Understanding phishing techniques

Mohamed Douss

Understanding phishing techniques

Overview

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

Costs of phishing – Financial loss

Phishing can lead to devastating **financial losses** for individuals as well as businesses.

For an individual, if a hacker manages to access sensitive bank account information, personal funds and investments are at risk of being stolen.

For businesses, financial losses can extend to regulatory fines and remediation costs. exemplified by the figures below:

$3.92M
average total cost of a data breach

90%
of data breaches are caused by phishing

76%
of businesses reported being a victim of a phishing attack

30%
of phishing messages get opened by targeted users

65%
increase in phishing attempts in the past year

$12B
losses caused by business email compromise scams

Understanding phishing techniques

Costs of phishing – Data loss and reputational damage

Phishing attacks often attempt to access more than just money from companies and individuals. Instead, they attempt to steal something much more valuable - data.

When phishing attacks successfully trigger data breaches, phishers can also cause damage individuals' reputation by:

- Using the victim's credentials for illegal activities or to blackmail the victim's contacts
- Publishing the victim's personal information to embarrass them
- Impersonating the victim to send out fake emails or malicious posts

For businesses, phishing can also lead to data breaches that will impact consumer trust.

Understanding phishing techniques

Types of phishing techniques

As phishing messages and techniques become increasingly sophisticated, despite growing awareness and safety measures taken, many organisations and individuals alike are still falling prey to this pervasive scam.

We will delve into the five key phishing techniques that are commonly employed:

1) Link manipulation
2) Smishing
3) Vishing
4) Website forgery
5) Pop-ups

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".

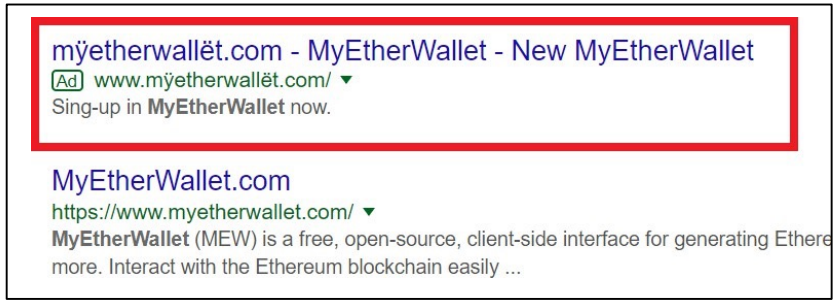
A more convincing scam could even display a legitimate URL that actually leads to an unexpected website.

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.



Understanding phishing techniques

Types of phishing techniques – Smishing

Smishing is a form of phishing where someone tries to trick a victim into giving their private information via a **text message**.

The most common form of smishing is a text with a link that automatically downloads malware. An installed piece of malware can steal personal data such as banking credentials, tracking locations, or phone numbers from contact lists to spread the virus in hopes to exponentially multiply.

Another smishing tactic is to pose as a legitimate and well-known institution to solicit personal information from victims. In some cases, scammers masquerade as tax authorities to get users' financial information and use that to steal their money.

Understanding phishing techniques

Types of phishing techniques – Vishing

Vishing is the **telephone** version of phishing, or a **voice scam**. Similar to email phishing and smishing, vishing is designed to trick victims into sharing personal information, such as PIN numbers, social security numbers, credit card security codes, passwords and other personal data.

Vishing calls often appear to be coming from an official source such as a bank or a government organisation. These vishers even create fake Caller ID profiles (called 'Caller ID spoofing') which makes the phone numbers seem legitimate.

Recently, vishers are even able to impersonate people through mimicking voices using artificial intelligence and trick victims into transferring money to them.

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 (US$243,000).

(Click to read more)

THE WALL STREET JOURNAL.

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

PHOTO: SIMON DAWSON/BLOOMBERG NEWS

Understanding phishing techniques

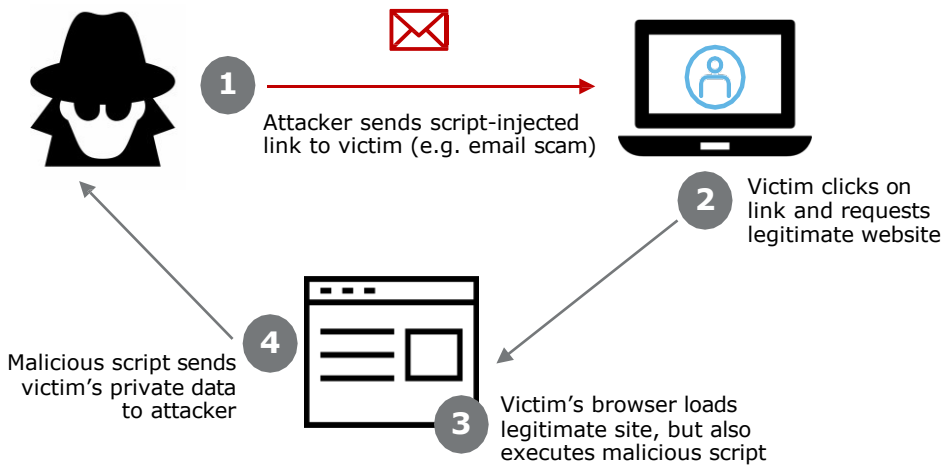
Types of phishing techniques – Website forgery

Website forgery works by making a malicious website impersonate an authentic one, so as to make the visitors give up their sensitive information such as account details, passwords, credit card numbers.

Web forgery is mainly carried out in two ways: **cross-site scripting** and **website spoofing**.

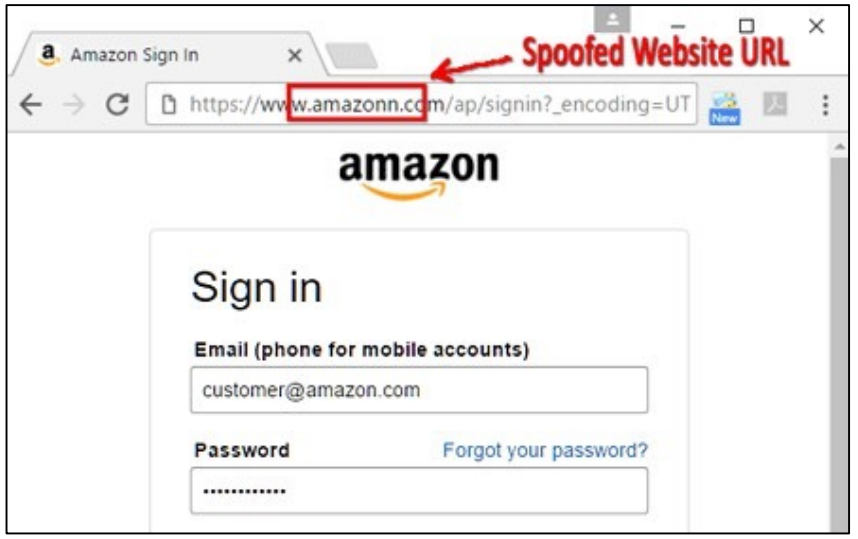
Cross-Site Scripting

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.



Understanding phishing techniques

Types of phishing techniques – Pop-ups

Pop-up messages, other than being intrusive, are one of the easiest techniques to conduct phishing scams.

They allow hackers to steal login details by sending users pop-up messages and eventually leading them to forged websites.

In-session phishing

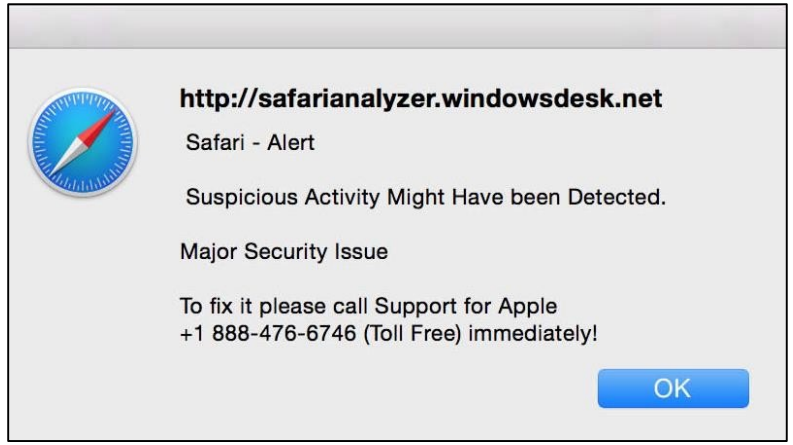
This variant of phishing works by displaying a pop-up window during an online banking session, asking the user to retype his username and password as the session has expired.

The user enters his details, not expecting the pop-up to be a fraud as they had already logged into the bank's website.

"Pop-up tech support"

Another widespread pop-up phishing scam is the "popup tech support."

When browsing the Internet, you will suddenly receive a pop-up message that your system is infected and you need to contact your vendor for technical support.



Understanding phishing techniques
Case studies

Ethereum Classic, 2017

Several people lost thousands of dollars in cryptocurrency after the Ethereum Classic website was hacked in 2017.

Using social engineering, hackers impersonated the owner of Classic Ether Wallet, gained access to the domain registry, and then redirected the domain to their own server where they extracted Ethereum cryptocurrency from victims.

Google Docs, 2017

In May, more than 3 million workers worldwide were forced to stop work when phishers sent out fraudulent email invitations on Google docs inviting recipients to edit documents.

When the recipients opened the invitations, they were taken to a third-party app, which enabled hackers to access individuals' Gmail accounts.

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.

Understanding phishing techniques

Protect yourself from phishing – General principles

Be cautious of all communications. Do not respond to phishing attempts – report them immediately.

Beware of pop-ups. Legitimate organisations do not ask for personal information via pop-up screens.

Do not click on phishing links. If an email looks suspicious, don't click any links in it and don't open its attachments.

Install a phishing filter. While it won't keep out all phishing messages, it will reduce the number of attempts.