnaissance operation [16].

Phishing Mechanisms

Before understanding the various approaches to phishing and its counter-measures, it is essential to zoom into the process of phishing. What are the entities involved and what steps are involved in phishing? Phishing attacks are primarily performed to let the recipient release information to the attacker. An assault of this type is performed by an *attacker*, sometimes also called a phisher, who impersonates a trustworthy site. The attacker links to a website for the purpose of creating a mimic of the website, thus he or she creates a malicious one. This phishing website provides all the details of the target to the attacker. In almost all the cases, targets fail to recognize phishing websites from legitimate ones, falling victim to the traps laid by the phisher [6].

Phishing attacks have several steps that attackers follow to obtain information. In [28], five major steps are identified for the phishing process. This includes attack planning, attack setup, attack execution, fraud and post-attack phase. In another study[21], three major steps i.e. lure, hook and catch have been described as the major phase of a phishing attack. In general, the attacker first prepares for the attack by coordinating it. As a sub-step, the victim on which data has to be collected and the legitimate website which has to be mimicked are chosen in this step. The next step entails planning and crafting of an email that looks real to make the victim such it can release his or her information. The third step is sending the prepared e-mail to the intended recipient, and

then, obtaining information about the 'victim'. The final step will occur if the victim falls into the phisher's trap and the initiation of the gathering of information phase begins

Based on various studies, we identify five stages to describe a phishing attack i.e. attack planning, compose, attack execution, data gathering and enacting fraud. Figure 2 shows the process. Below, we discuss each of the steps in detail. In **step 1**, the (attacker) plans for and coordinate, perform research and gather all the information about the environment, victim. In step2, the attacker uses a phishing website to create an email. This email's structure should make it seem authentic and credible. Instead of an email, a phone call, SMS or any other medium can be used. The victim (target) receives this crafted email from the attacker in step 2.

The attacker will then send the information to the target. The target would not be able to feel the difference between a legitimate email and a phishing one, The target will open the attachment or click on the link which will take her to the phishing website. In step 4, the phishing website gives the attacker the login information. In step 5, the attacker will gather all of the victims records and using the victim's credentials, he can enact the fraud.

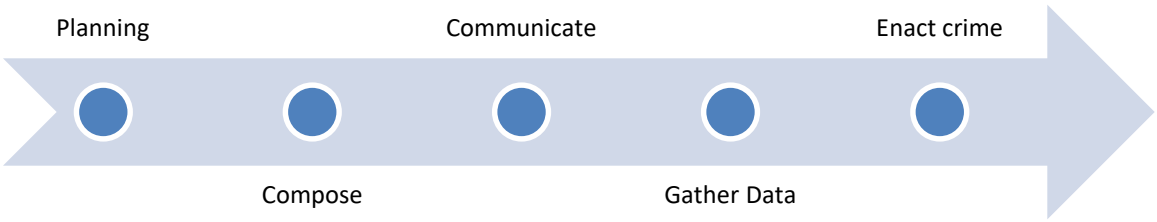

Figure 2: Proposed 5-step process for phishing attack

After having a brief discussion on phishing, we will now discuss the counter measures for phishing. According to [14], three types of approaches can be employed. This includes anti-phishing systems, models and frameworks, and human-centric mitigation strategies.

Types of Phishing Attacks

In this section, we will discuss the various types of phishing attacks proposed in literature. Phishing attempts frequently target email addresses, phone numbers, banking information, credit card

numbers, and account passwords [2]. The attacker or phisher uses social engineering to steal the victim's personal information and account information. [20] classified various types of phishing attacks into spear phishing, email phishing, malware phishing and ads-phishing. [28] classified phishing attacks based on various criteria such as communication medium, target environment, attack techniques and counter-measures. Figure 3 presents various types of phishing attacks.

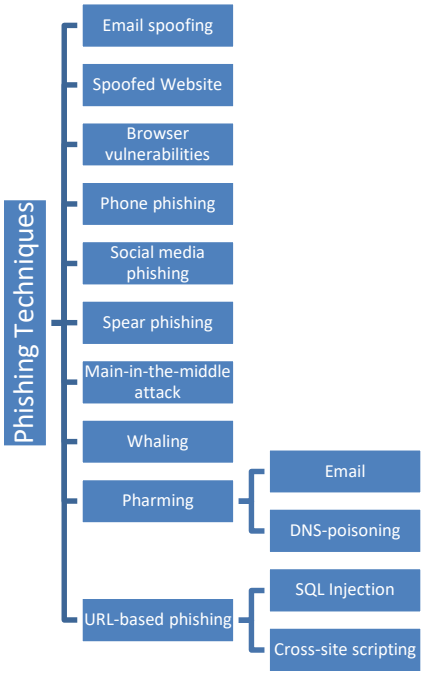

Figure 3: Various types of phishing attacks

1.7. Email spoofing

One of the technique to perform phishing is via emails. In this technique, the attacker spoof to be from some higher authority and gain the trust of the end-user [27]. A software link or attachment is provided. Alternatively, advertisements may be sent to the victim. The victims of these phishing assaults will lose the confidentiality and integrity of their personal information [2]. In this direction, several AI-based phishing solutions have been proposed in [32].

1.8. Brower vulnerabilities

Exploiting browser vulnerability is another type of phishing that has been reported in 30% of the cases. The attackers are always in search for a vulnerability in browser to crack the victim computer [27].

1.9. Spoofed Website

The webpage that the phisher creates for a faked website will seem real and comparable to a legitimate website [29]. When consumers click the website link and continue engaging with the falsified websites, there is a great chance that their personal information will be exposed and stolen by the phisher. This fraud website's link is shared with users by email or any other media sources [11].

1.10. Phone Phishing

Since phone calls or text messages are used as the method, phone phishing is also known as Vishing or Smishing [2]. The attacker communicates with the end-user via phone or mobile [27]. They pretend to be a good guy or someone that the targets know very well. A typical example is PIN code. Codes are produced for clients for any kind of transaction for online banking. The bank may forward a realistic security alert message to the target. They are asked to call a specific number to get information. The victim is directed by an authentic source within the email or the Short Messaging Service. After the attack is completed, the attacker can use the details of the victim to gain access to his/her messaging account and be in a position to conduct phishing to other persons in the victim's' contact list. They are also called flier strategies. The phisher may also use Caller Identification (CID) spoofing to disguise as calling from a truste source [29].

1.11. Social Media Phishing

Given that most individuals today use social media sites, this is one of the most recent techniques for phishing attacks. Social media phishing may take place in a number of ways, including account hijacking, frauds, the dissemination of malware, and impersonation assaults directed at victims [10]. As social media is located outside the network perimeter, this kind of attack takes more time to identify and block these threats than the other strategies [29].

1.12. Spear Phishing

Spear phishing targets a person, entity or organization [27]. The attacker picks a target and allures him or her into divulging sensitive information. The spear phishing also involves carefully created emails. These emails may contain information targeting specific organizations or

individuals [16]. There can be varying levels of personalization involved in spear phishing such as addressing the victim by its name, or involving impersonation. In the email template, the artists ending to the e-mail is mentioned to be flexible and the attacker may adapt it to the specific recipient. In the email, the information may be belonging to the target such as name, position held and employer among other details would have to be provided.

The most obvious channels of spear phishing attacks are social networking websites such as LinkedIn where it would be easy for them to find out the details of the person's profession[10].

Man-in-the-middle attack

An attacker sits in between the communicating entities and gains access to the sensitive information [27]. When the parties exchange information, they are intercepted and using various techniques of social engineering and traffic analysis, sensitive information can be obtained.

Whaling

In such type of attack, the assailant pretends as a senior member of an organization [27]. The victim are generally the other employees of the organization. For instance, whaling happens when an attacker targets a CEO or other executive. Before the actual attack, the attacker spends a great amount of time profiling the target. Like other types of attacks, the attacker would send the victim an email and try to convince them to give information [6]. Due to the focus on the highest-ranking executives, this attack is recognized as a very risky endeavor. The reason is that such bands deal with the most critical information about the company. The whaling is reported is 20% of the total phishing attacks [27]

Pharming

Another kind of phishing attack is pharming. It doesn't target any specific people using this method as compared to other methods. However, even without needing to target any particular person specifically, the assault might harm a vast number of individuals [6]. Pharming may be carried out in one of two ways. In the first technique, the attacker emails a piece of code to the target that alters all of the local host files. The host files would change the URLs into numerical strings so that the system could utilize them to access websites. Despite inputting the proper URL, this results in a redirect to the malicious site for the target. In the second type of attack, which is known as DNS Poisoning. This method actually affects the domain name system table and does not affect the local host files of the machine. The result of these manipulation is that the target ends up being taken to negative websites. The victim thinks that they are going to genuine sites; however, with DNS poisoning, they are directed to malicious ones [10].

URL Based Phishing

Attackers are coming up with novel techniques to deceive end-users. One of the techniques is to design a innocent looking URL similar to a genuine / benign URL [17]. For instance, for www.facebook.com, they can design a URL www.faceb00k.com. To design a fake URL, the attacker uses several techniques as follows [17,19]:

- The attacker may use SQL injection or cross-site scripting.
- The attacker may use an organization name with a different top level domain (TLD)
- The attacker may use a different protocol such as shttp instead of http
- The attacker my design a URL by slightly changing the spelling
- The attack may hide the URL in href part of the link and provide text such as "Click here" to user
- Combo squatting can be done where the attacker registers a domain explicitly to launch a phishing ttack
- The attacker may use tinyrul to shorten a URL

Anti-Phishing Solutions

Numerous tools are available to combat phishing attacks. The anti-phishing solutions are also known as phishing assault solutions. Phishing prevention and phishing detection are the two primary categories of anti-phishing solutions. In various studies, approaches such as multi-factor authentication and mitmproxy has been used for anti-phishing [27]. Similarly, a number of datasets have been developed to detect URL based phishing such as PhishTank, Alexa, JoeWein, CommonCrawl and OpenPhish [17].

Finally, there are various phishing detection tools available in the market. The primary function of these tools is to recognize and exclude phishing sites. Such toolbars can be viewed by the user as additional tools that are normally embedded in web browser. A warning informs the user about the risks of accessing a phishing site is displayed.

We now discuss the popular phishing detection techniques first. This is followed by phishing prevention techniques.

Phishing Detection

It is very important to identify a phishing attack. Various solutions have been proposed in literature. We can classify the existing approaches to detection of a phishing URL as follows[17,19]. Figure 4 provides a summary of these approaches.

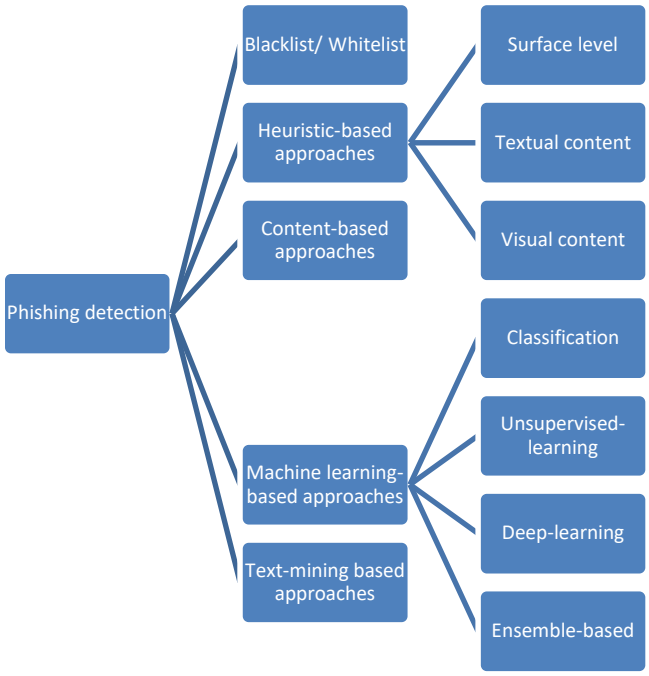

Figure 4: A summary of phishing detection techniques

Blacklist/ White listing

The simplest technique is to black-list those URLs that are most likely to be phishing websites [23]. For this purpose various types of features of URL such as length of the URL, binary features, suspicious words, special symbols, brand names, protocol and data URI can be used. However, these approaches are unable to detect zero-day phishing sites. In some studies, string matching solutions have been proposed [24].

An approach to handle this is that the given blacklist, the list of phishing websites is frequently updated. However, normally these webpages are entered and updated by the system manually. Blacklists are particularly useful for trivial usage because they are very accurate. However, as discussed earlier, one major disadvantage of using blacklists is that they can seldom find websites which are involved in phishing for a short time. Besides this, the blacklist cannot identify the phishing website if no one has reported of the phishing website.

Heuristic-based approaches

Another approach is the heuristic approach for phishing identification. The website's contents are examined using the heuristic-based technique. Surface level content, textual information and visual content are the three different types of heuristic-based approaches. The surface-level content heuristic just looks at the website's URL. The textual content heuristic analyzes the keywords or words used on the page. The last visual content heuristic is looking at the website's design.

Content-based approaches

In such type of attack, the actual content of the subject is checked for phishing. For instance, in a number of approaches, the content of the website is analyzed for detection. Features such as login form, tag type, hyperlink, CSS and images are used to classify phishing attacks [24]. One can also consider the factors such as the age of a domain or the number of occurrences in search result to detect the phishing URL [19]. Similarly, the content of an email can be analyzed to detect phishing [27].

Machine learning based detection

Different machine learning based solutions have been proposed for detection of phishing. [28] classified these approaches as those based on classification, clustering, anomaly detection, which are again then based on URL based and content-based approaches. Below, we discuss some of the approaches for machine learning based detection of phishing attacks.

Classification based approaches

[20] has proposed a layered solution based on machine learning for detection of phishing attacks. The authors used support vector machines, XG Boost, random forest, ANN, linear regression, decision trees, Naïve Bayes and support vector machine algorithms for detection of phishing attacks. For instance, LSTM has been used in various studies to detect phishing based on the URL information [17]. Besides that, hybrid features from both URL and HTML content can be used to detect phishing. In [19], PhishHeaven has been proposed as a machine learning solution for detection of phishing URL.

Unsupervised-learning techniques

Anomaly detection based on un-supervised learning using auto-encoders have been cited in various studies [17].

Deep learning-based approaches

Using machine learning can detect based phishing. However, machine learning requires manual feature-engineering and is a tedious job. For this reason, several deep learning based solutions have also been proposed. The authors in [23] proposed an NLP and deep-learning based solution for detection of phishing attacks. They used GLOVE embeddings and evaluated different algorithms such as LSTM, BiLSTM, GRU and BiGRU. A machine learning technique based on HTTP headers for detecting phishing attacks have been presented in [24]. According to [24], deep neural networks, CNN, RNN, LSTM, GRU, auto-encoders, restricted Boltzman machines and deep belief networks have been proposed for detection of phishing attacks.

Ensemble-based approaches

In various studies, ensemble based approaches have been proposed that combined multiple machine learning classifiers and then used voting or other approaches for detection of phishing attacks For instance a novel approach to detect phishing has been presented in [31].

Text-mining based approaches

Several techniques based on text mining has been proposed in literature for phishing detection. For these approaches, techniques such as TF-IDF, regular expression, latent semantic analysis, and topic models have been used [28].

Phishing Prevention

Phishing prevention can be performed via software or user awareness. We now discuss these two techniques in detail.

Phishing prevention using software

Phishing prevention of this type involves adding an additional layer of protection upon user as they login to the website in order to stop phishing attacks. An example is two-factor authentication, which verifies a user's identity before allowing access to their login account on a website, adds an additional degree of protection [4].

Education

Education is one of the crucial approach to ensure the avoidance of phishing [5]. APWG and Carnegie Mellon University has came up with various users' anti-phishing education program. To warn users about phishing, further educational initiatives include the development of games and training simulations.

Auditing and Policy

The auditing and policy approach ensures various security policies and practices are put in place in businesses to help staff in spotting cyber-attacks. Generally, these security regulations are governed by policies that let personnel make decisions regarding the nature of a possible action [10]. The policy approach can be regarded as a defensive tactic to manage employee behavior while being attacked online.

Training and Awareness (ETA)

Auditing and policy procedures are effective only when they are implemented together with awareness, education, and training programs. User is provided training on how to be attentive and

identify a phishing attack while they are doing regular activities and interacting with other users online. It is identified that training emails embedded with text and graphics are proven to be effective [28]. IQ test experiments can be designed as well to help users in identifying phishing emails.

Consumer Awareness

Finally, the end-user must be made aware of the need of keeping their user credentials private and in a safe place. In the event of any suspicious developments in their business or bank account, they should provide credential to the cyber security unit as soon as feasible [4].

Phishing and Human Factors

In this section we will discuss various studies on human factors involved in phishing. We will discuss the psychological aspects related to phishing

Simulations

In [16], authors have developed a simulation environment called SpearSim to study the spear phishing attacks. The simulation identifies that people with high information availability are more susceptible to spear phishing.

Behavioral studies

In another study[21], Nigerian universities were selected to determine the impact public beliefs, age, status and gender. It was found that these factors doesn't influence the scam susceptibility and vulnerability rates. The authors also discussed various psychological factors impacting the success of a phishing attack. These factors include neuroticism, extroversion, openness, agreeableness, and consciousness.

Psychological factors

[28] has identified what personal and contextual attributes make people prone to phishing attacks. They identified that curiosity and urgency are very important tenets. Stress also plays a very important role. Older people are found to be less impulsive to emails. Gender is also found to play a significant role.

4. Discussions & Emerging trend

The paper has discussed various types of phishing attacks and their counter-measures. Based on the study, following are important findings. Deep learning algorithm have been highly effective in countering and detecting phishing attacks.[1]. Most of the phishing attacks (around 96%) are currently being conducted via emails. In those emails, malicious links are created and sent through emails. When the user clicks on those links, they are redirected to a malicious webpage or a file attachment. In addition, attackers may send malicious software/ files as attachment to emails that can be used to further launch ransomware attacks/ malware attacks [17]. It is very difficult to

prevent phishing attack currently. But, most of them can be avoided reduces through proper awareness among the end-users. They can be educated about the precautions and necessary steps to follow while being present over the internet.

The large share of phishing attacks are targeted towards financial services [17], then on shipping, cloud storage services and payment services. We now turn our discussion on two popular emerging trends in phishing.

Phishing attacks and generative AI

We must end the discussion with a note on the use of generative AI in developing phishing attack. [18] have discussed how phishing attacks can be generated using ChatGPT. The severity of such incidence stems from the fact that these tools are not detected by anti-phishing software. [19] has also stressed on the fact that AI tools can be used to generate phishing URLs. [24] also highlighted similar issue where the generative AI tools can be used to clone a website, generate phishing code, obfuscation and other phishing steps. For resolving phishing issues, several AI-based and LLM based solutions have been proposed in [32,33].

Phishing and blockchain

Blockchain is also facing severe forms of phishing attacks and is a major cause of concern[22]. According to various studies, more than 50% of attacks on Ethereum blockchains are phishing attacks. Amongst the various solutions to address phishing attack in blockchain is the consensus based protocol. Several machine learning and deep learning based solutions have also been proposed. For a detailed comparison of various approaches, readers are referred to [22].

5. Conclusion

Phishing attacks target private information like usernames, passwords, and financial information, and they present a serious risk to people and organizations all over the world. Over time, these attacks have become more complex. Hence, it's critical to keep informed on the most recent defenses. Specifically, with the advancement in society and the modern transformations coming up, the importance of anti-phishing solutions can’t be denied. Hence, this paper presented a systematic literature review on phishing attacks, their detection and counter measures.

The findings of the literature research showed that the various techniques and procedures proposed in literature may help in effectively identify and stop phishing assaults. In terms of popularity, deep learning algorithms, machine learning methods, and different heuristic approaches have been found to be very effective. The paper also highlighted various emerging trends in phishing.

In a nutshell, this survey paper provides a comprehensive analysis of phishing attacks and the countermeasures used. It also highlights the significance of user education, technological

advancements, and the implementation of multiple defense mechanisms that can be used to reduce the likelihood of falling prey to a phishing attack.

References:

[1] Apandi, S. H., Sallim, J., &Sidek, R. M. (2020, February). Types of anti-phishing solutions for phishing attack. In IOP Conference Series: Materials Science and Engineering (Vol. 769, No. 1, p. 012072). IOP Publishing.

[2] Rikzan, F. I. F., &Zolkipli, M. F. (2023). A Study of Phishing Attack towards Online Banking. Borneo International Journal eISSN 2636-9826, 6(1), 65-72.

[3] Vanitha, G. Detection of Phishing Attack.

[4] Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. Prevention.

[5] Vega, J., Shevchyk, D., & Cheng, Y. A Literature Survey of Phishing and Its Countermeasures.

[6] Shankar, A., Shetty, R., & Nath, B. (2019). A review on phishing attacks. International Journal of Applied Engineering Research, 14(9), 2171-2175

[7] Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise Credential Spear-phishing attack detection. Computers & Electrical Engineering, 94, 107363.

[8] Asaad, R. R., & Saeed, V. A. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. Applied computing Journal, 227-244.

[9] Alsufyani, A. A., &Alzahrani, S. M. (2021). Social Engineering Attack Detection Using Machine Learning: Text Phishing Attack.

[10] Salahdine, F., &Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

[11] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques–a review of Cyber Defense Mechanisms. IJARCCE, 11(7), 153-160.

[12] Desolda, Giuseppe, et al. "Human factors in phishing attacks: a systematic literature review." ACM Computing Surveys (CSUR) 54.8 (2021): 1-35.

[13] Sameen, M., Han, K. and Hwang, S.O., 2020. PhishHaven—An efficient real-time AI phishing URLs detection system. IEEE Access, 8, pp.83425-83443.

[14] Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S. and Porras, J., 2023. Mitigation strategies against the phishing attacks: A systematic literature review. Computers & Security, p.103387, Elsevier

[15] Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J. and Linkman, S., 2009. Systematic literature reviews in software engineering–a systematic literature review. Information and software technology, 51(1), pp.7-15.

[16] Xu, T., Singh, K. and Rajivan, P., 2023. Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. Applied Ergonomics, 108, p.103908., Elsevier

[17] Asiri, S., Xiao, Y., Alzahrani, S., Li, S. and Li, T., 2023. A survey of intelligent detection designs of HTML URL phishing attacks. IEEE Access, 11, pp.6421-6443., IEEE

[18] Roy, S.S., Naragam, K.V. and Nilizadeh, S., 2023. Generating phishing attacks using chatgpt. arXiv preprint arXiv:2305.05133.

[19] Sameen, M., Han, K. and Hwang, S.O., 2020. PhishHaven—An efficient real-time AI phishing URLs detection system. IEEE Access, 8, pp.83425-83443.

[20] Shaukat, M.W., Amin, R., Muslam, M.M.A., Alshehri, A.H. and Xie, J., 2023. A hybrid approach for alluring ads phishing attack detection using machine learning. Sensors, 23(19), p.8070.

[21] Yoro, R.E., Aghware, F.O., Akazue, M.I., Ibor, A.E. and Ojugo, A.A., 2023. Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. International Journal of Electrical and Computer Engineering, 13(2), p.1943.

[22] Joshi, K., Bhatt, C., Shah, K., Parmar, D., Corchado, J.M., Bruno, A. and Mazzeo, P.L., 2023. Machine-learning techniques for predicting phishing attacks in blockchain networks: A comparative study. Algorithms, 16(8), p.366., MDPI

[23] Benavides-Astudillo, E., Fuertes, W., Sanchez-Gordon, S., Nuñez-Agurto, D. and Rodríguez-Galán, G., 2023. A phishing-attack-detection model using natural language processing and deep learning. Applied Sciences, 13(9), p.5275.

[24] Begou, N., Vinoy, J., Duda, A. and Korczyński, M., 2023, October. Exploring the dark side of ai: Advanced phishing attack design and deployment using chatgpt. In 2023 IEEE Conference on Communications and Network Security (CNS) (pp. 1-6). IEEE.

[25] Shukla, S., Misra, M. and Varshney, G., 2024. HTTP header based phishing attack detection using machine learning. Transactions on Emerging Telecommunications Technologies, 35(1), p.e4872., Wiley

[26] McConnell, B., Del Monaco, D., Zabihimayvan, M., Abdollahzadeh, F. and Hamada, S., 2023, June. Phishing Attack Detection: An Improved Performance Through Ensemble Learning. In International Conference on Artificial Intelligence and Soft Computing (pp. 145-157). Cham: Springer Nature Switzerland.

[27] Arshad, A., Rehman, A.U., Javaid, S., Ali, T.M., Sheikh, J.A. and Azeem, M., 2021. A systematic literature review on phishing and anti-phishing techniques. arXiv preprint arXiv:2104.01255.

[28] Aleroud, A. and Zhou, L., 2017. Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, pp.160-196.

[29] Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I., 2021. Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, p.563060.

[30] Mangut, P.N. and Datukun, K.A., 2021. The current phishing techniques–perspective of the nigerian environment. World Journal of Innovative Research, 10(1).

[31] Basit, A., Zafar, M., Javed, A.R. and Jalil, Z., 2020, November. A novel ensemble machine learning method to detect phishing attack. In 2020 IEEE 23rd International Multitopic Conference (INMIC) (pp. 1-5). IEEE.

[32] Eze, C.S. and Shamir, L., 2024. Analysis and prevention of AI-based phishing email attacks. Electronics, 13(10), p.1839.

[33] Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J. and Park, P.S., 2024. Devising and detecting phishing emails using large language models. IEEE Access.