**CHAPTER–1**

**INTRODUCTION**

Phishing is a security threat to steal the credential information like username, password and credit card details. A phishing attack is a leading cause of credential loss in the internet world and occurs because of poor security and lack of awareness. In the internet world, providing security to the client is very important because of client satisfaction. In this attacker sends a link to the victim through mail or network, then victims click the link and submit their credentials without any awareness about the phishing attack. It is one type of security threat in the internet world. An extension aims to reduce the phishing attack in the browser, which is working as a background. It detects the phished URLs and information to the user.

* 1. **INTRODUCTION TO DOMAIN ( PHISHING )**

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website that matches the look and feel of the legitimate site. Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators. Attempts to deal with phishing incidents include legislation, user training, public awareness, and technical security measures. A phishing technique was described in detail in a paper and presentation delivered to the 1987 International HP Users Group in the 1980s. The first recorded mention of the term is found in the hacking tool AOHell (according to its creator), which included a function for attempting to steal the passwords or financial details of America Online users in the 1990s. The first known phishing attack against a retail bank was reported by The Banker in September 2003. It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing. Recently, the company block. one, which developed the EOS.IO blockchain, was attacked by a phishing group who sent phishing emails to all customers, aimed at intercepting the user's cryptocurrency wallet key. Phishing attack increase year by year, there is no constant interval in the phishing report. Phishing on AOL was closely associated with the warez community that exchanged unlicensed software and the black hat hacking scene that perpetrated credit card fraud and other online crimes. The term was used because "<><" is the single most common tag of HTML that was found in all chat transcripts naturally, and as such could not be detected or filtered by AOL staff. The symbol <>< was replaced for any wording that referred to stolen credit cards, accounts, or illegal activity. Since the symbol looked like a fish, and due to the popularity of phreaking it was adapted as "Phishing". AOHell, released in early 1995, was a program designed to hack AOL users by allowing the attacker to pose as an AOL staff member, and send an instant message to a potential victim, asking him to reveal his password. To lure the victim into giving up sensitive information, the message might include imperatives such as "verify your account" or "confirm billing information". AOL enforcement would detect words used in AOL chat rooms to suspend the accounts of individuals involved in counterfeiting software and trading stolen accounts. Eventually, AOL's policy enforcement forced copyright infringement off AOL servers, and AOL promptly deactivates accounts involved in phishing, often before the victims could respond. The shutting down of the warez scene on AOL caused most phishers to leave the service.



***Figure 1.1 Phishing***

## COURTESY: PHISHING BY CASEY CRANE

In general, a phishing scam is a type of cyber attack that cybercriminals use to get users to perform some type of action. These emails are often sent out in mass to trick unsuspecting individuals into falling for their scams. Think of your best bud — the Nigerian Prince who keeps trying to get you to take his money for "safekeeping." However, phishing has evolved significantly since his royal highness first entered the scene. There is now a variety of phishing attacks targeting businesses each day. Some involve the use of emails and websites; others may use text messages or even phone calls. Attacks use these methods to get users to provide personal or account information or to make wire transfer funds to fraudulent accounts. The cybercrime industry is reaching unprecedented levels. Cybersecurity Ventures reports that the damages of cybercrime are expected to cost the world $6 trillion annually by 2021 — of which phishing is anticipated to play a significant role.

**1.2 TYPES OF PHISHING ATTACK:**

**1.2.1 BUSINESS EMAIL COMPROMISE:**

The first type of phishing we’ll discuss is known as CEO fraud. In a nutshell, CEO fraud occurs when a cybercriminal sends an email to a lower-level employee typically someone who works in the accounting or finance department while pretending to be the company’s CEO or another executive, manager, etc. The goal of these emails is often to get their victim to transfer funds to a fake account. Just a bit of bonus info for your upcoming trivia night: In the U.S., CEO fraud is often referred to as business email compromise (BEC), which the FBI says costs businesses billions of dollars.

**1.2.2 CLONE PHISHING**

The idea behind a clone phishing attack is to take advantage of legitimate messages that the victim may have already received and created a malicious version of it. The attack creates a virtual replica of a legitimate message hence, the attack's clever name and sends the message from an email address that looks legitimate. Any links or attachments in the original email are swapped out for malicious ones. The cybercriminal often uses the excuse that they're re-sending the original message because of an issue with the previous email's link or attachment to lure end-users into clicking on them. We wish we could say that this doesn't work; unfortunately, though, it often does because it catches users unawares.

**1.2.3 DOMAIN SPOOFING**

The next type of phishing we want to mention is known as domain spoofing. This method of attack uses either email or fraudulent websites. Domain spoofing occurs when a cybercriminal “spoofs” an organization or company’s domain to: make their emails look like they’re coming from the official domain, or make a fake website look like the real deal by adopting the real site’s design and using either a similar URL or Unicode characters that look like ASCII characters. In the case of an email-based attack, a cybercriminal forges a new email header that makes it appear like the email is originating from a company’s legitimate email address. In a website domain spoof, the cybercriminal creates a fraudulent website and with a domain that looks legitimate or is close to the original.

**1.2.4 EVIL TWIN**

Evil twin phishing involves a cybercriminal creating a Wi-Fi hotspot that looks like the real one they’ll even use the set service identifier (SSID) that is the same as the real network. When end-users connect, the attacker can then eavesdrop on their network traffic and steal their account names, passwords, and view any attachments that the user accesses while connected to the compromised hotspot.

**1.2.5 HTTPS PHISHING**

58% of all phishing websites are now served via HTTPS. The approach cybercriminals use in these attacks is to send an email with only a legitimate-looking link in the email body. There's often no other content except for the link itself, which may be clickable or a non-active link that requires the recipient to copy-and-paste the URL into their web address bar.

**1.2.6 SMISHING**

SMS phishing, or “smishing,” is a form of phishing that capitalizes on the world’s addiction to text messaging and instant communications. Ever receive a text message from Chipotle? How about Ticketmaster? Smishing is a way for cybercriminals to lure users into downloading malicious payloads by sending text messages that appear to come from legitimate sources and contain malicious URLs for them to click on. It could be something disguised as a coupon code 20% off your next burrito purchase or it could be an offer to win free tickets to an upcoming show.

**1.2.7 SPEAR PHISHING**

A spear-phishing attack is a targeted form of phishing. Unlike general phishing emails, which use spam-like tactics to blast thousands of people in massive email campaigns, spear-phishing emails target specific individuals within an organization. They use social engineering tactics to help tailor and personalize the emails to their intended victims. They may use email subject lines that would be topics of interest to the email recipients to trick them into opening the message and clicking on links or attachments.

**1.2.8 VISHING**

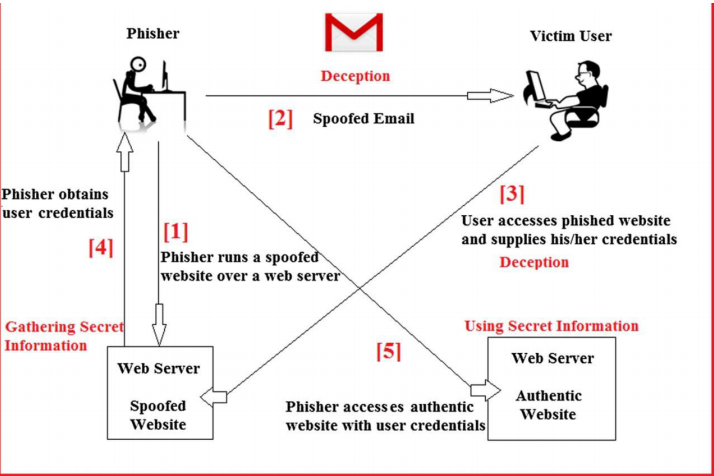
Vishing is voice phishing (phishing over the phone), then you're correct. A vishing attack occurs when a criminal calls your phone to try to get you to provide personal or financial information. They often use automated calls that re-route individuals who fall for their tactics and end up speaking with the criminals themselves. They also use mobile apps and other techniques to spoof their phone number or to hide their phone numbers entirely. These attackers frequently use a variety of social engineering tactics to trick you into providing this information. They also are known to pretend to be someone else the IRS, your bank, or an executive at your company who claims to work at another branch. They'll claim that you owe taxes, or that your credit card has suspicious activity and needs to be shut down right away… they'll first just need to verify your personal information before they can close the card and reissue a new one.

**1.2.9 WHALING**

Whaling, a form of spear phishing, is a lot like the inverse version of CEO fraud. Instead of targeting lower-level individuals within an organization, the cybercriminal instead targets high-level executives such as CEOs, CFOs, and COOs. The goal is to trick the executive into revealing sensitive information and corporate data. These targets are carefully selected because of their access and authority within an organization. These attacks often use email and website spoofing.

**1.3 WORKING OF PHISHING ATTACK THROUGH EMAIL**

Figure 1.2 represents how the phishing attack works through email. Phishing attacks can vary, but they have a few things in common: They exploit human nature rather than exclusively technological vulnerabilities They trigger emotions by suggesting their request is urgent They spoof a trusted identity Here’s how they work: The targeted victim receives a phishing email with either a URL link or attachment purporting to be from a trusted sender, such as a bank or business service provider. For URL phishing attacks, the email message may ask the recipient to log into a financial or service account. If the recipient clicks the URL link, they are taken to a fake webpage which looks very similar to the site of the organization the attacker is imitating. Attackers also leverage attachments to deliver malicious macros or software that runs when the user opens the document or enables its contents. The open attachment installs malware on the user’s machine that can let the attacker steal information or take control of the system.



***Figure 1.2 Working of phishing attack through email***

# COURTESY: HOW PHISHING ATTACK WORKS BY JOE SCHWARTZ

**1.3.1 PHISHER**

A phisher is a person, who tricks the internet user to scam their credential details. Phishers have become more skilled at forging websites to appear identical to the expected location, even including logos and graphics in the phishing emails to make them more convincing.

**1.3.2 VICTIM**

A victim is an internet user, how targeted for a phishing attack. They receive an email from the phisher based upon the things related to their greedy things, and they submit their credential for login without any awareness about the phishing attack.

**1.3.3 PHISHED OR SPOOFED EMAIL**

Phishing emails come in many forms, but the one thing they all have in common is that they contain a payload. This will either be an infected attachment that you’re asked to download or a link to a bogus website that requests login and other sensitive information.

**1.3.4 AUTHENTIC WEBSERVER**

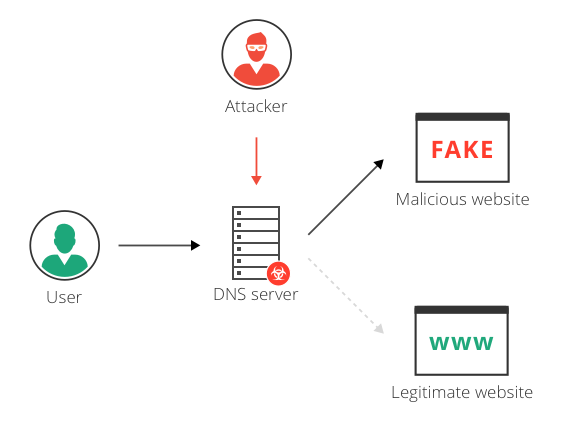
An authentic web server is a legitimate web server which contains the legal things of the organization about their clients; through which client request their service and receive the service. For this, they need protection by providing username and password to the clients.

**1.3.5 SPOOFED WEBSERVER**

Web spoofing is to trick users to connect to a different Web server than they intended. Web spoofing may be done in several ways. It can be done by simply providing a link to a fraudulent Web site that looks legitimate or involve more complex attacks in which the user's request or Web pages requested by the user are intercepted and altered. Phisher uses a spoofed server to scam internet users.

**1.4 WORKING OF PHISHING ATTACK THROUGH NETWORK**

Figure 1.3 represents How a phishing attack works through the network. DNS spoofing is an attack in which traffic is redirected from a legitimate website such as www.google.com to a malicious website such as google.attacker.com. DNS spoofing can be achieved by DNS redirection. For example, attackers can compromise a DNS server, and in this way "spoof" legitimate websites and redirect users to malicious ones.



***Figure 1.3 Working of phishing attack through the network***

# COURTESY: PHISHING ATTACK THROUGH BY IMPERVA

### 1.4.1 DOMAIN NAME SERVER (DNS)

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.

**1.4.2 DOMAIN NAME**

A domain name is your website name. A domain name is an address where Internet users can access your website. A domain name is used for finding and identifying computers on the Internet. Computers use IP addresses, which are a series of numbers. However, it is difficult for humans to remember strings of numbers. Because of this, domain names were developed and used to identify entities on the Internet.

**1.4.3 DOMAIN IP ADDRESS**

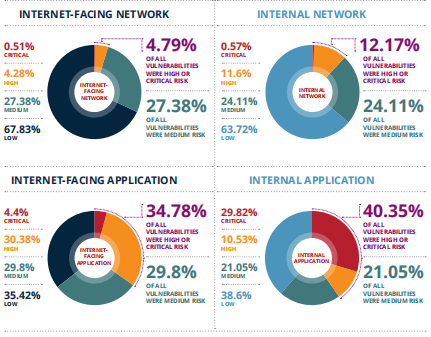
An Internet Protocol, or IP, address is different than a domain name. The IP address is an actual set of numerical instructions. It communicates exact information about the address in a way that is useful to the computer but makes no sense to humans. The domain name functions as a link to the IP address. Links do not contain actual information, but they do point to the place where the IP address information resides. It is convenient to think of IP addresses as the actual code and the domain name as a nickname for that code. A typical IP address looks like a string of numbers. It could be 232.17.43.22, for example. However, humans cannot understand or use that code. To summarize, the domain name is a part of the URL, which points to the IP address.

**1.4.4 ATTACKER**

An attacker replaces the IP address of the legitimate webserver to the malicious web server in a DNS server, which will redirect the internet user to the malicious site and it will mostly happen within the LAN network.

**1.5 PROBLEM DEFINITION**

As per the 2019 report, we also delve into "internal" cybersecurity, looking at metrics which may not seem as important, but are a valuable defense in the case of APT, malware infection, ransomware or other internal attacks. These leverage common vulnerabilities in corporate networks to spread across the enterprise. This report provides a glimpse of a global snapshot across dozens of industry verticals on how to prioritize what is important, as not all vulnerabilities are equal.



***Figure 1.4*** ***Phishing attack from 2016 - 2019***

**COURTESY: PHISHING ATTACKS ON HTTPS BY SAM COOK**

More than 60% of security professionals estimate that their organization's security function, spend over 3 hours per day validating false-positives, according to our 2019 cyber survey at Infosecurity Europe. leveraged to compromise entire local governments and councils. Dozens of cities were hit by coordinated ransomware attacks that forced services offline and demanded payment for restoration. Some cities even capitulated and paid the ransoms.

The current cybersecurity skills shortage is being experienced by the security professionals who responded to the survey. Only 32% feel they are fully-staffed and the remainder, 68%, need more staff to manage their organization's cybersecurity and comfortably deal with vulnerability intelligence. Despite AI/ML and investment in cyber, only a small percentage of organizations believe they have a high degree of confidence in their ability to measure, mitigate and manage cyberattacks.

Artificial Intelligence (AI) and Machine Learning (ML) have been high on the investment radar for some time, however, it appears in early 2020 that the paradigm is losing some of its shine. The market is realizing plenty of snake oil relating to AI technologies, but we will have to wait and see if the dial moves in a positive direction this year, as a result of significant AI marketing and investment in 2019. Despite AI/ML and investment in cyber, only a small percentage of organizations believe they have a high degree of confidence in their ability to measure, mitigate and manage cyberattacks.

More than 8 Billion records were breached in 2019. A few examples: Quest Diagnostics: 11.9 mils, Houzz: 48.9 mils, Capital One: 100 mils, Dubsmash: 161.5 mils, Zynga: 218 mil – Many of which were web application layer vulnerabilities and were preventable issues, if appropriate secure development and visibility practices were adhered to.

**1.6 OBJECTIVE**

The main objective of Phishing alerts is to make the browser think smart in case of an attack and also to make the alerts faster so that the possibility of secure the victim's sensitive information. Day by day the phishing attacks are increasing worldwide and lead to the loss of much sensitive information. Many reasons for this are self-detection which means manual detection, less awareness about the phishing attack and victims are attracted due to greedy things. This is a situation that is prevailing in our day to the day internet world. A thought of finding some solution to resolve this problem comes up with this idea of giving the alerts about phishing URL as soon as possible and in TIME….!!!! Because after all time matters a lot if everything is done in time, at least the victim will be alerted before they going to lose their credential details due to a phishing attack.

**1.7 KEYWORDS**

**1.7.1 PHISHING**

Phishing is an online scam where criminals impersonate legitimate entities to trick victims into sharing sensitive information or installing malware. The term "phishing" is a play on the word "fishing" since in both cases someone throws out the bait and waits for users or fish to "bite". Most often hackers do this via malicious emails that appear to be from trusted senders by including a link that will seem to take you to the company's website. Once you fill in your data, that sensitive information can be stolen.

Figure 1.5 represents a phishing attack. That data can be any private information that could be valuable, such as login credentials, financial or even personal data. Phishing is considered a type of social engineering attack because it relies on human failures instead of hardware or software.



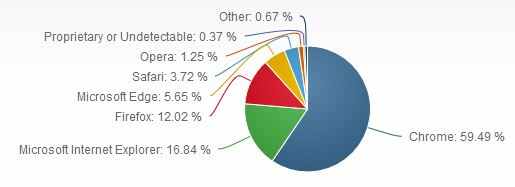
***Figure 1.5 Phishing***

**COURTESY: PHISHING BY GABRIELA GAVRAILOVA**

**1.7.2 BROWSER**

A browser is a software application used to locate, retrieve and display content on the World Wide Web, including webpages, images, video, and other files. As a client/server model, the browser is the client run on a computer or mobile device that contacts the Web server and requests information. The web server sends the information back to the browser which displays the results on the Internet-enabled device that supports a browser.

Today's browsers are fully-functional software suites that can interpret and display HTML Web pages, JavaScript, AJAX and other content hosted on web servers. Many browsers offer plug-ins that extend the capabilities of the software so it can display multimedia information, or the browser can be used to perform tasks such as videoconferencing, to design web pages or add anti-phishing filters and other security features to the browser. The three most popular desktop browsers, according to Net Marketshare (June 2019), is Chrome (66.46%), followed by Firefox (9.50%), Microsoft Internet Explorer (8.84%), and Edge (4.71%). Other major browsers include Apple Safari, Sogou Explorer and Opera.

****

***Figure 1.6 Browser usage statics***

**COURTESY: BROWSER BY VANGIE BEAL**

**1.7.3 INTERNET USERS**

Over 460 million internet users, India is the second-largest online market, ranked only behind China. By 2021, there will be about 635.8 million internet users in India. Despite the large base of internet users in India, only 26 percent of the Indian population accessed the internet in 2015. This is a significant increase in comparison to the previous years, considering the internet penetration rate in India stood at about 10 percent in 2011. Furthermore, men dominated internet usage in India with 71 percent to women's 29 percent.

The Internet is perceived predominantly as a requirement for the youth in both rural and urban India with activities like social networking, entertainment, etc. That makes the internet an integral part of daily life.



***Figure 1.7 Internet users***

**COURTESY: INTERNET USERS BY MANIKANDAN ANNAMALAI**

**1.7.4. PLUGIN**

An extension, in computer operating systems, is a piece of software that enhances or "extends" the capabilities of a programming language or other applications. An extension adds extra features to an already working standalone application. Usually, an extension itself is not independently functional and needs other software with which to work.

**1.8 AN OUTLINE OF EXISTING SYSTEM**

In existing system plugin's are available, they are provided by Microsoft, Netcraft, and Google. These organizations provide the security service to other organization that in need, in return they pay it. But normal internet user, who can't get these service, they are also a victim for the attackers, who can only detect phished URL by manual checking.

**1.8.1 DISADVANTAGES OF EXISTING SYSTEM**

* There is no existing system for automatic check and report about the attack.
* In today's busy life, if an internet user in attack without awareness, they can't check the URL manually.
* But if an internet user doesn't have awareness, the victim's credential details can be used for any illegal activity.
* Security in the domain of Phishing is still under research.

**1.9 SUMMARY**

Phishing has higher rates of attack than any other security attack in India. Hence, awareness about the attack alone is not sufficient to prevent attacks and save victims sensitive information. The solution proposed in this work to address this sensitive information problem is the phishing alerts. This phishing alert is augmented with a classification algorithm, which in turn becomes smart enough to decide the action plan after an attack starts. This works out even in the case where internet users accessing illegal activities. As technological advancements enable internet users to secure sensitive information, farther and prevent an attack, experts are using a blacklist to collect URL of the previous attack that could be reduced, if the same attack is happening. Up to 85% of attack can be detected using the classification algorithm and there is some level of false rate detection. Mortality rates can be reduced. Thus, this phishing alerts replaces the role of human upon an attack by making itself intelligent. Also, phishing alerts will reduce the loss of sensitive information due to the intelligence of an extension.