future internet

MDPI

Review

Phishing Attacks Survey: Types, Vectors, and Technical Approaches

Rana Alabdan

Department of Information Systems, College of Computer and Information Sciences, Majmaah University, Majmaah 11952, Saudi Arabia; r.alabdan@mu.edu.sa

Received: 4 September 2020; Accepted: 27 September 2020; Published: 30 September 2020

Abstract: Phishing attacks, which have existed for several decades and continue to be a major problem today, constitute a severe threat in the cyber world. Attackers are adopting multiple new and creative methods through which to conduct phishing attacks, which are growing rapidly. Therefore, there is a need to conduct a comprehensive review of past and current phishing approaches. In this paper, a review of the approaches used during phishing attacks is presented. This paper comprises a literature review, followed by a comprehensive examination of the characteristics of the existing classic, modern, and cutting-edge phishing attack techniques. The aims of this paper are to build awareness of phishing techniques, educate individuals about these attacks, and encourage the use of phishing prevention techniques, in addition to encouraging discourse among the professional community about this topic.

Keywords: phishing attacks; phishing types; phishing vectors; phishing technical approaches

1. Introduction

Phishing is a social engineering technique that, through the use of various methodologies, aims to influence the target of the attack to reveal personal information, such as an email address, username, password, or financial information. This information is then used by the attacker to the detriment of the victim [1]. The term phishing is derived from the word "fishing", spelt using what is commonly known as Haxor or L33T Speak. The logic of this terminology is that an attacker uses "bait" to lure the victim and then "fishes" for the personal information they want to steal.

The first instance of this technique was reported in 1995 when attackers used phishing to convince victims to share their AOL account details [2,3]. The word "phishing" was first printed in media in 1997 [4]. Subsequently, phishing has grown and developed. Attackers have devised new methods and utilized new media, and it is now one of the primary attack vectors used by hackers.

As of 2018, Symantec found that email-based phishing rates had fallen to 1 in 3207 emails, from 1 in 2995 emails in 2017 and 1 in 392 in 2013 [5,6]. The proportional incidence of this generic type of phishing attack consistently fell during the past four years; however, this may in part be due to a greater number of emails being sent rather than a reduction in phishing attempts. Despite this apparent decrease in phishing attacks, the APWG (the Anti-Phishing Working Group) reported that phishing rates rose to their highest levels since 2016 in the third quarter of 2019 [7,8]; the trends in unique phishing websites between 2013 and 2019 can be seen in Figure 1. Furthermore, phishing attacks continue to be widely utilized; for example, spear phishing is the most common infection vector for the distribution of malware, used by 71% of groups in 2018 and 65% of groups in 2019 [9], as can be seen in Figure 2. Furthermore, the number of phishing Uniform Resource Locators (URLs) increased by 20% between 2017 and 2018 [6], with two-thirds of these phishing sites now utilizing a Secure Sockets Layer (SSL). This was the highest rate since 2015, leading to the new and concerning conclusion that https is no longer a suitable indication of a site's safety [7].

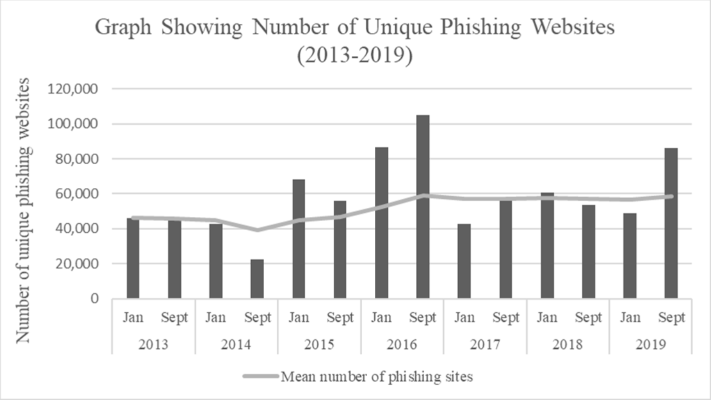


Figure 1. Number of unique phishing websites between 2013 and 2019.

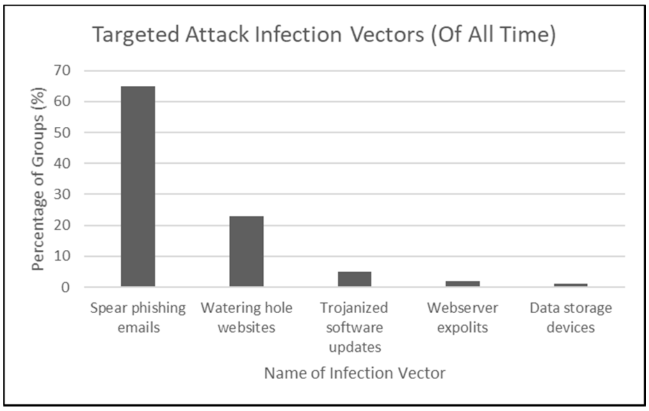


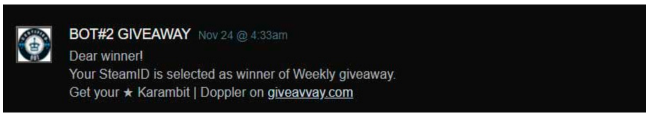
Figure 2. Targeted attack infection vectors (Anti-Phishing Working Group).

In recent years, the main focus of phishers has been SaaS (Software as a Service) and webmail, which accounted for 33% of the attacks against a range of industry sectors [8]. IBM identified that 27% of phishing attacks in 2018 were focused on webmail services. It was also noted that 29 percent of the attacks against businesses that were analyzed by X-Force identified the source of the breach as a phishing email [10].

Regarding the financial aspects of phishing, Symantec found that in the underground economy "custom phishing page services" are being sold for between USD 3 and 12 [6], indicating that the overhead for setting up a custom phishing attack is minimal. It has also been found that gift cards are now among the most common ways for a scammer to cash out their earnings [7]. The FBI estimated the 2018 victim loss due to phishing was USD 48,241,748, with 26,379 people affected by this type of scam [11].

In 2018, the FBI received around 100 complaints, with the most commonly targeted industries being healthcare, education, and air travel, which resulted in a combined net loss of approximately USD 100 million dollars. This scam involved the use of phishing emails to target employees and discover their login credentials. These were then used to gain access to the payroll system, after which rules were implemented by the phishers so that employees no longer received notifications about changes made to their accounts. The phisher was then able to change account holders' direct debit information to funnel the funds into their own account, which in this instance involved a prepaid card [10].

From industries such as healthcare and education to individuals playing games online, the impacts of phishing attacks are widely felt. An example is a phishing scam that aimed to steal the user login credentials for Steam (a PC gaming platform) by offering a "free skin giveaway" (Figure 3). The scam was initiated by a comment left on a user's profile, which once clicked directed the victim to the phishing site with information about the giveaway and even a fake scrolling chat bar to give an impression of legitimacy. Here the victim was prompted to "login via Steam", which took them to a fake login screen where their credentials were captured. The attack extended to generating a real Steam guard code (i.e., two-factor authentication), which granted the phisher access to the victim's account to sell items and further promote the scam (see Figure 3) [11]. MMOs (massive multiplayer online games) are also a common target for phishers as "loot box" style goods can be sold on the online black market. An example of this type of phishing scam recently targeted the MMO Elder Scrolls Online [12].



BOT#2 GIVEAWAY Nov 24 @ 4:33am
Dear winner!
Your SteamID is selected as winner of Weekly giveaway.
Get your ★ Karambit | Doppler on giveavvay.com

Figure 3. Examples of Steam phishing attempts.

Phishing also played a part in the first successful cyber attack on a power grid, which took place in Ukraine in December of 2015. IT staff and network administrators of various companies that handled power distribution for Ukraine were targeted with spear phishing attacks. The attack involved a malicious Microsoft Word document that provided a prompt to enable macros. Once clicked, the macro installed the malware BlackEnergy3 on the system, thus providing a backdoor for the attackers. This eventually resulted in the successful shutdown of 30 substations and left 230,000 people without power for up to six hours. This example demonstrates how powerful and devastating a well-planned and well-executed phishing attack can be. It is also clear even trained IT professionals cannot always identify these types of attacks [13].

The above discussion indicates that phishing is a major problem that needs to be comprehensively understood to be combated. Therefore, this paper reviews a broad range of characteristics from classic, current, and cutting-edge phishing techniques, including identifying areas in which anti-phishing techniques are missing or lacking. It is also hoped that this paper will encourage the adoption of preventative phishing practices by raising the awareness of the types of phishing techniques that exist, especially on an individual level.

To foster better understanding, the phishing techniques discussed in this paper are split into three key groups that are interconnected. These are:

1. The medium
2. The vector
3. The technical approach

This grouping is used to highlight the fact that certain vectors can be used on certain media and only specific technical approaches can be used on specific vectors.

The remainder of the paper is broken down into various sections. Section 2 consists of a literature review containing information about the different types of phishing approaches. Section 3 outlines the various phishing methods and techniques. Section 4 details the various phishing resources, Section 5 outlines the more general anti-phishing techniques, Section 6 outlines phishing in relation to cyber resilience, Section 7 discusses the current challenges and trend of phishing attacks, and finally, Section 8 contains the concluding remarks.

2. Literature Review

This section contains a review of the relevant literature. At present, several papers exist regarding phishing; of these, the most recent and comprehensive is that of Chiew et al. [14]. However, there is an overall lack of published papers, as can be seen in Figure 4, which shows the number of phishing-related papers published per year by the Institute of Electrical and Electronics Engineers (IEEE).

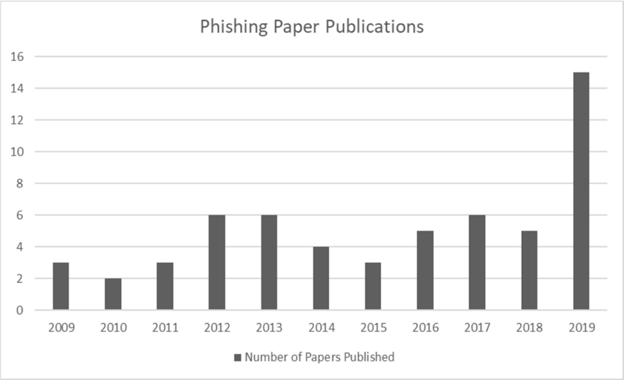


Figure 4. Number of phishing papers published by year in IEEE (the Institute of Electrical and Electronics Engineers) Access.

As Chiew et al. pointed out in their 2018 paper, researchers have tended to publish findings about anti-phishing techniques rather than discuss the phishing techniques themselves [14]. Nonetheless, a selection of reviews relating to phishing have been published in recent years [15–19]. Phishing has been described as having a lifecycle, that is, a phishing attack can be broken into stages [15,16,19]. These are often summarized as follows:

1. Planning—this involves identifying the targets, the information sought, and creating/identifying the tools and techniques that will be used in the attack (such as emails with malicious links and the spoof sites these links direct to).
2. Phishing—the stage during which the identified targets are phished using the resources created in Stage 1.
3. Infiltration—depending on the method used, this stage will vary but it essentially consists of the response from the target and gaining access to the personal information sought.
4. Data collection and exploitation—this is the stage at which the phisher extracts the information sought and utilizes it to achieve the ends established during the planning phase. This often involves fraud whereby the attackers impersonate the victims to access their accounts, etc. Another common occurrence is the selling of this personal data on the online black market.
5. Exfiltration—finally, the phisher attempts to remove as much evidence of their attempt as possible (such as the deletion of fake sites). There may also be some analysis on the success of the attack and assessment of future attacks.

Mohammad et al. simplified this process to a three-stage lifecycle of planning (Stage 1 above), collection (essentially Stages 2 and 3 of the above lifecycle), and fraud (Stages 4 and 5 above) [20]. In 2014, Chaudhary [17] reviewed the literature related to phishing, damage caused by phishing techniques, anti-phishing techniques, and the effectiveness of these techniques. Although thorough, this paper did not provide details about the technical approaches of phishing and did not include more modern techniques such as QRishing.

Suganyas's 2016 [18] paper provided a brief overview of phishing techniques, but more attention was given to anti-phishing techniques. The details of each method were also not comprehensively discussed, and a high-level overview was instead provided.

Purkait (2012) [19] provided a detailed review of the literature regarding these anti-phishing techniques through the analysis of 358 papers and 16 doctoral level theses. This review also focused almost solely on the preventative and protective measures rather than the technical approaches used by the phishers. It found that current anti-phishing techniques were widely deployed across the internet, and that all of the current approaches were purely preventative measures. Other papers have also explained phishing in relation to the wider area of social engineering [8,21].

In 2007, Singh examined the emergence of new phishing techniques in the banking sector [22]. These techniques were grouped into four categories [23]:

- The dragnet method
- The rod and reel method
- The lobsterpot method
- The gillnet phishing method

Of these categories, dragnet phishing is the use of spam email to target a mass audience, which causes pop-ups or websites bearing legitimate identity elements (e.g., logos) to illicit an immediate response.

The rod and reel method targets victims who have already been contacted and the target is prompted into revealing personal details via the use of false information.

The lobsterpot method utilizes a spoofed website identical to the legitimate site so that the victim willingly provides their personal details believing they are logging into the legitimate site.

The gillnet phishing method involves introducing malicious code into websites and email to infect the target's device. An example is the introduction of a trojan or keylogging virus caused by opening an email, or the manipulation of system settings so that when a user attempts to access a legitimate site they are redirected to a spoofed site as used in the lobsterpot method.

Phishing, being a form of cyber attack, can be classified within the classification structures of other attack models. For example, if we apply the model proposed by Hausken et al. [24], we can see that depending on the method of phishing applied and the phisher's end goal, phishing can fall into a variety of categories. The 5 categories identified by Hausken et al. that apply to phishing attacks are:

(1) Attacks against a single element—easily done with phishing just target one of the people who has access to the element and use their credentials to destroy, edit, or copy the element.
(2) Attacks against multiple elements—more difficult, but if the phisher manages to phish someone within the organization who is more senior than the people with access to the elements, they could assume their identity and utilize their authority to order the destruction of these elements.
(3) Consecutive attacks—using a series of attacks to destroy elements can be achieved with phishing as the method of infiltration. However, when the attacks start, if phishing is found to be the cause, additional infiltration may become harder.
(4) Random attacks—one of most common methods of phishing. Spam uses random attacks to steal the credentials of anyone who falls for the bait.
(5) Combination of intentional and unintentional impacts.

Categories 6 and 7 (incomplete information and variable resources, respectively) do not directly relate to phishing attacks.

Furthermore, when we consider the system structures that phishing can be applied to, we see a difference between phishing attacks and the other papers that Hausken et al. considered. Phishing can be applied to any of the 8 system structures outlined as phishing based on the flaw in human nature and not technology itself. Provided a person has the authority to do what the phisher wants to achieve, then with enough effort, planning, and the combined use of one or more phishing techniques and social engineering; then the infiltration or destruction of any of the system structures should be achievable. These system structures are defined by Hausken et al. as: single element, series systems, parallel systems, series-parallel systems, networks, multiple elements, interdependent systems, and other types of systems. Obviously, some of these will be easier for a phisher to destroy than others. Some particularly tricky systems would be a parallel system (where all the elements need to be destroyed to destroy the system) or multiple elements (where none of the elements are linked).

3. Phishing Methods and Techniques

The overall technique of phishing can be broken down into three constituent components:

- The medium
- The vector
- The technical approach

These components are interlinked, with some vectors only suitable for certain media and some technical approaches only suitable for specific attack vectors. The medium can be summarized as the means by which the attacker communicates the phishing attack to the victim; this is further discussed in Section 3.1.

The vector is the avenue of attack and is often limited by the medium. This is outlined further, with discussion of the various types of vectors, in Section 3.2. The technical approaches are the methods deployed during the attack, which are often used in conjunction with social engineering techniques to enhance the attacker's chance of success, for example, cross-site scripting (XSS) or browser vulnerabilities.

3.1. Phishing Media

The medium used is the first consideration in phishing attacks. The medium limits the vectors and technical approaches (explored more in later sections) that can be applied. The medium itself is the method by which the phisher interacts with the target. There are three key media through which this interaction can take place, these are:

- Voice
- Short messaging service (SMS)/multi-media messaging (MMS)
- Internet

Voice, that is, speech and the use of language, is one of the oldest and most effective methods by which humans interact and convey information. It is often said that the use of language is what sets humans apart from other sentient creatures. Thus, it can be expected that this medium can be utilized to deceive individuals into revealing their personal information to those who wish to utilize it for their own benefit.

In its modern form, SMS (short messaging service) is known as "texting". This involves communication through the use of short text-based messages, sent through a mobile network. This later developed into MMS (multi-media messaging service), which allows the transfer of content in addition to text, such as photos, videos, or audio clips [25,26]. This medium provides a number of convenient ways in which a phisher can interact with targets and attempt to steal their personal data [27].

The final medium considered is the internet. From its inception as the ARPANET [28] to the nebulous mass of websites now available, the constantly changing and developing nature of the internet means new methods of communication are being continually devised. This collection of communication methods is available in one convenient location and ranges widely from email to Instagram and Snapchat [29], each of which provides a means for phishers to "hook" potential victims. In the following section the specific vectors and channels that utilize these different media are discussed.

3.2. Phishing Vectors

As stated above, vectors are dependent upon the medium the attacker is using and is the channel through which the phishing attack is conducted (see Figure 5).

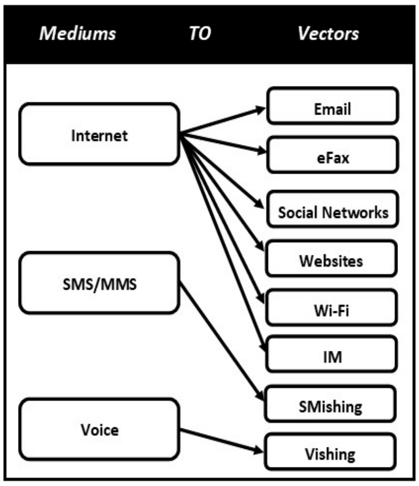


Figure 5. How media map to vectors.

3.2.1. Vishing

Vishing is the method of phishing that involves the use of voice. Although the use of a telephone to attempt an individual scam is not new, the introduction of voice over IP (VoIP) technology resulted in an increase in this practice. Vishing itself uses the ability to spoof a number so that a call IMappears to originate from a legitimate source. VoIP is used to obscure the actual physical location from which the call originates, and the victim is then manipulated into revealing information. VoIP and modern technologies have facilitated this form of deception because the cost of calls—including international calls—is negligible. Furthermore, the use of automation systems further improves the phishers attacks by making them indistinguishable from legitimate calls [30]. There are many reasons this method of phishing is successful [31], for example:

- Trust—telephones have a greater record of trust. In a 2007 survey, a phone call was rated the least suspicious form of communication [10].
- Automation—acceptance of automated telephone systems.
- Call centers—the extensive use of call centers means people are accustomed to strangers calling and asking for personal details. This also reduces the suspicion of phishers with foreign accents.
- Victim age—a larger share of the globally aging population is accessible through telephone than by email. This is also a demographic that is easier to manipulate.

3.2.2. Smishing

The medium of SMS/MMS is responsible for the vector of smishing. This is the use of the short messaging service to implement phishing attacks. There are two main approaches using this methodology. The first method involves sending a SMS pretending to be a trusted authority (such as a bank, etc.) containing a vital message, e.g., regarding the message recipient's identity or theft of banking information. The victim is then directed to a fraudulent website or phone number, which requires the victim to login or provide some identifying information. Once this has occurred, attackers can then use the details they have gathered to their own benefit.

The other method involves the sending of a text to a victim that either directly contains malware or provides a link to a website that contains malware. Once the malware is installed, the phisher can continue with their attack, which may range from simply stealing the target's contacts and messages, to creating a bot-net or accessing authentication codes for logins or purchases [30,32].

3.2.3. Email

The medium that comprises the widest range of vectors is, predictably, the internet. The first vector to consider is that of electronic mail (email). With this vector, specially crafted emails are distributed to targets enticing them to perform actions that will make their personal data available to the attacker. Email is an advantageous vector for phishers because emails can easily be distributed to a large quantity of recipients. Furthermore, it allows the geographical location of the sender to remain unknown. An outline of this technique can be seen in Figure 6. There are also a wide range of technical approaches that phishers can take when using this vector, such as address spoofing, etc. These will be further discussed in Section 3.3.

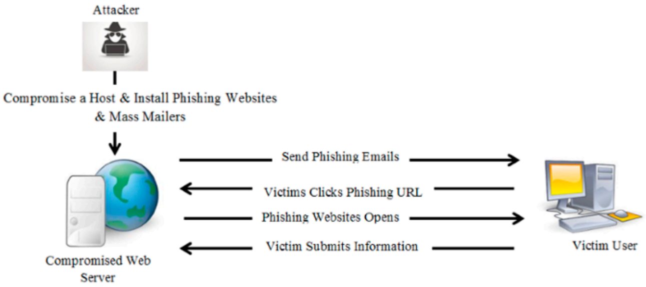

Attacker
Compromise a Host & Install Phishing Websites & Mass Mailers
Send Phishing Emails
Victims Clicks Phishing URL
Phishing Websites Opens
Victim Submits Information
Compromised Web Server
Victim User

Figure 6. Outlines of email phishing attacks [13]. Reprinted by permission from Springer Link: Telecommunication Systems, (Defending against phishing attacks: taxonomy of methods, current issues and future directions, Gupta et al.), [COPYRIGHT] (2018).

3.2.4. EFAX

eFax is similar to a traditional fax although without the need for a fax machine. Sites such as efax.com utilize IP (internet protocol) to transmit faxes, in comparison with traditional methods that utilized phonelines. The advantage of this method is that faxes can be sent to a recipient's machine as emails, thus removing the need for a fax machine. However, due to the online nature of this method of communication it opens a new avenue by which phisher attacks can be made to attain victims' personal information [33].

3.2.5. IM

Instant messaging (IM) was one of the earlier forms of online communication, first implemented as IRC (internet relay chat). Subsequently, instant messaging systems such as MSN Messenger and Yahoo! Messenger were devised. At the present time, these forms of instant messenger are usually combined with other social media, such as Facebook messenger, although instant messenger clients that are not linked directly to social media, such as WhatsApp and Telegram, also remain in use. Messages are now not just text based but can include emojis, photos, gifs, files, and hyperlinks. Moreover, the IM client may also provide features for audio and video calling. This method of communication is now far more popular than SMS messages, making it an ideal environment for phishers. Online, real-time chat allows phishers to engage a victim and induce them to reveal personal details via scams such as the commonly used "your account has been locked/hacked please enter your login details".

3.2.6. Social Networks

From the beginning of the 21st century, social media has grown significantly and allows people to communicate, connect, and share their experiences. Examples are Twitter, Facebook, and LinkedIn, which allow users to connect and identify other users who share the same interests, life outlooks, or hobbies. The main use of these platforms, however, is to follow the posts of real-world identities. Niche social media platforms exist that are dedicated to specific areas, including sites such as Pinterest and Tumblr. This nature of sharing personal details online is an excellent resource for phishers to identify groups of targets and potentially approach victims.

3.2.7. Websites

Fraudulent websites are another source of phishing attack. These sites appear to be legitimate and are used to harvest victims' personal details when the victim attempts to login. Various methods can be used by an attacker, as explained in Section 3.3. Furthermore, as the general users of the internet are more inclined to believe that phishing attacks are mainly carried out through emails and other messaging services, they tend to be less security conscious when visiting websites, as such making them vulnerable to these types of phishing attacks [32,34].

3.2.8. Wi-Fi

Wi-Fi phishing usually takes place in public hotspots, and as such is normally a non-targeted form of phishing attack. However, this vector could also potentially be used in a spear phishing (or perhaps whaling) attack, where a specific public hotspot is chosen because a given target regularly visits and uses the Wi-Fi [35].

Wi-Fi phishing can take several forms. The usual form involves installing malware on the victim's device to harvest credentials or redirect to spoofed sites, much like the other forms of phishing outlined above. There are also methods that intercept traffic on these networks to steal the personal information being transmitted by the people using the public hotspot. This technical approach is discussed in Section 3.3.10.

3.3. *Phishing Technical Approaches*

By using one or more of the vectors outlined above, phishers can employ the technical approaches outlined below to gain access to the victim's personal details.

3.3.1. Spear Phishing

Spear phishing [34] is a targeted approach to phishing in contrast with the generic mass production of spam mail. More accurately, it is a targeted attack against an individual or organization that utilizes specially crafted materials (usually emails that appear to have come from people the victims already know), to improve the chances that the individual who opens the email will be tricked into doing whatever it is the sender desires. To this end the email content must also appear to be innocuous, that is, it must also relate to something the target finds relevant, so that the email and instructions do not raise the suspicion level of the intended victim. The email may refer to the target by name and include information that the target would not suspect others to have access to, in addition to the service the phisher is impersonating. For this purpose, LinkedIn (or other forms of social media) is a common platform for a phisher to conduct research for this type of attack because it is relatively easy to find a target's profession and other personal details. Focusing on specific targets requires additional time and effort in the planning phase by the phisher, but with the advantage of a higher chance of pay off [19]. As described previously, spear phishing remains the largest infection vector [5] for an attack. The attack itself is dependent on the goal of the phisher and may vary from a "click the link" scenario to downloading a malware-laced attachment.

The success of a spear phishing attack relies on fundamental aspects of human psychology. These are:

- Authority—humans tend to comply with demands of authority figures demand.
- Commitment—the principle that once a human has taken a position on a topic, they feel pressured to defend that stance.
- Liking—the principle that people are more likely to do things for people they like (this may be only superficial; for instance, complying with people of their own age or sharing their interests).
- Contrast—this makes an initially unreasonable option seem more appealing because it is preferable to a choice presented in tandem with the first option.
- Reciprocity—humans like to return or reciprocate in kind objects presented to them by another.

- Scarcity—perceived value is used to entice a person to perform a desired action when the availability of this offer is limited.
- Social proof—that is, herd mentality. A person is more likely to follow the majority rather than risk making a mistake.

Use of these principles increases the chance of success of a phishing attack [36,37]. For example, a common technique seen in phishing emails is the use of the scarcity principle. This involves tricking the victim into clicking a malicious link by disguising it as a "once-in-a-lifetime" offer that is only available for a limited time. Because the time to take advantage of this opportunity is limited, the probability of the victim clicking the link immediately, without thinking, is increased. Another commonly seen example is the use of authority. In this scenario, the victim is informed that something has happened (i.e., a successful login attempt from another country), and the victim must first login before this issue can be rectified. In this scenario, the phisher makes a demand from a place of authority with which the victim is expected to comply without question. These principles can also be used in other forms of phishing or manipulation, but in spear phishing attempts, these factors can be applied more accurately.

Several studies have identified that older women are by far the most susceptible to phishing attacks [36,37]. Among the principles outlined above, the most effective methods involve the use of scarcity or authority in all age groups. However, older users show more susceptibility to reciprocation, whereas younger users are more vulnerable to the use of scarcity. Both studies also found that there was a large discrepancy between self-reported susceptibility (indicated as low) and actual susceptibility (found to be high) that was particularly marked in older generations. The most successful area for spear phishing seems to be the legal area, with participants showing a surprising immunity to emails that targeted the subject's finances [37].

Advance Persistent Threats (APTs) are the most likely sources of spear phishing attacks as they have the resources to closely investigate their targets and craft high quality fake emails, as can be seen in their use in Operation Aurora and against the French foreign ministry [38]. Since APTs tend to utilize zero-day exploits, spear phishing attacks are perfect for the distribution of this type of malware because, although this method may be slow, it is a low-profile method of attack. If the attack is successful, the phisher can remain hidden and perform espionage or sabotage, which are often the objectives of an APT.

To create high-quality phishing emails that are relevant to the target, a phisher must first research their victim. There are various methods a phisher may use to achieve this goal. The first is browser sniffing, which reveals the websites frequently used by the target by assessing access time through analysis of cookies, the Domain Name System (DNS) cache, or URLs. If the access time for a particular site is short, then it is likely the target frequents the site. In order to sniff this information, the attacker must first use a website with advertisements or another means to embed JavaScript, such as a Hyper Text Markup Language (HTML) email, to deploy a script which will in turn inform the phisher of the access times for sites. With this information, the phisher can now more carefully craft an email to appear as if it originates from a site the victim is familiar with.

3.3.2. Whaling

Whaling is a targeted method of phishing similar to spear phishing, although it differs in the fact that the sole targets are senior level executives (or other high-ranking employees) whose position provides them with privileged access to data within their company [15,39,40]. Because this is a highly targeted attack, phishers take time to ensure their scam is as indistinguishable from legitimate mail as possible. The most likely vector for this attack is either eFax or email. As in the case of spear phishing, the attacker's goal is to induce the target to install malware to provide access to the target's system. The malware is distributed in the usual manner of an infected attachment or as a link to download the malware. The malware's purpose is to monitor keystrokes and/or grant the attacker access to the infected system from which they can continue their attack, thus utilizing the high-level privileges they have obtained. Whaling itself may only be the preliminary stage of the overall attack, with a rise in what is referred to as business email compromise (BEC), which is further discussed in Section 3.3.3.

3.3.3. BEC

BEC (business email compromise) is a form of phishing attack (a sub-type of spear phishing) that focuses purely on government, non-profit, and commercial organizations to inflict a negative effect (normally financial) on that organization. As the name implies, the aim is to compromise the corporate emails of the employees of the company and use the victim's access to inflict damage; this typically takes the form of data mining and invoice scams. This scheme has a knock-on effect whereby compromising one account can lead to the compromise or manipulation of another, also known as a launchpad attack [41]. It is common for phishers to spend weeks or months inside a company's networks to identify the perfect exploit. This can be done by analyzing, for example, the organization's billing system, its vendors, or a specific employee (preferably a high-ranking executive) [7]. Then, an email is sent requesting the transfer of funds according to the attacker's wishes. The advantage of this method of attack is that the phisher does not steal money directly but engineers the theft using another party.

This methodology was first reported as an emerging threat in 2013 and since then has been closely monitored [42]. In 2018, the FBI was notified about 20,373 counts of BEC, which led to the loss of around USD 1.2 billion [11], representing the greatest loss recorded for any form of cybercrime.

The Anti-Phishing Working Group (APWG) found that in BEC attacks the phishers use domain names they register (i.e., as close to the address they are impersonating as possible) to increase their chances of tricking targets. In recent years, this type of scam has seen an increasing use of gift cards as a method of "cashing out". In the third quarter of 2019, APWG found that gift cards were used in 56% of cases, with payroll diversion as the second most common method (25%), and the remaining 19% involving the use of direct transfer [7].

The level of sophistication in these attacks can vary greatly; some are relatively simple and comprise only a single email from a disposable email account. In contrast to this, there are incredibly detailed and well-executed schemes. In these instances, immense research is conducted on the person the attacker wishes to impersonate, in addition to the target. Effort is made to make it appear as if phishing emails come from a genuine source, by either buying domains or stealing the login credentials of the individual the phisher wants to impersonate. The most commonly targeted position in this type of attack is the CEO, which make up 41% of targets. The CEO is also the position the attackers are most likely to attempt to impersonate, being used in 31% of attempts [43].

This particular method of phishing is becoming increasingly hard to detect using automated tools. Thus, at the present time, the only real defense against this attack is user education [44].

3.3.4. Cross-Site Scripting (XSS)

Modern websites often use client-side scripting to improve a user's experience. Unfortunately, this leaves the client open to a form of attack known as cross-site scripting (XSS or CSS). XSS is similar to SQL injection in that it is a form of code injection. However, unlike SQL, which targets the query function of databases, XSS targets the HTML outputs. The code may be written in languages such as Java, NET, or PHP. This exploit is present in many websites that are poorly constructed and do not sanitize user inputs, which in turn provides the opportunity for malicious actors to insert their code [45,46]. The code itself may be injected into data fields within a website or into the URL of a website with this vulnerability.

The reason XSS attacks are implemented is to bypass the same-origin policy (SOP). This policy states that scripts loaded from one domain may not access the data that belongs to any other domain. Thus, login credentials and other personal information should not be accessible to websites other than the one to which they belong. During an XSS attack, this policy is circumvented as the malicious script is run when the victim loads the webpage in their browser. This script will then attempt to access the sensitive data stored in the victim's browser, such as cookies, and then transfer it to the phisher's secure server. Using this information, a phisher can then gain access to the user's account and impersonate them.

There are two basic methods by which cross-site scripting can take place. These are stored XSS and reflected XSS. Of these two methods, stored XSS (also known as persistent XXS) has the greatest impact. In this method, malicious code is stored on a web applications server as a resource (for example, in a database), to be accessed by everyone who accesses that specific resource. The attack itself is not launched until the victim requests the generation of a dynamic webpage that includes the use of the resource that hold this malicious code. An example of this type of request is a comments section, blog, or bulletin board where, if the script is not sterilized, the victim loads a webpage on which the attacker previously made a comment that contained a script. When the page is loaded by any subsequent user, their browser executes the script and, while the user reads the comment, their personal data is extracted and captured on the attacker's server. This process continues until the script is removed.

The second type of cross-site scripting attack is reflected XSS. In this instance, the script is not permanently stored, rather the script is "reflected" back at the user immediately. In this method the phisher can send a specially crafted link that is aimed at a HTTP query that contains the malicious code as a parameter that, when the victim clicks the link, is submitted and the code is immediately "reflected" at the victim in the form of the webpage showing the results of the query. When the script runs, the victim's personal data is stolen and transmitted to the attacker.

3.3.5. Cross-Site Malicious CAPTCHA Attack

Another means of bypassing the SOP is to manipulate the user into giving away their personal information. That was achieved by Gelernter and Herzberg in their 2016 study by creating a cross-site malicious CAPTCHA attack. In this attack, a CAPTCHA is used to display the user's information captured from a legitimate site. The victim then completes and submits the capture, which in turn delivers the victim's private details held by the legitimate site to the phisher. In this type of attack CAPTCHAs do not need to be used; alternatives include games or typing tests, that is, any form in which the user's private information can be displayed and sent to the attacker [47].

3.3.6. QRishing

A QR (quick response) code is a matrix containing a layout of black and white pixels that are used to store and communicate compressed information. Two-dimensional QR codes are quickly replacing outdated one-dimensional barcodes because they are more readable and contain more information. To access the information stored within a QR code, an optical scan is used to read them, which in many cases means photographing the codes. Then, a QR code reader decodes the information contained within the QR code and processes it, for example, by opening an app store if the QR code is advertising a new application for mobile devices.

Due to the growing number of smart mobile devices, QR codes are being more commonly used by businesses both internally (e.g., for tracking, payment, and discounts) and externally to direct people to their websites, apps, and products [48]. QR codes can now often be seen on the packaging of products, newspapers, and billboards.

Unfortunately, the ease with which QR codes can be made and distributed has made them an ideal method for phishing attacks. This is further enhanced by the fact that humans are unable to understand the content of a QR code before it is deciphered with a QR code reader. Furthermore, many QR code readers perform the action necessary to see the QR code's content without first seeking approval from the user; for example, opening a URL in a browser [49]. Continuing with this example, a phisher could post QR codes around an area that pretended to be advertisements for a legitimate product or company. Then, the QR codes direct scanners of these code to a malicious URL, where a drive-by download takes place, thus infecting the victim's device, before redirecting them to the legitimate website. The victim would be unaware of the attack but would now have a compromised device that transmits their personal data to the phisher. Alternatively, the link could direct them to a spoof of the legitimate site, asking them to login, and simply stealing their credentials. Even if the QR code reader does first present the URL for inspection by the victim, the use of URL shortening techniques means that it is harder for users to determine whether a URL is legitimate.

Thus, QRishing is a dangerous variant of phishing that can easily be combined with other techniques explained in this paper in potentially devastating attacks.

3.3.7. Social Engineering

Social engineering is the manipulation of a person or persons to reach an objective by abusing the victim's emotions, gullibility, charity, or trust [50]. Social engineering is one of the oldest techniques available to phishers and the hacking community at large. An early example is the Greek myth of the trojan horse, which could be called an ingenious piece of social engineering. Because it requires no specific medium or vector, it is one of the most versatile technical approaches. It has been defined as "the art and science of getting people to comply with your wishes" [51] and has no singular technical defensive strategy [52].

Social engineering skills can be categorized as demonstrated by Hassan et al.; for example [52]:

- Impersonating staff—fundamental to social engineering because appearing in a position of power increases the odds of the victim falling for the manipulation; for example, a victim is more likely to share their password with an IT employee than to a random stranger.
- Hoaxing—convincing the victim that something untrue is true. Often leading to action out of fear.
- Creating confusion—an attacker can create confusion to obtain the information they seek, especially in physical situations; for example, setting off a fire alarm may cause people to leave their PCs unlocked and unattended, providing the attacker with access.
- Reverse social engineering—this is the most subversive method of social engineering, involving significant effort to set up and plan. As a result, the attacker appears to be in a position of power or authority, and thus victims approach them to ask questions and willingly provide their personal details.

The overall goal of a social engineering attack is to prevent the target from acting rationally and to instead rely on emotions that can be manipulated. This includes emotions such as:

- Greed
- Fear
- Anger
- Patriotism
- Friendship
- Sense of duty
- Sense of belonging
- Sense of authority
- Philanthropy
- Vanity

By utilizing these emotions and preventing the target from acting rationally, a phisher can manipulate a target into acting without proper consideration and thus yield personal details.

Examples of these emotion-based attacks are the classic "Nigerian Prince" or "You've won the lottery" scams, which take advantage of potential targets' greed. These attacks attempt to manipulate the target by effectively bribing them using, for example, a story about a wealthy individual who has money he wishes to transfer and for which he requires assistance. In return for providing this help, the victim is promised substantial compensation, but only after the victim provides something to the "wealthy individual", such as a small payment or bank account number, physical address, etc., so that a background check can be performed. The victim's greed for the large sum of money they have been promised compels them to do the phisher's biding. This approach can be combined with the methods outlined in Section 3.3.1 regarding scarcity—that is, if the victim doesn't act then the rich individual "will find someone else who will"—thus potentially further clouding the victim's judgement and causing them to act rashly.

Sense of duty and belonging is another emotion that can be easily manipulated. For example, if the victim is part of an online group, the phisher can pretend to also belong to the group. By insinuating that other members of the group have already taken part, the phisher can ask the victim to sign a partition or make a donation relating to a cause around which the group is based. This increases the likelihood that the victim will fall for the ploy because signing or donating will be seen as a duty of all members of the group.

A third example is based on fear, particularly when a phisher impersonates an authority figure. A phisher, for example, may inform a victim that their account will be terminated while pretending to represent the group responsible for that account. This can be further enhanced with a sense of urgency (e.g., a threat is made to terminate the account if action is not taken within 2 h of the receipt of the message) [53].

Semantic attacks are social engineering attacks that do not involve direct communication but instead rely upon human interaction with computers [54]. These attacks are aimed at the means by which users interact with their computers, in order to breach a victim's system and steal their personal data [35]; for example, the careful construction of a phishing website so that it does not prompt the suspicion of the targets.

The social engineering techniques outlined above are deployed in most phishing attempts across all media and most vectors.

3.3.8. Drive-by Download

Drive-by download is a versatile method of malware and shell code delivery, which utilizes avenues such as HTML emails, internet relay chat (IRC), or visited websites. After a victim has been induced to act, malicious code (often written in JavaScript) executes and utilizes browser exploits or plugins to secretly download and install malware on the victim's machine without their consent [55].

When a drive-by download is hosted on a webserver, the attacker has two main options. The first is to redirect the targets to a webserver owned by the attacker. The second, and more effective option, involves the sabotage of legitimate webservers so that they now host these exploits. This method improves the chances of the attack succeeding because the victim's suspicions are not raised if they have good reason to believe a site is legitimate [56].

The most common form of malware installed by a drive-by download is either a trojan, spyware, or botnet. A trojan is malware that is hidden within a legitimate program. Thus, the victim installs or runs a program believing it to be a genuine piece of software, also causing the embedded malware to be executed. Trojans are frequently used to install keyloggers or screen capturing software, which are tools an attacker can use to harvest a victim's personal details. A botnet is a form of malware that allows an attacker to use the victim's device for the attacker's own purposes through remote access. Remote control of the victim's device is conducted using a command and control center. A botnet can also run on a variety of protocols and architectures including HTTP, IRC, P2P (peer to peer), and instant messaging [57]. Turning devices into bots within a botnet allows phishers to use the botnet to perform a variety of tasks [58]:

- Proxy services
- Distribution and installation of additional malware
- Update current malware
- Scanning for exploits and vulnerabilities
- Surveillance
- Sending spam and phishing emails by acting as relays

- Redirect to phishing websites
- Pay-for-click services
- DDOS (Distributed denial of service) attacks

Symantec found that the number of botnet URLs increased by 57.6%, from 1.2% of all URLs to 1.5% of all URLs, between 2017 and 2018.

Botnets can also be used to instigate fast-flux attacks. Fast-flux is a method of assigning different IPs to the same domain name. This is often used by genuine sites to balance site demand by sharing the load among servers, thus improving performance and reliability. Phishers have devised methods to exploit this system in which botnets are used to hide their sites, thus making it harder for them to be found and shut down, and allowing attacks to persist for longer [57,59,60]. The botnet is used as a proxy that hides the all-important Command and Control (C & C) server, thus allowing the attack to be maintained and the bots to be organized. The fast-flux service allows the attack to continue even if some of the bots are taken down, because the domain can be changed to the IP of another bot. The only criterion for maintaining the attack is that bots are recruited faster than they are disabled [61]. A summary of a bot's lifecycle within a botnet is provided in Appendix A.

We can compare the lifecycle of a bot (in Appendix A) to the flowchart from Hausken's 2020 paper [62] (a copy of which is provided in Appendix B) regarding when the methods employed by the defender are sufficient. If we take the botnet waiting for a command as the attacker deciding whether to continue or start an attack, then the processes of attacking and defending are remarkably similar. In the flowchart found in Hausken's paper, action is taken until the uncertainty of the actor is below a pre-determined threshold (it is worth noting that this threshold can change over time) at which point the process ends. If we take a botnet based DDOS attack as an example, this threshold may be that an attack has been averted or managed (the load has been successfully shared such that the company is unaffected). For the attacker, the decision to discontinue the attack could be a result of multiple factors, for instance the identification of too many bots by the defenders (severely reducing the effectiveness of the attack), the attack being unsuccessful (the attack did not have the desired effect), or that the attacker had achieved their goal. Any or all of these would result in the attacker halting their attack and maybe the disintegration of their botnet. The feedback loops of these two flowcharts are similar with both parties deciding whether the uncertainty of their action is above or below a threshold, and this determines whether they take future action. In Hausken's paper, uncertainty is given a broad meaning that can involve outcomes, preferences, consequences, beliefs, and probabilities.

Hausken's model can also be applied to anti-phishing in general. Here, the threat would be the different methods of phishing attacks being attempted for infiltration and uncertainty in this case would be the outcome of mitigation or prevention of phishing attacks. This can be applied to multiple defenders working together sharing information (this is discussed more in Section 7). In this instance, if both defenders put in effort for defense against these attacks and share information, there is a greater likelihood of success; however, if one player puts in little or no effort and simply free loads of the other, then defense for both companies becomes harder, leaving both companies above their uncertainty thresholds.

Session hijacking can also be performed with malware introduced by drive-by download. This allows the phisher to monitor the victim's internet traffic. The malware first waits for the user to authenticate themselves via a secure session and then hijacks the session. The malware can then perform the action desired by the phisher without the victim's knowledge [18,63].

3.3.9. Malvertizing

Malvertizing, which is distinct from adware, makes use of online adverts as a means of distributing malware to victims. This form of attack is less focused than some of the other types discussed and can have wide ranging effects. In this approach, the phisher uses an advertisement-hosting service to host an advert that contains malware that is activated when the victim clicks on the advert. This malware infects the victim's machine to steal personal data and channel this data to the phisher [64]. An overview of this technique is shown in Figure 7.

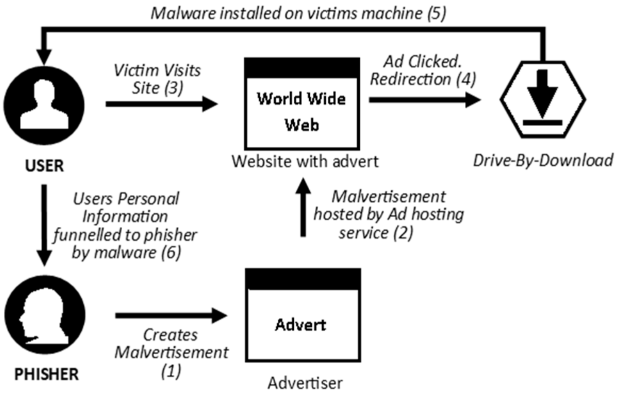

Malware installed on victims machine (5)
Victim Visits Site (3)
World Wide Web
Ad Clicked. Redirection (4)
USER
Website with advert
Drive-By-Download
Users Personal Information funnelled to phisher by malware (6)
Malvertisement hosted by Ad hosting service (2)
Advert
PHISHER
Creates Malvertisement (1)
Advertiser

Figure 7. Outline of malvertizing attack.

The main advantage for a phisher is that malvertizing is hard to detect and prevent, particularly because the malware is hosted on a legitimate ad website. Malvertizing is difficult to prevent because ad services do not require customers (i.e., advertisers) to provide specific details about the ad or themselves to be able to subscribe to the service. It is also extremely difficult for ad hosting services to check if ad redirects are malicious because most ads will include a redirect to the product being advertised [65]. Moreover, the use of legitimate ad hosting services means that these malicious ads can be seen on legitimate sites without requiring the site to be hacked or manipulated. Seeing an ad on a reputable site immediately imbues potential victims with a false sense of security because many victims are unlikely to be aware of the lack of verification required to create an advertisement online, and as a result are more likely to click it. The malvert can also make use of the ad hosting site's "customer profiles" and algorithms, which in turn allows the phisher to target specific demographics; for example, Experian has developed a 17-category system with 71 sub-categories allowing for refined targeting of specific groups of people [66].

3.3.10. Wiphishing

Wiphishing (also known as an evil-twin attack) is a method of phishing that utilizes wireless networks as the vector for the attack. The phisher inserts themselves between the victims and the real access point (AP). This is done using a rogue access point, which uses the same SSID and frequency as the genuine network. By placing this access point so that the signal of the rogue AP is stronger than that of the genuine network, the victim's device will be tricked into connecting to the rogue AP. Then, the phisher is able to monitor network traffic and access the information that is transmitted over the rogue AP. This type of attack is common at free Wi-Fi hotspots available in locations such as coffee shops, hotels, or travel hubs. The success of this type of attack is also enhanced because general users of these public hotspots are likely to accept unsigned or incorrectly signed certificates [67].

An advantage of this approach for the phisher it that special hardware may not be required. It has been found that wireless access points can be established using the hotspot feature on a smartphone or laptop software (for example airbase-ng) [68].

3.3.11. Browser Vulnerabilities

Browsers are software applications that host content that can be displayed, retrieved, and changed on the world wide web. This content consists of text, images, videos, and other files such as executables. Browsers use a client–server model: the browser, used on a computer or mobile device, acts as the client; and the webserver, which hosts the information for users to access, acts as the server. The webserver sends the respective information to the client and the results are displayed on the browser application on the client machine or mobile device.

A browser vulnerability is a weakness in a browser that can be exploited by a malicious user who can then perform unauthorized actions on the victim's machine. All web browsers have weaknesses or vulnerabilities; although different browsers have varying degrees of vulnerability to different types of attacks, no browser is truly secure against vulnerabilities that can be exploited by a malicious attacker. This is due to browser design issues and flaws, the frequency with which these issues are updated and patched, the degree to which the browser is integrated into the system, and the permissions assigned to it.

3.3.12. Tab-Napping

Tab-napping is a type of attack performed by phishers, scammers, and hackers. The term is derived from the words "tab" and "kidnapping", where tabs are individual webpages that can be opened simultaneously in one browser window.

In this particular method of attack, attackers make use of the fact that potential victims have unattended tabs in their browser application while they are looking at other tabs. Using this as an opportunity to attack, malicious hackers attempt to redirect the victim's unattended webpages to malicious webpages or URLs without the user noticing. From these URLs, phishing attacks can then be performed to execute scripts and extract vulnerable data and information from the user.

Let us consider an example scenario of a tab-napping attack. In this scenario, a victim logs into their Facebook account and enters their relevant details. When the person browses their feed, he sees an interesting link for something he might be interested in; he clicks on the link which then opens in another Table While the user is looking at this second tab, a script is executed without the user's knowledge, which redirects the previous tab (i.e., the tab logged into Facebook) to a fake Facebook login page. When the user returns to the first tab, he assumes he was logged out because the session timed out, so re-enters his details into the login form. The login form simply refreshes and/or redirects the user to his previous session, and he is unaware that the malicious attacker now has access to the victim's valid credentials. Using these credentials, the attacker now has access to the victim's account and can proceed to collect vulnerable data and information about the victim.

The only means by which a general user can protect themselves from such an attack is to check the URL in the address bar of the browser and, if applicable, that the website is using the HTTPS protocol. If the URL appears suspicious for any reason, then the user should close the tab, and open a new tab and type the desired URL.

Most web developers make use of use of the syntax [use target = "_blank"] to open links to a new Table This practice is vulnerable to attacks; although it opens a link in a new tab, as desired, the syntax also allows the opened page to access the initial page and change its URL because it makes use of the JavaScript "windows.opener" property. Therefore, a malicious hacker can make use of this syntax to execute code that instead opens a malicious URL in the initial page when the link is clicked; this code is "windows.opener.location.replace" (malicious URL). To prevent this from happening, the web developer should use "nofollow noopener noreferrer" in conjunction with the earlier syntax.

3.3.13. Typo Squatting

Typo squatting is a type of URL hijacking that targets users who make a typographical error when entering a website address (e.g., a user types Facebok.com instead of Facebook.com). This is a form of cyber squatting in which a malicious user creates websites that use someone else's brand and copyright. When potential victims make a typographical error, they are led to an alternative website that is owned by the hacker and looks like the original website. Using this website, the hacker can then proceed to perform various malicious activities, such as stealing sensitive information (e.g., login or payment details) using fake login forms or selling products or services. These sites are also capable of downloading malicious software to the victim's system, requiring only that the victim visits the website. These types of downloads are called drive-by downloads and are employed by most typo squatters to spread malicious software capable of stealing sensitive data. Typo squatting is not limited only to a misspelled domain name but can also be used if the user enters a wrong domain extension, e.g., com instead of .org.

A few preventive measures that a user can employ are to bookmark or pin websites that are visited frequently; use speech recognition software; use web searches to ensure the intended website is reached; never click suspicious links received from chats, email, or other media; and always have anti-viral software updated to the latest version and anti-virus databases updated to the latest available. In a phishing attack, these malicious hackers register or buy domain names which are similar to the original company with the intention of tricking victims. Such an instance occurred when the website AnnualCreditReport.com was launched; multiple domain names with similar names were purchased by malicious users to trick visitors into sharing their sensitive and personal information without their knowledge. Attackers also sent the users phishing emails pretending to be the legitimate website to induce targets to follow a link to the malicious website.

3.3.14. Sound Squatting

Sound squatting, more commonly known as voice squatting or skill squatting, is another form of cyber squatting. In this method, the attacker uses a voice user interface (VUI) to exploit the usage of homonyms and errors caused by input. A homonym is a word that sounds similar to another word but is spelt differently. Virtual assistants make use of keywords activated by a person's voice to open third-party applications. To exploit this, a malicious hacker registers a fake third-party application with a voice keyword similar to an authentic application. Thus, when a user requests or calls for the particular application, the virtual assistant opens the fake third-party application instead. When opened, this fake application then proceeds to steal sensitive information from the user and install more malicious software. The main issue with these applications is that they can run for long periods in the background without the user's knowledge.

Skill squatting when coupled with smart speakers, which are becoming more common in homes throughout the world, can be used to create complex phishing attacks. Smart speakers can often interact with other devices through the internet of things and even be used to make financial transactions, thus creating a whole new area for phishers to target. As shown by Kumar et al., who demonstrated that by creating a skill that utilized the command "Am X" when an Alexa user attempted to use the American Express skill (with the skill name "Amex"), the user could easily be redirected to a phishing version of the login screen for American Express and their credentials stolen [69]. Some countermeasures have been proposed for this whereby before a skill is accepted it could be checked to see if the skill could be mistaken for an already existing command, although this does not seem to have yet been implemented.

3.3.15. 404 Error Manipulation

In this type of attack, a malicious hacker uses a resource mapping technique. Resource mapping is used to identify valuable assets and information, and the strategizing methods by which the hacker can obtain those resources. Sites such as http://intranet are used exclusively by corporate networks and are not accessible to the general public. If a site implements the 404 error "Page Not Found", then the attacker can execute a cross-site history manipulation for resource mapping.

As an example, let us consider that a site uses the following configuration:

```
<error statusCode = "404" redirect = "Not_Found.aspx"/>
```

In such a case, the attacker can perform the following steps:

- Create an IFRAME with the src = "Not_Found.aspx"
- Remember the present value of the history.length
- Change the src of the IFRAME to, for example, "AnnualReport_2019.doc"

- If the value of the history.length remains the same then the specified resource does not exist. If it changes then the resource exists and then hacker can map the resource found and proceed to map more resources.

3.3.16. Click Jacking

Click jacking is an attack in which malicious hackers use multiple transparent or opaque layers to hinder users who click on a specific button or link to access an intended destination. The user is forced to click on these layers, either by deception or as a means of closing them. When a layer is clicked, it opens a web site that contains malicious applications or makes the user perform unexpected actions.

Let us consider an example in which a user visits a website that has a button which states "Click here for a free iPhone XS". Without the user's knowledge, a malicious hacker has created an invisible layer with an IFRAME which presents the user's email account. This button is lined up precisely above the "Delete All Messages" button in his email account. Because the IFRAME is invisible, when the user clicks on the "Free iPhone XS" button, he unknowingly clicks on the "Delete All Messages" button and deletes all the messages in his email account.

3.3.17. Malicious Browsing Extensions

Browser extensions are additional software that is installed within the browser application. They are pieces of code that are added to the code that runs the browser application. These extensions run like other software applications but rather than being installed directly on the computer, they are added to the browser application. An issue with extensions is that they are published via web stores and not appropriately screened. Thus, it is relatively easy for hackers to publish malicious browser extensions. As mentioned previously, because extensions are part of the code of the browser they do not run separately as an application but as a part of the browser. Since the browser is a trusted application, it is difficult for anti-virus software to detect and address these malicious extensions. In addition, although these extensions usually require a user's permission to work, most browsers grant and confirm extension permissions by default without consulting the user. Safe and legitimate extensions require the user to grant permission for the extension to view and change all data on websites visited by the user. If permission is refused, the extension is not installed.

To prevent the installation of such extensions, users should install a tracker blocker, which block websites and extensions from attempting to send data to third parties. In addition, users can examine the legitimacy of extensions by checking the developer and the description, reading reviews posted by other users, and assessing whether the reviews seem genuine. The user should also double check whether the extension is a legitimate extension rather than a malicious extension that makes use of or copies a legitimate logo to impersonate the original.

3.3.18. Man-in-the-Middle

Man-in-the-middle attacks comprise two forms. In the standard man-in-the-middle (MITM) attack, a malicious user intercepts a direct communication between two parties, whereas a man-in-the-cloud (MITC) attack intercepts communication between the user and cloud services.

In an MITM attack, a malicious user intercepts and reconfigures data used by a service provider and using party. The attacker then proceeds to contact the service provider pretending to be the using party. The attacker can then proceed to steal credentials, account information, and financial data, and use resources authorized for the user. Examples of tools used for conducting these attacks are Ettercap and the Metasploit Framework.

In an MITC attack, the attackers exploit a vulnerability present in the cloud's synchronization token system. When a connection with the user and the cloud is established, a synchronization token is allotted to both parties to serve as a key to be used between them. Each connection made between the user and the cloud creates a new, unique synchronization token for that particular connection. If an attacker intercepts the connection between the user and the cloud, they can determine the synchronization token. After identifying the token, the malicious hacker can then impersonate the cloud service to establish a connection with the user and disconnect the previous authentic connection using the authentic synchronization token. If successful, the next time the user establishes a connection with the cloud, the token used will be one that the hackers send to the user. The user will unknowingly use this token to establish the connection. Once this connection is created, the attacker is granted access to the user and can proceed to perform malicious activities. Users in the cloud remain unaware they have been hacked because the attacker can always return the synchronization token to its original value at any time. An addition risk of this form of attack is that accounts that have been hacked are unable to be recovered.

To detect if they have been attacked, a user has the following options: Users can analyze the geo-locational history of any data synchronizations that took place. A more straightforward approach is to check if any social engineering attacks have been carried out against a user or determining if any Switcher malware was installed in the system. This type of attack can also be detected by email anti-virus gateways or trusted anti-virus software.

There are several methods a user can employ in order to mitigate such attacks, namely: When the user has detected an MITC attack, he can assess the impact of the attack and gather evidence that the attack happened. Experienced or skilled hackers will attempt to remove all traces that an attack occurred but, in some cases, may not be able to remove all the evidence; this can be because a clean-up process failed or was not undertaken. The user can then proceed to remove all malware files that exist in the system. The user should also delete and remove his current cloud account and create a new one, which ensures that the attacker will no longer be able to make use of the synchronization token.

By completing these steps, a user can successfully prevent a man-in-the-cloud attack from happening and increase the security of his cloud infrastructure. An outline of this type of attack is shown in Figure 8 [70].

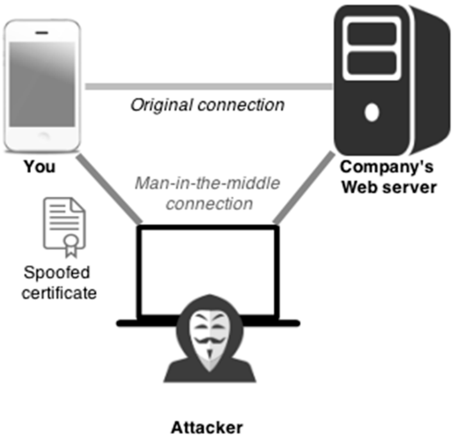


Figure 8. Outline of a man-in-the-middle attack [70].

3.3.19. Mobile Phones

Malicious hackers also make use of a method known as phone phishing. Phone phishing is a criminal activity in which the malicious hacker performs a social engineering attack through a telephone or mobile phone to obtain sensitive and private information; this information is then used for the attacker's gain. Phone phishing has several forms of attack and the most popular are:

- SMS phishing: Phishers send victims texts with a fraudulent URL, which is disguised as a legitimate source and instructs users to send their personal information or to download a specific app.
- Call phishing: Phishers pretend to be a legitimate organization such as a bank or tax agency and instruct the user to share their personal and sensitive information.

- Social media phishing: Phishers create fake profiles to entice victims to take part in giveaways and romantic scams and then proceed to ask the victims to send large amounts of money and share their personal information.
- Application phishing: Many legitimate applications and games use advertisements as a means for users to earn rewards or increase profit. Malicious hackers can therefore use this to display their own advertisements which, when clicked on by a user, lead to opening a malicious link or downloading a malicious application.

Examples of these social engineering attacks include the following: (1) The attacker calls the victim and informs them that they have won a substantial amount of money; if the victim wants to claim the reward, they must send their personal information, including their account credentials. (2) An attacker calls the victim and pretends to be an authority from the victim's bank. The attacker claims there is an issue with the victim's account credentials and advises that the account will be blocked unless the victim confirms their sensitive information, such as bank account and card details.

3.3.20. GUI-Squatting

This is a new type of phishing attack aimed at mobile devices developed by Chen et al. This is an automated method of generating platform-independent phishing apps in as little as 3 s. The genuine app is first analyzed and the interactive components of the login page extracted using canny edge detection and edge dilation to first segment the GUI components before using a convolutional neural network to classify these components (e.g., buttons, text boxes, etc.). From this analysis, a GUI is generated by combining code snippets for each element, trying to mimic the real app as closely as possible. Deception code is then introduced, which siphons the user's personal details to a remote server and generates a pop-up to mislead the user into believing that the issue is a technical issue with the app rather than a security threat [71]. This method has been proved to bypass many modern anti-phishing techniques including layout similarity, visual similarity, personalized indicators, and window integrity methods. Sixty-one anti-viruses were also unable to detect the generated app as being malicious.

This method generates high-quality copies of existing apps that are capable of bypassing existing phishing prevention and detection techniques to steal a user's login credentials. This coupled with the very short creation times creates the perfect tool for large scale phishing attacks against mobile devices.

3.3.21. Session Fixation

This type of attack is conducted when the session ID used for the users' authentication process is not protected. The hacker makes use of packet sniffing tools to determine the session ID and session key. With this information, the hacker is able to masquerade as the certified authority and perform spoofing attacks. Examples of packet sniffing tools are Wireshark Packet Sniffer and SmartSniff.

Another method in which this is achieved is when an attacker has gained access to a user's account credentials. Various techniques can be employed to achieve this, ranging from phishing to using spyware and cookie poisoning. When an account has been successfully hacked, an attack can be used to obtain a user's personal information and any corporate data he may hold, in addition to jeopardizing his cloud computing services. Thus, an unauthorized user is able to gain access to a legitimate user's account.

Users can detect if they have been hijacked by checking if any threats have been made toward their cloud computing account. When a threat is detected, hardware and software used to combat the issue should be installed because these protect data from attackers. Emails should always be double-checked and verified before clicking on any embedded links, particularly if the emails appear to be important for work or requests to reset passwords.

3.3.22. JavaScript Obfuscation

Obfuscation is the process of creating obfuscated code, which is source or machine code that is difficult for humans to understand and decipher. This is similar to encryption, but the difference is that machines can understand and execute the code.

When code is obfuscated, the logic behind the code is hidden from outside users. This reduces the file size and, therefore, increases the speed of the transfer of data from the client and server. Obfuscation also makes reverse engineering of code extremely difficult.

Obfuscation was first introduced at DEFCON 16 in 2008. Recent analysis of the code of compromised websites found that the code deployed by malicious hackers used the same techniques as those demonstrated at DEFCON 16. Using obfuscation, the hackers were able to hide the fact that they used placed malicious links on the web site, which allowed them to collect victims' personal information and sensitive data.

4. Phishing Resources

As a cybercrime, phishing requires a certain level of technical proficiency. Unsuccessful phishing attempts are typically performed by low-level hackers and are thus easily detectable and distinguished. Hackers who perform successful phishing attacks are generally proficient.

However, products have recently been released online that provide Phishing-as-a-Service (PhaaS). These products remove the technical barrier to performing successful phishing; the remaining constraint, if any, is a financial issue.

4.1. Phishing Kits

A phishing kit is a web component that acts as the back end—that is, the final step—of a phishing attack. This means that the hacker has already and successfully replicated and impersonated a well-known brand or organization. This kit is capable of mirroring the exact design of legitimate websites to make a fake website look authentic. The goal of a phishing kit is to provide an environment that looks authentic for sufficiently long to induce a user to unsuspectingly share their sensitive data. Most phishing kits are located on a compromised webserver or website and are hosted online for up to 36 h before they are detected and removed or flagged for removal. Modern phishing kits have been developed that block the IP ranges of the world's largest security companies, such as Kaspersky, McAfee, and Symantec. Another method used to mask phishing kits is when a host is compromised; due to the fact that the host has a good or neutral reputation they can successfully avoid passive detection measures.

4.2. Neosploit

Neospoilt is a toolkit used by hackers to compromise a target host. This toolkit attempts to download malicious files that could cause severe damage to the system. The toolkit downloads a specific Trojan called Mebroot, which alters the Master Boot Record (MBR) of the hard disk and then uses rootkit techniques to hide itself. The trojan initializes the MBR and proceeds to search the MBR for the partition table. Using the partition table, the trojan attempts to establish which partition the computer system boots from. After this is established, it begins to copy and move the original MBR to sector 62 of the hard disk. It then installs its kernel loader onto sectors 60 and 61 of the hard disk, overwriting all pre-existing data. Finally, using the previously acquired knowledge of the active boot partition, it moves the system pointer to near the end of that particular partition and installs a rootkit driver. When this driver is being installed, the installation process overwrites up to 1149 sectors on the hard disk that were previously allocated to authentic values created by the computer system. The trojan then creates a .dll file that performs a specific operation, which forces the user to restart their compromised system and tells the user that there are essential updates that need to be installed. Once the system is restarted, the system boots from sectors 60 and 61, and the rootkit then begins to patch the windows kernel, thereby granting the trojan full access to the system. The trojan then creates a back door that bypasses the local firewall and creates a connection to the malicious hacker. When this connection is established, the hacker has completed his task and has remote access to the targets system.

4.3. Online Resources

Different types of phishing tools can be found online and on the dark web. As mentioned previously, web services such as Cyren exist that offer PhaaS. These services can be one-off phishing attack kits for around $50 or full-service subscriptions that cost around USD 50 to 80 per month.

In addition, phishing tools are available for testing and simulating phishing attacks. Simulating attacks serves as an effective training tool and helps users protect themselves from common vulnerabilities. These tools also contain user awareness and training modules. Examples of such tools are:

- SecurityIQ PhishSim—this is a Software-as-a-Service (SaaS) platform which is available for free but has limited features. It contains an interactive education module and provides reports and phishing campaigns. This was developed by the InfoSec Institute.
- LUCY—this is a social engineering platform that simulates phishing attacks and provides the user with various scenarios and templates. A free version is available, but the paid version contains additional features.
- Metasploit—this is a penetration testing tool that consists of a phishing awareness management component. It also contains training for users and simulations. It was developed by the company Rapid7. Two versions are available: a free version with limited features and a Pro version that offers full functionality; the Pro version also offers a 14-day trail.

5. Current Anti-Phishing Methodologies and Techniques

Anti-phishing methods for specific phishing techniques have been briefly outlined in the relevant segments of Section 3. However, most research into anti-phishing techniques focuses on general phishing detection and prevention; in this section we will outline these general methodologies looking at both computerized and non-computerized methods being deployed. These methods of anti-phishing can be classified under the defense model proposed by Hausken et al. [24] and fall into two of the 6 proposed categories, these are:

- Protection—technical or organizational measures to protect a target. The anti-phishing techniques in the remainder of this section can be classified in this category.
- Multilevel defense—layered protection where the inner defenses can only be attacked when the outer ones are destroyed. This would apply when a business deploys more than one method to prevent phishing. For example, a technical prevention method like blacklisting (see Section 5.2.1) and education of employees (Section 5.1.2) as a second layer of defense. However, Hausken et al. state that the outer layer must be destroyed before the inner can be attacked, in this example the outer defense is much more likely to be circumvented rather than destroyed.

Although not covered in this section, redundancy could also be used in the event of a phishing attack being used for a drive-by-download of ransomware or another destructive virus. The other defense measures outlined (false targets, separation of system elements, and preventative strike) do not really apply to the prevention of phishing attacks.

5.1. Traditional Non-Computerized Anti-Phishing Techniques

There are a variety of ways that phishing can be prevented. In this section we look at the range of non-technical methods that can be used to prevent phishing attacks.

5.1.1. Legal

One way to prevent phishing attacks is to have the proper legal recourse against these phishing attacks. However, legislation relating to this was slow to catch on, with the first instance of this being shown in 2005 in the state of California in the USA, with some other states such as Texas following suit. However, the federal government (and most other states) have not passed legislation regarding phishing attacks specifically and instead choose to prosecute offenders under more general computing laws such as fraud.

The United Kingdom followed suit, enacting more severe sentences for cybercrime, including fraud and identity theft. Under the fraud act established in 2006, computer-aided fraud can result in up to 10 years in prison. This act also includes statutes that prevent the owning of a phishing site with the intent to deceive users and commit fraud [72]. Canada also adopted an anti-spam act in 2010 that seeks to protect Canadians from cybercrime.

The US company Microsoft has taken a stance against phishing, collaborating with governments outside the US to help prevent phishing attacks and bring justice to those perpetrating them. For example, in 2011, Microsoft signed an agreement with the Australian government to prevent phishing by training law enforcement officials.

Whilst these laws will act as a deterrent for more casual phishers, more serious threats like advanced persistent threats will not be threatened by these laws. As such it is vital other methods of phishing prevention are developed and implemented.

5.1.2. Education

One of the most common practices for preventing phishing attacks is to educate individuals to identify phishing emails. This is mainly implemented by businesses who have training set up for their staff. This sort of training can be delivered by a variety of different methods ranging from games [73] to simulated phishing emails. Simulated phishing emails have also been developed into embedded training methods. This particular method of training is where subjects are sent fake phishing emails that have "bypassed" other methods of detection, to see how many would click the malicious link included. However, when the subjects clicked the link, they are instead provided with training material about phishing. This training method has been shown to have a positive impact on more persuasive phishing emails, although little improvement was noted on less persuasive phishing emails [74].

5.2. Technical Anti-Phishing Techniques

This section covers the more technical approaches to preventing and detecting phishing attacks.

5.2.1. Black and White Listing

The primary method by which the threat of phishing websites are mitigated is the use of black and white listing. Blacklisting is an approach whereby an extensive list of domain names or URLs of suspicious or harmful sites is maintained and users can check to see if the site they are being directed to is likely a phishing site. Blacklisting can cause severe financial harm to a phishing site by reducing the amount of traffic by up to 95% [72]. There are many publicly available blacklists available, although some are more effective than others. The primary characteristics that define the effectiveness of a public blacklist can be defined as how long it takes to update the blacklist and the accuracy of the phishing detection used by the blacklist. The use of blacklisting is now often included in browser-based security tools (browser plug-ins and anti-phishing toolbars) for automated detection of suspicious sites to help prevent users from being tricked into entering their credentials into illegitimate sites. There are also other anti-phishing tools that have been developed that scour the internet for clones of official websites to aid in the detection of phishing sites.

Whitelisting is a database of legitimate sites rather than suspicious ones. However, this method of phishing detection is impractical as it is near impossible to predict the sites the user will go to, and any new site would be classified as suspicious even if it was a legitimate site.

5.2.2. Heuristic Detection

This is the method of detecting and preventing phishing attacks by extracting features from phishing sites. This method is severely currently limited as heuristic features may not be present in phishing sites, and if the phisher knows the detection features or algorithms used, they can easily bypass detection.

5.2.3. Visual Similarity Detection

In this method of phishing detection, the similarity between a suspicious site and a database of legitimate website features (including logos, icons, screenshots, and document-oriented models) is computed. If the similarity score is a above a threshold, then this suggests that the suspicious site is being mimicked. This is useful as attackers will often copy legitimate sites to fool their targets into parting with their credentials. However, this method is far from infallible as it can be easily bypassed by the phisher if they simply slightly adjust some visual elements without effecting the overall look or content of their mimicked page.

5.2.4. Machine Learning

Since the detection of phishing emails, messages, and websites is mainly a matter of classification, most current research focuses on machine learning approaches. A range of different machine learning techniques have been researched and implemented including decision trees, neural networks, and support vector machines (SVM). These have been used for a variety of anti-phishing techniques from phishing email detection [75] to identifying discrepancies between the websites' structures, its HTTP transactions, and the site's supposed identity [76].

Machine learning methods of phishing detection are much more versatile and able to detect changes in phishing sites that could cause other detection methods to bypass the site. Machine learning can provide the ability to prevent against even zero-day phishing attacks if provided with enough training data. This methodology, although powerful, is highly dependent on the size and quality of the training dataset and the fine tuning of hyperparameters to obtain optimal accuracy [77].

6. Phishing and Cyber Resilience

Protecting critical assets or networks from disruption or attack is one of the primary concerns in both cyber-security and risk analysis. When these two fields intersect the concept of cyber resilience is born, which can simply be defined as an entity's ability to plan for, absorb, recover from, and successfully adapt in the face of adverse cyber events [78]. Phishing is of course an adverse cyber event that can lead to even greater disruptions to an entity's network or assets if properly utilized by attackers.

Typical analysis of an entity's cyber resilience involves a number of indices; these include robustness, redundancy, security, vulnerability, and resilience. However, these indices do not take into consideration the crossover between the cost effectiveness of a measure and its ability to prevent adverse events. This was noticed by Bier et al. [79] who devised a new measure, defensibility. Bier defined defensibility as a dimensionless index, where a modest investment would significantly improve an entity's cyber resilience by reducing the disruption or damage from an attack. This acknowledges that you could spend a fortune defending a particular system to little effect, but it may be both cheap and easy to defend a similarly at-risk system. This measure could be particularly useful for helping risk managers and analysts to decide which systems can be successfully improved without wasting investments on systems that would give negligible improvements to the overall defense of the entity.

If phishing could be prevented, an entity would be a lot more cyber-secure and cyber-resilient, as it is often the primary attack vector [5] with businesses often being the targets with business email compromise (see Section 3.3.3) being a common phishing technique resulting in the loss of billions of dollars [11]. However, as we have seen in Section 5 whilst there are many anti-techniques currently in service, with more being developed, none of these are 100% effective. This is a factor that is understood in cyber resilience, hence the preparation to absorb and recover from attacks. With all that said, phishing would probably score quite highly on the defensibility measure outlined by Bier et al., as it is often a primary source of infection and infiltration resulting in huge losses for companies and modest investment in phishing email detection and employee training may reduce the success of these attacks. There is also examples of phishing attacks being components of more severe, infrastructure damaging attacks, like the attack on the Ukrainian power grid resulting in a five-hour power outage [13]. As such, all entities, be it a national government to a private business, can do is prepare; hence the need for cyber resilience.

As has been established in Section 3 of this paper, phishing is a versatile attack that can utilize an ever-growing range of vectors and techniques. One of these new approaches involves the use of IoT (Internet of Things)-connected devices in phishing attacks, like the example of Alexa sound squatting in Section 3.3.14. This is a rather benign example; however, IoT is not limited to voice assistants and is in fact a massive attack surface that could be used to devastating effect. As Hausken [78] pointed out, in the future it will no longer be necessary to physically infiltrate locations to hijack a vehicle such as a plane, train, or truck; any of which could be used in devastating or catastrophic attacks, with phishing as a method of digital infiltration used by these malicious actors. Use of these methods could result in substantial damage to civil infrastructure.

A 2018 paper by Bostick et al. [80] looked at using the science of resilience instead of historic risk assessments to inform policy decisions in relation to the decimation of civil infrastructure by hurricanes Katrina and Sandy in the USA. Whilst no damage of this scale has been inflicted by a cyber attack as of yet, as there have been very few successful large cyber attacks that resulted in damage to civil infrastructure (especially in Western society), it remains a very real possibility that could have catastrophic implications. As such, lessons can be learnt from Bostick et al. in regards to implementing and using cyber resilience strategies over simple risk assessments within civil infrastructure, government, and private companies. There are two main advantages to adopting this strategy. Firstly, resilience acknowledges that circumstances may evolve during the recovery period. Secondly, resilience supports the identification of resilience management strategies throughout the whole system, as resilience requires a holistic understanding of the system. However, it is a consideration that shifting to this new method of policy development may pose an issue for a generation who bases decisions solely on threshold-based risk management. The adjustment of funds going from preventing and withstanding adverse events to preparing to weather them and incur some loss may not sit well with shareholders and investors, as they may not be fully aware that some threats (especially cyber threats) cannot be fully prevented, and that they will have to decide what level of loss is acceptable [80].

Due to all the factors discussed in the above section, it is imperative that companies, firms, and other entities thoroughly assess their cyber resilience and the factor that phishing can play in it.

7. Discussion of Current Challenges and Trends in Phishing Attacks

Phishing attacks are one of the most prevalent threats to the whole internet community from individual users to large corporations and even service providers. As has been discussed above, there are current methods for detection and prevention of phishing techniques, but there is yet to be a comprehensive solution to this phishing problem [81]. Due to the huge variety of techniques and the constant introductions of new vectors, developing detection and prevention methods is a challenge that will not be simplified or eradicated with the passage of time, as shown by October of 2019 having by far the highest phishing rates in the last three years, and the mean number of phishing websites steadily increasing throughout 2019. The trend for the top targets for phishing attacks remains web-mail and software-as-a-service, with these making up over 30% of detected attacks, followed by payment sectors and financial institutions in 2020. There has also been a 20% increase in social media attacks since the start of 2020 [7,8,82].

One of the challenges faced by those trying to combat phishing is distinguishing phishing websites from legitimate sites. In recent years, the use of SSL by phishers to make their site seem more genuine has been growing and is now up to 78% of all detected phishing sites [83]. Before, even if a target was directed to a phishing site, most modern browsers display a warning if the connection to the site is not secure (HTTP rather than HTPPS) or is using a suspicious certificate. However, with the increasing use of SSL, it makes it significantly easier for non-tech savvy targets to be fooled by these fake sites and the use of SSL on phishing apps for mobile devices makes their detection much harder. Some antivirus software now provide browser add-ons to assess the reputation of a site and display warnings if the site is found to be disreputable. However, this system does rely on the community rating these sites, a system that could be manipulated with enough effort, but it should identify simple phishing sites with ease. These will be effective for businesses and users who are capable of installing them, or even knowing to install them, but as shown above in Section 3.3.1, the primary targets of phishing attacks are the older generations who are less likely to know about these technologies.

Virtual private networks (VPN) are becoming more commonplace in recent years and whilst often advertised for their ability to change users' location, they do provide a layer of security for some types of phishing attacks, especially wiphishing. However, this type of protection is one of the least-used protective measures as many users find them complicated to use, especially in older generations [84].

Anti-malware software is also important for some types of phishing where malware is installed (such as drive-by-download). However, whilst many are aware and do have these installed on computers (82%), adoption of this on mobile devices is significantly lower (around 37%) [84]. This is a major issue; as outlined above, mobile devices can be targets for phishing attacks just as easily as email or any other vector. Detection of desktop phishing attacks is different from detection of mobile phishing attacks due to the difference in architectures [85]. Furthermore, the accuracy of a mobile phishing attack is a vital issue among researchers in this field. Some anti-phishing solutions for mobile devices have been implemented; but still, there is still a lack of a comprehensive solution for this issue [83]. Mobile devices are also important to secure for their secondary feature as a method of two-factor authentication, be it using an authenticator app or a text message, which many sites and services now insist on, or highly recommend. For hackers, this does pose a problem as one-time passwords are a lot harder to bypass than just a password; however, with access to the mobile device where these are sent would allow them to access accounts protected by this method of authentication. As such, it is vital that new phishing detection and prevention methods focus on both mobile devices and how they can be used in connection with more standard phishing attacks.

Since most currently implemented phishing detection methods involve a heuristic or simple blacklisting approach it is still possible for phishing attacks to go unnoticed by these systems if the phisher takes precautions. These may include implementing semantic changes to emails when distributing spam mail, using different sending addresses, or utilizing a botnet of infected devices to mitigate the detection of a phishing site [85,86]. Anti-phishing techniques are unable to detect all types of phishing attacks as they can come from so many different vectors and via different mediums. This lack of a comprehensive solution makes protection for the general public an issue as many lack the knowledge or money to properly defend themselves. Businesses meanwhile can have all the protection they can afford and all it takes is one person to ignore a warning or make a mistake and the phisher can infiltrate the company and escalate their control using lateral phishing (phishing people from within the company using a legitimate company email address). It is also vital that any anti-phishing methods are done in real time as after the target has taken the "bait", it will be too late.

Another challenge for those studying this area is identifying the source of the breach in real life cyber attacks. Phishing is often used as a method of infiltration or infection [5], but more sophisticated hackers (such as Advanced Persistent Threats (APT)) will often try and remove as much evidence of their cybercrimes as possible when in the exfiltration stage of the attack. This makes it harder to identify the source of the breach and leaves less information about zero-day exploits or the other cutting-edge methods employed by these malicious actors.

Phishing like any other cyber-crime does not exist in isolation, and as such, the future of internet security will likely involve several attackers and multiple defenders applying a multitude of different cyber attacks and defense techniques simultaneously or in tandem. Therefore, communication and distribution of information is an important part of anti-phishing, as well as something that defenders want to limit or prevent among the attackers. For example, if a phisher gains access to a company's network, the company does not want the structure of their network to be disclosed to other cyber criminals, making them vulnerable to other forms of attack. However, this may pose some challenges. Hausken's 2017 paper [87] looks at the concept of information sharing between attackers and defenders in the face of cyber attacks. The first consideration is that information sharing for the attackers comes at little cost; besides giving away the information, little is actually known of the dissemination of this information, as some research suggests that hackers would actually like to keep discovered information to themselves, to improve their reputations and keep them ahead of the competition. However, other theories suggest that hackers rarely keep secrets within their community, and as such, the information they gather would be readily available if you know where to look. This compares to when companies band together and share information in defense. Investment in cyber-security is often underfunded, and when included in this information sharing dynamic, some companies will free load off others, rather than investing in their own defenses. In Hausken's model, two attackers are up against two companies, with the first round of the game establishing the firm's defenses, and from here on the two attackers decide whether to attack and/or share information with each other. It was noted that when the effectiveness of information sharing among the firms increased, firms tended to utilize information sharing rather than investing in defense. It also showed that increased interdependence between firms will lead to increased information sharing among the attackers, which in turn leads to attackers launching combined attacks. For the attackers, information sharing is a priority when attacks are costly and the company's defenses are cheap. The second hacker may be disadvantaged and given less information and could be deterred by the reputation gain of the first hacker. Since phishing is a method of infiltration and is sometimes used for the delivery of malware, the information about information sharing within this study is relevant. As stated above, one attacker may gain access to one company using phishing and acquire knowledge of the company's network, policies, and the managerial structure; and share it with the second attacker. The first attacker may also be suitably placed within one organization to assist with an attack on a firm that the company is sharing information with by moving within, and between, the companies by phishing internally using a legitimate company email address. Using a legitimate company email address would be extremely beneficial in this example as there is already trust between the two companies due to their history of information sharing.

This leads to the main challenge of phishing prevention, education, and awareness. Though this is an issue throughout the cyber security field, educating the public and employees should be a priority on this particular issue since, as shown above, there are not many automated systems to compensate for the users lack of knowledge or simple mistakes. The fact that cyber security is an issue that some users do not take seriously until it is too late is cause for major concern, with those willing to pay for general cyber threat protection coming in at around 50% of those surveyed [83]. It is worth considering that the only real way to combat phishing and other cybercrime would be to establish societal change, educating people more thoroughly—and from a younger age, especially since access to technology and the internet becomes easier for younger generations. It has been shown that the use of role-play scenarios (like in a game) can increase the effectiveness of phishing detection training by up to 36%, using a technique like this in educational institutions could help younger generations to be better prepared against phishing attacks [88]. To some extent, businesses could take steps to help reduce phishing attacks. This would include things like purchasing web and email domain names that could be easily mistaken for their company and redirecting to the legitimate site; this technique is already used by some large businesses, but having to pay extra could be a problem for smaller or non-profit organizations. In the long run, this would help companies by maintaining their reputation.

Whilst researching for this paper, it became clear that the majority of current and past research regarding phishing primarily focuses on the technical approaches used by phishers and the technical prevention techniques that are being developed. However, very few of the papers analyzed aspects of the targets or tried to identify demographics or behaviors of the subjects who are most susceptible to phishing beyond standard categorization of age and gender. There is also little analysis of the effectiveness of each type of medium, vector, and technical approach against the demographics of the targets. Furthermore, there is little research into the motivations behind phishing attacks besides the most common reason of financial gain, either directly or by selling the victims credentials on the online black market (where depending on the account, the credentials can go for between $1 and $100, with even greater returns for online banking accounts depending on their contents [5]). An interesting avenue of future research could be to examine phishing from an attacker's perspective and to analyze the emotions and motivations of the phisher that could be manipulated to make preventing or apprehending phishers easier, like how the 2018 paper by Hausken et al. [89] demonstrated that attackers can be motivated by either tangible results such as economic or more abstract concepts like human or symbolic value.

Much of the latest research into technical prevention and detection methods for phishing seem to primarily focus on message content rather than other forms of phishing such as malvertizing, tab-napping, or squatting techniques. One of the main focuses of recent research has been Natural Language Processing (NLP), this technique will allow for better detection and filtering of phishing emails that implement semantic changes to get past existing filters. Research suggests that this technique is more accurate in filtering out phishing emails than existing techniques, although these methods are yet to be implemented on larger datasets [90,91]. Neural networks are also being considered as methods of phishing prevention; however, these are often criticized as they require long training periods and the knowledge of experts to tune the parameters. There is also research into other areas of machine learning being used to try and combat phishing attacks.

Future research could be done to understand the human aspects that allow for the exploitation of phishing and effective education methods, as this area is not reliably covered by the literature with most current research going into newer detection methods and tools. It would be interesting to see which education methods implemented by businesses could be used on the public; perhaps free webmail clients distributing fake or sanitized phishing attacks to educate their users, this could also be extended to other mediums like SMS or social media. Another method might be short television or radio adverts with helpful tips for avoiding phishing scams, as whilst government and organizations often have comprehensive information about reporting and spotting phishing, it is rarely advertised and information has to be sought out. This paper also serves as a record of past, current, and emerging phishing techniques to provide a good basis for further research into this fascinating area.

8. Conclusions

In conclusion, this paper highlights that phishing is a current and vital global issue. Phishing remains one of the primary infection vectors for malware [9], the primary method of infiltration used in breaches, and is the number one method used in social engineering attacks [92]. There is also the worrying trend that the number of phishing sites that were detected by the end 2019 were at the highest levels since 2016 (as shown in Figure 1). As technology continues to evolve, the range of phishing vectors will continually grow, and malicious actors will undoubtedly find ways to exploit these new vectors in more sophisticated, cutting-edge phishing attacks (for example the recent development of QRishing or the application of sound squatting on voice assistants like Amazon's Alexa). This paper shows that services are being provided to any user to perform phishing attacks for a fee. A comprehensive review of the various types of phishing attacks, from historic to the cutting edge, are presented. Each type of attack is presented and reviewed. The presented literature review, which explains the various characteristics of the different approaches and types of phishing techniques, may serve as a base for developing a more holistic anti-phishing system. Hence, it is hoped this paper will serve to build awareness amongst researchers and users, and encourage the development of anti-phishing methods by providing a broad and comprehensive knowledge base of existing phishing techniques. Finally, this paper will help to identify those areas in which anti-phishing efforts are lacking.

Funding: This research received no external funding.

Conflicts of Interest: There are no conflict of interest.

Appendix A

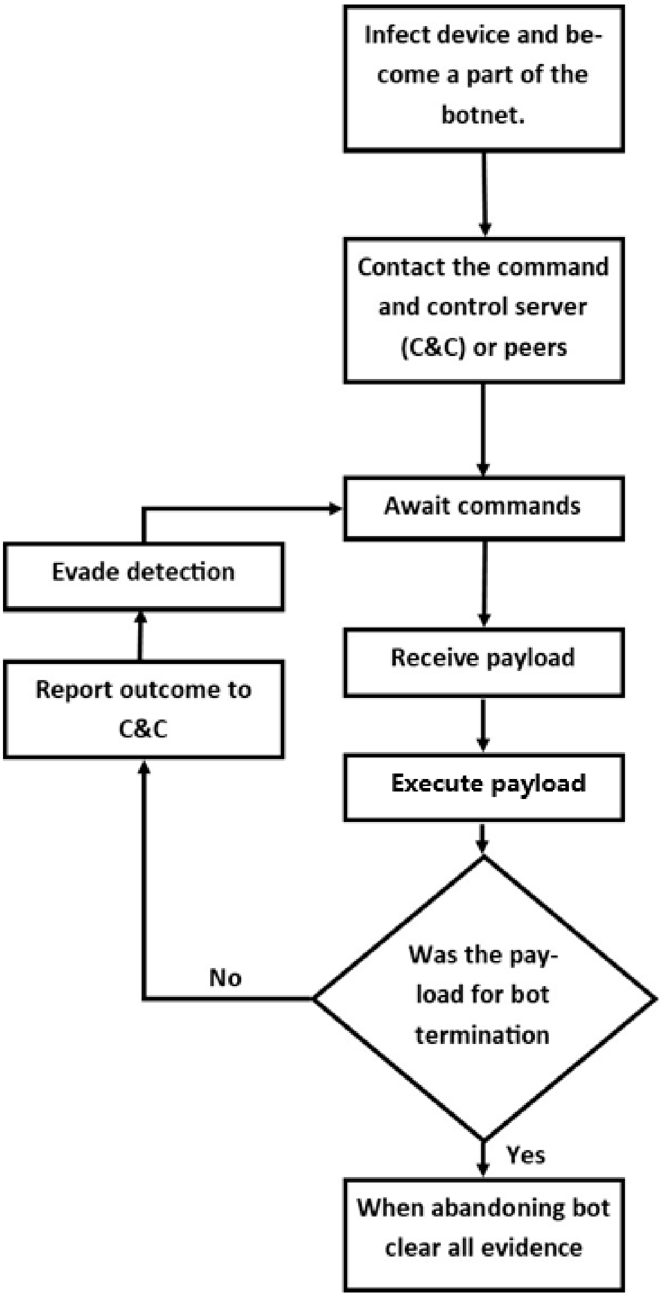

Infect device and become a part of the botnet.
Contact the command and control server (C&C) or peers
Await commands
Evade detection
Receive payload
Report outcome to C&C
Execute payload
No
Was the payload for bot termination
Yes
When abandoning bot clear all evidence

Figure A1. Flowchart Demonstrating the Lifecycle of a Bot.

Appendix B

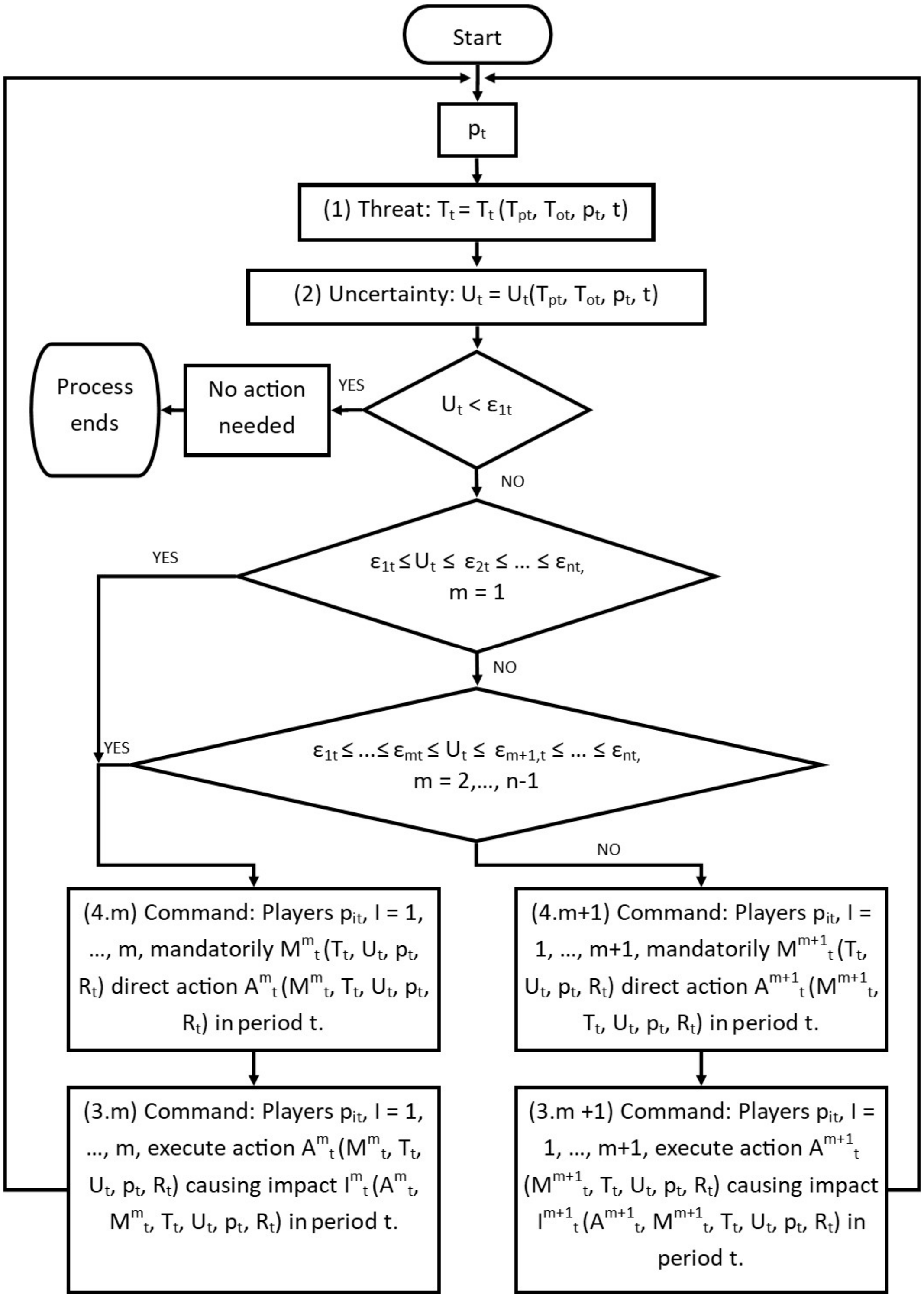

Start
p_t
(1) Threat: $T_t = T_t (T_{pt}, T_{ot}, p_t, t)$
(2) Uncertainty: $U_t = U_t(T_{pt}, T_{ot}, p_t, t)$
$U_t < \varepsilon_{1t}$
YES
No action needed
Process ends
NO
$\varepsilon_{1t} \leq U_t \leq \varepsilon_{2t} \leq \ldots \leq \varepsilon_{nt},$ m = 1
YES
NO
$\varepsilon_{1t} \leq \ldots \leq \varepsilon_{mt} \leq U_t \leq \varepsilon_{m+1,t} \leq \ldots \leq \varepsilon_{nt},$ m = 2,..., n-1
YES
NO
(4.m) Command: Players p_{it}, I = 1, ..., m, mandatorily $M^m{}_t(T_t, U_t, p_t, R_t)$ direct action $A^m{}_t(M^m{}_t, T_t, U_t, p_t, R_t)$ in period t.
(4.m+1) Command: Players p_{it}, I = 1, ..., m+1, mandatorily $M^{m+1}{}_t(T_t, U_t, p_t, R_t)$ direct action $A^{m+1}{}_t(M^{m+1}{}_t, T_t, U_t, p_t, R_t)$ in period t.
(3.m) Command: Players p_{it}, I = 1, ..., m, execute action $A^m{}_t(M^m{}_t, T_t, U_t, p_t, R_t)$ causing impact $I^m{}_t(A^m{}_t, M^m{}_t, T_t, U_t, p_t, R_t)$ in period t.
(3.m +1) Command: Players p_{it}, I = 1, ..., m+1, execute action $A^{m+1}{}_t(M^{m+1}{}_t, T_t, U_t, p_t, R_t)$ causing impact $I^{m+1}{}_t(A^{m+1}{}_t, M^{m+1}{}_t, T_t, U_t, p_t, R_t)$ in period t.

Figure A2. Figure 1 from [62]. Described as: Formalizing the precautionary principle for n players p_t, accounting for (1) a threat T_t in a time period t, t = 1, 2, 3, . . . , (2) uncertainty Ut assessed against thresholds ε_{mt} and $\varepsilon_{m+1,t}$, m = 1, . . . , n − 1, (4) command $M^m{}_t$, and (3) action $A^m{}_t$.

Appendix C

Table A1. Table containing a summary of phishing method examples.

Phishing Method	Author	Year	Samples	Country
Vishing	E. O. Yeboah-Boateng and P. M. Amanor	2014	Mrs. Sinclair	United Kingdom
	G. Ollmann	2007		
	M. Jakobsson	2007		
Whaling	A. Shankar, R. Shetty, and B. Nath	2019	Perpetrator: Evaldas Rimasauskas Victim: two US-based companies	Perpetrator: Lithuania Victims: United States
	J. Hong	2012		
	T. Dakpa and P. Augustine	2017		
BEC	Anti-Phishing working group	2019	Victims: multi-national companies	International
	I. C. C. (IC3) Federal Bureau of Investigation (FBI)	2019		
	M. Jakobsson	2019		
	K. M. Bakarich and D. Baranek	2019		
	S. Mansfield-Devine	2016		
	S. Aviv, Y. Levy, L. Wang, and N. Geri	2019		
Cross-Site Scripting	L. K. Shar and H. B. K. Tan	2018	Victim: eBay	International
	P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna	2007		
Cross-Site Malicious Captcha Attack	N. Gelernter and A. Herzberg	2016	Victim: N/A	International
QRishing	C. Joshi	2019 2013	Victim: QR code users	International
	T. Vidas, E. Owusu, S. Wang, C. Zeng, L. F. Cranor, and N. Christin			
Social Engineering	K. D. Mitnick and W. L. Simon	2003	Victim: holiday shoppers	International
	G. Harl	1997		
	M. Hasan, N. Prajapati, and S. Vohara	2010		
	B. Christensen	2014		
	P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge	2007		
	R. Heartfield and G. Loukas	2015		

Table A1. *Cont.*

Phishing Method	Author	Year	Samples	Country
Drive-by Download	M. Cova, C. Kruegel, and G. Vigna	2010	Victim: Onlinevideoconverter.com Users	International
	V. L. Le, I. Welch, X. Gao, and P. Komisarczuk	2013		
	Z. Zhaosheng, J. F. Zhi, L. Guohan, R. Phil, C. Yan, and H. Keesook	2008		
	J. Milletary	2005		
	J. Nazario and T. Holz	2008		
	R. Puri	2003		
	T. Moore and R. Clayton	2007		
	M. T. Banday and J. A. Qadri	2007		
Malvertizing	T. Nagunwa	2014	Victim: Onlinevideoconverter.com Users	International
	A. K. Sood and R. J. Enbody	2011		
	C. Dwyer and A. Kanguri	2017		
Wiphishing	J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor	2009	Perpetrators: Russian military agency, GRU Victims: international anti-doping agencies	International
	F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel	2015		
Browser Vulnerabilities	P. Satish and R. Chavan,	2017	Victim: Google Chrome users	International
Tab-Napping	A. MahaLakshmi, N. Swapna Goud, and Dr. G. Vishnu Murthy	2018	Victim: internet browser users	International
SQL Injection	J. Clark	2012	Perpetrators: Vladimir Drinkman, Alexandr Kalinin, Roman Kotov, Mikhail Rytikov, Smilianets Victim: Heartland Payment Systems	Perpetrators: Russia Victim: United States
	K. Ahmad	2010		

Table A1. *Cont.*

Phishing Method	Author	Year	Samples	Country
Typo-Squatting	J. Spaulding, A. R. Kang, S. Upadhyaya, and A. Mohaisen	2016	Victim: internet users	International
Sound-Squatting	J. Spaulding, A. R. Kang, S. Upadhyaya, and A. Mohaisen	2016	Victim: virtual assistant users (e.g., Amazon Alexa)	International
404 Error Manipulation	A. Roichman	2010	Victim: Cloudflare users	International
Cloud Computing	Vayansky, Ike & Kumar, Sathish	2018	Victim: Office 365 users	International
	P. Suryateja	2018		
Click Jacking	D. Kavitha	2015	Victim: Facebook users	International
Malicious Browser Extensions	L. F. DeKoven, S. Savage, G. M. Voelker, and N. Leontiadis	2017	Victim: internet browser users	International
Man-in-the-Middle	F. Callegati, W. Cerroni and M. Ramilli	2009	Victims: medium and large European companies	International
	A. Mallik, A. Ahsan, M. M. Z. Shahadat and J. C. Tsou	2019		
	X. Liang, S. Shetty, L. Zhang, C. Kamhoua and K. Kwiat	2017		
	R. Jabir, S. Khanji, L. Ahmad, O. Alfandi and H. Said	2016		
Mobile Phone	G. Kumar	2016	Victims: Android users	International
	B. Amro	2018		
Session Fixation	P. Shital and R. Chavan	2017	Victims: iOS users	International
	M. Johns, B. Braun, M. Schrank and J. Posegga	2010		
Javascript Obfuscation	P. Likarish, E. Jung and I. Jo	2009	Victims: users who were sent a link	International
	A. A. Orunsolu and A. S. Sodiya	2017		

References

1. Stavroulakis, P.; Stamp, M. (Eds.) *Handbook of Information and Communication Security*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2010.
2. Jakobsson, M.; Myers, S. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*; Wiley: Hoboken, NJ, USA, 2006.
3. Rekouche, K. Early Phishing. *arXiv* **2011**, arXiv:1106.4692.
4. Rader, M.A.; Rahman, S.M. Phishing Techniques and Mitigating the Associated Security Risks. *Int. J. Netw. Secur. Appl.* **2013**, *5*, 23–41. [CrossRef]
5. Symantec. ISTR Internet Security Threat Report 2019. *Symantec* **2019**, *24*, 61. Available online: https://docs.broadcom.com/doc/istr-15-april-volume-20-en (accessed on 15 December 2019).
6. Symantec. ISTR Internet Security Threat Report 2015. *Symantec* **2015**, *20*. Available online: https://docs.broadcom.com/doc/istr-24-2019-en (accessed on 15 December 2019).
7. Anti Phishing Working Group. Phishing Activity Trends Report: 3rd Quarter2019. 2019. Available online: https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf (accessed on 15 December 2019).
8. APWG. Phishing Activity Trends Reports. Available online: https://apwg.org/trendsreports/ (accessed on 27 December 2019).
9. Symantec. ISTR Internet Security Threat Report Volume 23. 2018. Available online: https://www.phishingbox.com/assets/files/images/Symantec-Internet-Security-Threat-Report-2018.pdf (accessed on 15 December 2019).
10. IBM. IBM X-Force Threat Intelligence Index 2019. 2019. Available online: https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf (accessed on 15 December 2019).
11. ICC (IC3)/Federal Bureau of Investigation (FBI). Internet Crime Report 2018. 2018. Available online: https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219 (accessed on 20 December 2019).
12. Seals, T. Elder Scrolls Online Targeted by Cybercrooks Hunting In-Game Loot. *Threatpost* **2019**. Available online: https://threatpost.com/elder-scrolls-online-cybercrooks-in-game-loot/150934/ (accessed on 20 December 2019).
13. Zetter, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *WIRED* **2018**. Available online: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (accessed on 20 December 2019).
14. Chiew, K.L.; Yong, K.S.C.; Tan, C.L. A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Syst. Appl.* **2018**, *106*, 1–20. [CrossRef]
15. Shankar, A.; Shetty, R.; Nath, B. A Review on Phishing Attacks. *Int. J. Appl. Eng. Res.* **2019**, *14*, 2171–2175.
16. Shaikh, A.N.; Shabut, A.M.; Hossain, M.A. A literature review on phishing crime, prevention review and investigation of gaps. In Proceedings of the 2016 10th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2016), Chengdu, China, 15–17 December 2016; pp. 9–15.
17. Chaudhary, G.K. Development Review on Phishing: A Computer Security Threat. *Int. J. Adv. Res. Comput. Sci. Manag. Stud.* **2014**, *2*, 55–64.
18. Suganya, V. A Review on Phishing Attacks and Various Anti Phishing Techniques. *Int. J. Comput. Appl.* **2016**, *139*, 20–23. [CrossRef]
19. Purkait, S. Phishing counter measures and their effectiveness—Literature review. *Inf. Manag. Comput. Secur.* **2012**, *20*, 382–420. [CrossRef]
20. Mohammad, R.M.; Thabtah, F.; McCluskey, L. Tutorial and critical analysis of phishing websites methods. *Comput. Sci. Rev.* **2015**, *17*, 1–24. [CrossRef]
21. Atkins, B.; Huang, W. A Study of Social Engineering in Online Frauds. *Open J. Soc. Sci.* **2013**, *1*, 23–32. [CrossRef]
22. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
23. Singh, N.P. Online Frauds in Banks with Phishing. *J. Internet Bank. Commer.* **2007**, *12*, 1–27.
24. Hausken, K.; Levitin, G. Review of systems defense and attack models. *Int. J. Perform. Eng.* **2012**, *8*, 355–366.
25. Chawki, M. Phishing in Cyberspace: Issues and Solutions. 2006. Available online: http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions (accessed on 17 December 2019).
26. Skog, R.; Torok, E. Multimedia Messaging Service Routing System and Method. U.S. Patent 6947738B2, 20 September 2005.

27. El-Fishawy, S.; Othmer, K. Delivery of Voice Data from Multimedia Messaging Service Messages. U.S. Patent 7,133,687 B1, 7 November 2006.
28. Wang, Y.; Streff, K.; Raman, S. Smartphone security challenges. *Computer* **2012**, *45*, 52–58. [CrossRef]
29. Kleinrock, L. Comments on 'an early history of the internet'. *IEEE Commun. Mag.* **2011**, *49*, 12.
30. Frauenstein, E.D.; Flowerday, S.V. Social network phishing: Becoming habituated to clicks and ignorant to threats? In Proceedings of the 2016 Information Security for South Africa (ISSA), Johannesburg, South Africa, 17–18 August 2016; pp. 98–105.
31. Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *J. Emerg. Trends Comput. Inf. Sci.* **2014**, *5*, 297–307.
32. Jakobsson, M. The Human Factor in Phishing. *Priv. Secur. Consum. Inf.* **2007**, *7*, 1–19.
33. Jamil, A.; Asif, K.; Ghulam, Z.; Nazir, M.K.; Alam, S.M.; Ashraf, R. MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 5040–5048.
34. Caputo, D.D.; Pfleeger, S.L.; Freeman, J.D.; Johnson, M.E. Going spear phishing: Exploring embedded training and awareness. *IEEE Secur. Priv.* **2014**, *12*, 28–38. [CrossRef]
35. Heartfield, R.; Loukas, G. A Taxonomy of Attacks and a Survey of Defense Mechanisms for Semantic Social Engineering Attacks. *ACM Comput. Surveys* **2015**. [CrossRef]
36. Lin, T.; Capecci, D.E.; Ellis, D.M.; Rocha, H.A.; Dommaraju, S.; Oliveira, D.S.; Ebner, N.C. Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Trans. Comput. Interact.* **2019**, *26*, 32. [CrossRef]
37. Oliveira, D.; Rocha, H.; Yang, H.; Ellis, D.; Dommaraju, S.; Muradoklu, M.; Weir, D.; Soliman, A.; Lin, T.; Ebner, N.; et al. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, USA, 6–11 May 2017; Volume 2017, pp. 6412–6424.
38. Tankard, C. Advanced Persistent threats and how to monitor and deter them. *Netw. Secur.* **2011**, *2011*, 16–19. [CrossRef]
39. Hong, J. The Current State of Phishing Attacks. *Commun. ACM* **2012**, *55*, 74–81. [CrossRef]
40. Dakpa, T.; Augustine, P. Study of Phishing Attacks and Preventions. *Int. J. Comput. Appl.* **2017**, *163*, 5–8. [CrossRef]
41. Jakobsson, M. The Rising Threat of Launchpad Attacks. *IEEE Secur. Priv.* **2019**, *17*, 68–72. [CrossRef]
42. Bakarich, K.M.; Baranek, D. Something Phish-y is Going On Here: A Teaching Case on Business Email Compromise. *Curr. Issues Audit.* **2019**, *14*, A1–A9. [CrossRef]
43. Mansfield-Devine, S. The imitation game: How business email compromise scams are robbing organisations. *Comput. Fraud Secur.* **2016**, *2016*, 5–10. [CrossRef]
44. Aviv, S.; Levy, Y.; Wang, L.; Geri, N. An expert assessment of corporate professional users to measure business email compromise detection skills and develop a knowledge and awareness training program. In Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy, Munich, Germany, 15 December 2019.
45. Shar, L.K.; Tan, H.B.K. Defending Against Cross Site Scripting Attacks. *IEEE Comput. Soc.* **2018**, *45*, 55–62. [CrossRef]
46. Vogt, P.; Nentwich, F.; Jovanovic, N.; Kirda, E.; Kruegel, C.; Vigna, G. Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. In Proceedings of the Network and Distributed System Security Symposium (NDSS 2007), San Diego, CA, USA, 28 February–2 March 2007.
47. Gelernter, N.; Herzberg, A. Tell me about yourself: The malicious CAPTCHA Attack. In Proceedings of the 25th International World Wide Web Conference (WWW 2016), Montréal, QC, Canada, 11–15 April 2016; pp. 999–1008.
48. Joshi, C. QR Codes in E-Commerce: 7 Ways Amazon is Getting It Right! *Beaconstac* **2019**. Available online: https://blog.beaconstac.com/2019/04/qr-codes-in-e-commerce-ways-amazon-is-getting-it-right/ (accessed on 21 December 2019).

49. Vidas, T.; Owusu, E.; Wang, S.; Zeng, C.; Cranor, L.F.; Christin, N. QRishing: The susceptibility of smartphone users to QR code phishing attacks. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7862, pp. 52–69.
50. Mitnick, K.D.; Simon, W.L. *The Art of Deception: Controlling the Human Element in Security*; Wiley: Hoboken, NJ, USA, 2003; ISBN 978-0-471-23712-9.
51. Harl, G. People Hacking—The Psychology of Social Engineering. *Text of Harl's Talk at Access All Areas III*. 1997. Available online: https://barzha.cyberpunk.us/lib/cin/se10.html (accessed on 21 December 2019).
52. Hasan, M.; Prajapati, N.; Vohara, S. Case Study On Social Engineering Techniques for Persuasion. *Int. J. Appl. Graph Theory Wirel. Ad Hoc Netw. Sens. Netw.* **2010**, *2*, 17–23. [CrossRef]
53. Christensen, B. PHISHING SCAM—'Request to Terminate Microsoft Account'. Hoax-Slayer. 2014. Available online: https://www.hoax-slayer.net/phishing-scam-request-to-terminate-microsoft-account/ (accessed on 21 December 2019).
54. Kumaraguru, P.; Rhee, Y.; Acquisti, A.; Cranor, L.F.; Hong, J.; Nunge, E. Protecting people from phishing: The design and evaluation of an embedded training email system. In Proceedings of the 2007 Conference on Human Factors in Computing Systems (CHI 2007), San Jose, CA, USA, 28 April–3 May 2007; pp. 905–914.
55. Cova, M.; Kruegel, C.; Vigna, G. Detection and analysis of drive-by-download attacks and malicious JavaScript code. In Proceedings of the 19th International Conference on World Wide Web (WWW 2010), Raleigh, NC, USA, 26–30 April 2010; pp. 281–290.
56. Le, V.L.; Welch, I.; Gao, X.; Komisarczuk, P. Anatomy of Drive-by Download Attack. In *Proceedings of the Proceedings of the Eleventh Australasian Information Security Conference—Volume 138*; Australian Computer Society, Inc.: Adelaide, Australia, 2013; pp. 49–58. [CrossRef]
57. Zhaosheng, Z.; Zhi, J.F.; Guohan, L.; Phil, R.; Yan, C.; Keesook, H. Botnet research survey. In Proceedings of the 2008 32nd Annual IEEE International Computer Software and Applications Conference, Turku, Finland, 28 July–1 August 2008; pp. 967–972.
58. Milletary, J. Technical Trends in Phishing Attacks. Available online: https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_50315.pdf (accessed on 21 December 2019).
59. Nazario, J.; Holz, T. As the net churns: Fast-flux botnet observations. In Proceedings of the 3rd International Conference on Malicious and Unwanted Software (MALWARE 2008), Fairfax, VI, USA, 7–8 October 2008; pp. 24–31.
60. Puri, R. Bots & Botnet: An Overview. SANS Institute. 2003. Puri, R. (2003). Bots & Botnet: An Overview. Available online: https://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299 (accessed on 21 December 2019).
61. Moore, T.; Clayton, R. Examining the impact of website take-down on phishing. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit on—eCrime '07*; ACM Press: New York, NY, USA, 2007; Volume 269, pp. 1–13. [CrossRef]
62. Hausken, K. The Precautionary Principle as Multi-Period Games Where Players Have Different Thresholds for Acceptable Uncertainty. 2020. Available online: https://doi.org/10.1016/j.ress.2020.107224 (accessed on 21 December 2019).
63. Banday, M.T.; Qadri, J.A. Phishing—A Growing Threat to E-Commerce. *Bus. Rev.* **2011**, *12*, 76–83.
64. Nagunwa, T. Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors. *Int. J. Cyber-Secur. Digit. Forensics* **2014**, *3*, 72–83. [CrossRef]
65. Sood, A.K.; Enbody, R.J. Malvertising—Exploiting web advertising. *Comput. Fraud Secur.* **2011**, *2011*, 11–16. [CrossRef]
66. Dwyer, C.; Kanguri, A. Malvertising—A Rising Threat to The Online Ecosystem. *J. Inf. Syst. Appl. Res.* **2017**, *10*, 29–37.
67. Sunshine, J.; Egelman, S.; Almuhimedi, H.; Atri, N.; Cranor, L.F. Crying Wolf: An Empirical Study of SSL Warning Effectivenes. In Proceedings of the 18th USENIX Security Symposium, Montreal, QC, Canada, 10–14 August 2009.

68. Lanze, F.; Panchenko, A.; Ponce-Alcaide, I.; Engel, T. Hacker's toolbox: Detecting software-based 802.11 evil twin access points. In Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC 2015), Las Vegas, NV, USA, 9–12 January 2015; pp. 225–232.
69. Kumar, D.; Paccagnella, R.; Murley, P.; Hennenfent, E.; Mason, J.; Bates, A.; Bailey, M. Emerging Threats in Internet of Things Voice Services. *IEEE Secur. Priv.* **2019**, *17*, 18–24. [CrossRef]
70. Raam, M. Cain and Abel—Man in the Middle (MITM) Attack Tool Explained. 2019. Available online: https://cybersguards.com/cain-and-abel-man-in-the-middle-mitm-attack-tool-explained/ (accessed on 27 December 2019).
71. Chen, S.; Fan, L.; Chen, C.; Xue, M.; Liu, Y.; Xu, L. GUI-Squatting Attack: Automated Generation of Android Phishing Apps. *IEEE Trans. Dependable Secur. Comput.* **2019**. [CrossRef]
72. Qabajeh, I.; Thabtah, F.; Chiclana, F. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Comput. Sci. Rev.* **2018**, *29*, 44–55. [CrossRef]
73. Misra, G.; Arachchilage, N.A.G.; Berkovsky, S. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. *arXiv* **2017**, arXiv:1710.06064.
74. Siadati, H.; Palka, S.; Siegel, A.; McCoy, D. Measuring the effectiveness of embedded phishing exercises. In Proceedings of the 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 2017), Vancouver, BC, Canada, 14 August 2017; Available online: https://www.researchgate.net/publication/319128761_Measuring_the_Effectiveness_of_Embedded_Phishing_Exercises (accessed on 21 December 2019).
75. Alghoul, A.; Al Ajrami, S.; Al Jarousha, G.; Harb, G.; Abu-Naser, S.S. Email Classification Using Artificial Neural Network. *Int. J. Acad. Eng. Res.* **2018**, *2*, 8–14.
76. Ying, P.; Xuhua, D. Anomaly based web phishing page detection. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), Miami Beach, FL, USA, 11–15 December 2006; pp. 381–390.
77. Somesha, M.; Pais, A.R.; Rao, R.S.; Rathour, V.S. Efficient deep learning techniques for the detection of phishing websites. *Sadhana Acad. Proc. Eng. Sci.* **2020**, *45*. [CrossRef]
78. Hausken, K. Cyber resilience in firms, organizations and societies. *Internet Things* **2020**, *11*, 100204. [CrossRef]
79. Bier, V.; Gutfraind, A. Risk analysis beyond vulnerability and resilience—Characterizing the defensibility of critical systems. *Eur. J. Oper. Res.* **2019**, *276*, 626–636. [CrossRef]
80. Bostick, T.P.; Connelly, E.B.; Lambert, J.H.; Linkov, I. Resilience science, policy and investment for civil infrastructure. *Reliab. Eng. Syst. Saf.* **2018**, *175*, 19–23. [CrossRef]
81. Jain, A.K.; Gupta, B.B. Phishing Detection: Analysis of Visual Similarity Based Approaches. *Secur. Commun. Netw.* **2017**, *2017*, 5421046. [CrossRef]
82. Anti Phishing Working Group. *Phishing Activity Trends Report: 4th Quater 2019*. 2019. Available online: https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf (accessed on 21 December 2019).
83. Anti Phishing Working Group. *Phishing Activity Trends Report: 2nd Quater 2020*. 2020. Available online: https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf (accessed on 21 December 2019).
84. Dupuis, M.; Geiger, T.; Slayton, M.; Dewing, F. The use and non-use of cybersecurity tools among consumers: Do they want help? In Proceedings of the 20th Annual Conference on Information Technology Education (SIGITE 2019), Tacoma, WA, USA, 3–5 October 2019; Volume 19, pp. 81–86. [CrossRef]
85. Goel, D.; Jain, A.K. Mobile Phishing Attacks and Defence Mechanisms: State of Art and Open Research Challenges. *Comput. Secur.* **2018**, *73*, 519–544. [CrossRef]
86. Gutierrez, C.N.; Kim, T.; Della Corte, R.; Avery, J.; Goldwasser, D.; Cinque, M.; Bagchi, S. Learning from the Ones That Got Away: Detecting New Forms of Phishing Attacks. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 988–1001. [CrossRef]
87. Hausken, K. Security investment, hacking, and information sharing between firms and between hackers. *Games* **2017**, *8*, 23. [CrossRef]
88. Wen, Z.A.; Lin, Z.; Chen, R.; Andersen, E. What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems—CHI '19*; ACM Press: Scotland, UK, 2019; pp. 1–12. [CrossRef]
89. Hausken, K. A cost–benefit analysis of terrorist attacks. *Def. Peace Econ.* **2018**, *29*, 111–129. [CrossRef]
90. Verma, P.; Goyal, A.; Gigras, Y. Email Phishing: Text Classification Using Natural Language Processing. *Comput. Sci. Inf. Technol.* **2020**, *1*, 1–12. [CrossRef]

91. Kumar, A.; Chatterjee, J.; Díaz, V.G. A Novel Hybrid Approach of SVM Combined with NLP and Probabilistic Neural Network for Email Phishing. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 486–493. [CrossRef]
92. Verizon Verizon: 2019 Data Breach Investigations Report. *Comput. Fraud Secur.* **2019**, *2019*, 4. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.