Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. This occurs when an attacker pretends to be a trusted entity to dupe a victim into clicking a malicious link, that can lead to the installation of malware, freezing of the system as part of a ransomware attack, or revealing of sensitive information.

Phishing is one of the oldest types of cyberattacks, dating back to the 1990s. Despite having been around for decades, it is still one of the most widespread and damaging cyberattacks.

Two key consequences of phishing are:

1. Financial loss
2. Data loss and legal lawsuits

Understanding phishing techniques

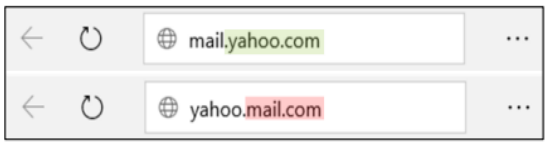
Types of phishing techniques – Link manipulation

Link manipulation is done by directing a user fraudulently to click a link to a fake website. This can be done through many different channels, including emails, text messages and social media.

1. Use of sub-domains

The URL hierarchy always goes from right to left. If you are accessing **Yahoo Mail**, the correct link should be mail.yahoo.com – where Yahoo is the main domain, and Mail is the sub-domain.

A phisher may try to trick you with the fraudulent link yahoo.mail.com which will lead you to a page with a main domain of Mail and a sub-domain of Yahoo.



2. Hidden URLs

This is when a phisher hides the actual URL of a phishing website under plain text, such as "Click Here" or "Subscribe".

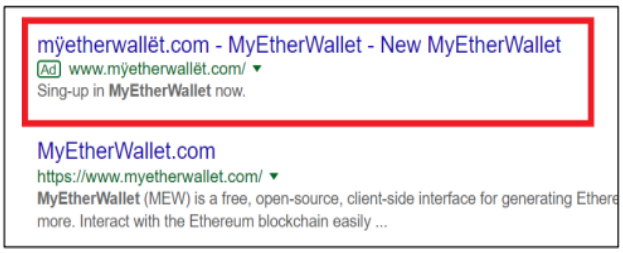
A more convincing scam could even display a legitimate URL that actually leads to an unexpected website.

3. Misspelled URLs

When a hacker buys domains with a variation in spellings of a popular domain, such as facebok.com, googlle.com, yahooo.com. This technique is also known as URL hijacking or typosquatting.

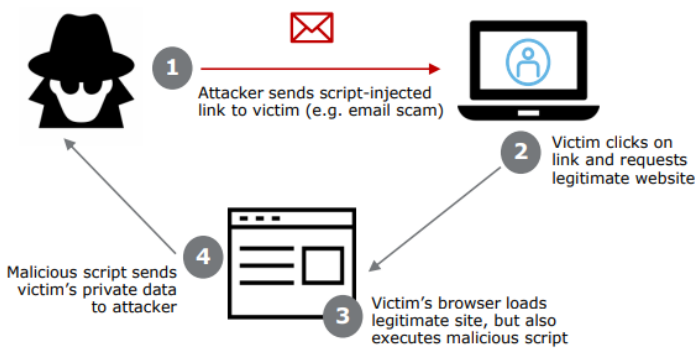
4. IDN homograph attacks

In this technique, a malicious individual misguides a user towards a link by taking advantage of similar looking characters.



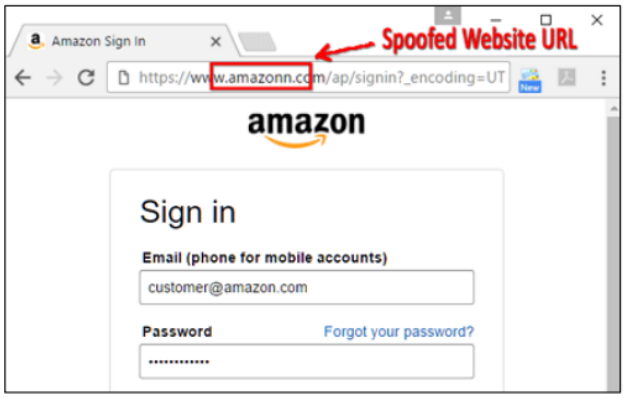
Cross-Site Scripting

This is when a hacker executes malicious script or payload into a legitimate web application or website through exploiting a vulnerability.



Website spoofing

This is done by creating a fake website that looks similar to a legitimate website that the user intends to access.



HOW TO IDENTIFY PHISHING WEBSITES?

IP Address

If an IP address is used as an alternative of the domain name in the URL, such as "http://125.98.3.123/fake.html", users can be sure that someone is trying to steal their personal information. Sometimes, the IP address is even transformed into hexadecimal code as shown in the following link "http://0x58.0xCC.0xCA.0x62/2/paypal.ca/index.html".

$$\underline{Rule}\text{: IF}\begin{cases}\text{If The Domain Part has an IP Address} \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$$

Long URL to Hide the Suspicious Part

Phishers can use long URL to hide the doubtful part in the address bar. For example:

http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd=_home&dispatch=11004d58f5b74f8dc1e7c2e8dd4105e811004d58f5b74f8dc1e7c2e8dd4105e8@phishing.website.html

$$\textit{Rule: IF}\begin{cases}URL\ length < 54 \rightarrow feature = \text{Legitimate}\\ else\ if\ URL\ length \geq 54\ and\ \leq 75 \rightarrow feature = Suspicious\\ otherwise \rightarrow feature = \text{Phishing}\end{cases}$$

Using URL Shortening Services "TinyURL"

URL shortening is a method on the "World Wide Web" in which a URL may be made considerably smaller in length and still lead to the required webpage. This is accomplished by means of an "HTTP Redirect" on a domain name that is short, which links to the webpage that has a long URL. For example, the URL "http://portal.hud.ac.uk/" can be shortened to "bit.ly/19DXSk4".

$$\underline{Rule}\text{: IF}\begin{cases}\text{TinyURL} \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$$

URL's having "@" Symbol

Using "@" symbol in the URL leads the browser to ignore everything preceding the "@" symbol and the real address often follows the "@" symbol.

$$\text{Rule: IF}\begin{cases}\text{Url Having @ Symbol} \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$$

Redirecting using "//"

The existence of "//" within the URL path means that the user will be redirected to another website. An example of such URL's is: "http://www.legitimate.com//http://www.phishing.com". We examin the location where the "//" appears. We find that if the URL starts with "HTTP", that means the "//" should appear in the sixth position. However, if the URL employs "HTTPS" then the "//" should appear in seventh position.

$$\text{Rule: IF}\begin{cases}\text{ThePosition of the Last Occurrence of "//" in the URL} > 7 \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$$

Adding Prefix or Suffix Separated by (-) to the Domain

The dash symbol is rarely used in legitimate URLs. Phishers tend to add prefixes or suffixes separated by (-) to the domain name so that users feel that they are dealing with a legitimate webpage. For example http://www.Confirme-paypal.com/.

$$\text{Rule: IF } \begin{cases} \text{Domain Name Part Includes } (-) \text{ Symbol } \rightarrow \text{ Phishing} \\ \text{Otherwise } \rightarrow \text{ Legitimate} \end{cases}$$

Sub Domain and Multi Sub Domains

Let us assume we have the following link: http://www.hud.ac.uk/students/. A domain name might include the country-code top-level domains (ccTLD), which in our example is "uk". The "ac" part is shorthand for "academic", the combined "ac.uk" is called a second-level domain (SLD) and "hud" is the actual name of the domain. To produce a rule for extracting this feature, we firstly have to omit the (www.) from the URL which is in fact a sub domain in itself. Then, we have to remove the (ccTLD) if it exists. Finally, we count the remaining dots. If the number of dots is greater than one, then the URL is classified as "Suspicious" since it has one sub domain. However, if the dots are greater than two, it is classified as "Phishing" since it will have multiple sub domains. Otherwise, if the URL has no sub domains, we will assign "Legitimate" to the feature.

$$\text{Rule: IF } \begin{cases} \text{Dots In Domain Part} = 1 \rightarrow \text{ Legitimate} \\ \text{Dots In Domain Part} = 2 \rightarrow \text{ Suspicious} \\ \text{Otherwise} \rightarrow \text{ Phishing} \end{cases}$$

Using Pop-up Window

It is unusual to find a legitimate website asking users to submit their personal information through a pop-up window. On the other hand, this feature has been used in some legitimate websites and its main goal is to warn users about fraudulent activities or broadcast a welcome announcement, though no personal information was asked to be filled in through these pop-up windows.

$$\text{Rule: IF } \begin{cases} \text{Popoup Window Contains Text Fields} \rightarrow \text{ Phishing} \\ \text{Otherwise} \rightarrow \text{ Legitimate} \end{cases}$$

Favicon

A favicon is a graphic image (icon) associated with a specific webpage. Many existing user agents such as graphical browsers and newsreaders show favicon as a visual reminder of the website identity in the address bar. If the favicon is loaded from a domain other than that shown in the address bar, then the webpage is likely to be considered a Phishing attempt.

$$\text{Rule: IF} \begin{cases} \text{Favicon Loaded From External Domain} \rightarrow \text{ Phishing} \\ \text{Otherwise} \rightarrow \text{ Legitimate} \end{cases}$$

The Existence of "HTTPS" Token in the Domain Part of the URL

The phishers may add the "HTTPS" token to the domain part of a URL in order to trick users. For example, http://https-www-paypal-it-webapps-mpp-home.soft-hair.com/.

$$\text{Rule: IF} \begin{cases} \text{Using HTTP Token in Domain Part of The URL} \rightarrow \text{ Phishing} \\ \text{Otherwise} \rightarrow \text{ Legitimate} \end{cases}$$

Understanding phishing techniques

How to spot phishing

1. Mismatched and misleading information

Pay attention to the domains/sub-domains, misspellings, and similar looking characters in URLs. To check for hidden URLs, hover your mouse cursor over a suspicious link to see the actual URL.

2. Use of urgent or threatening language

Be wary of phrases such as "urgent action required" or "your account will be terminated", as phishers often aim to instil panic and fear to trick you into providing confidential information.

3. Promises of attractive rewards

False offers of amazing deals or unbelievable prizes are commonly used to instil a sense of urgency to provide your confidential information. If it is too good to be true, it probably is.

4. Requests for confidential information

Most legitimate organisations would never ask for your personal information such as login credentials, credit card details and NRIC. When in doubt, contact the company directly to clarify.

5. Unexpected emails

If you receive an email regarding a purchase you did not make, do not open the attachments and links.

6. Suspicious attachments

Exercise caution and look out for suspicious attachment names and file types. Be extra wary of .exe files, and delete them immediately if they appear unexpectedly in your inbox.