Ways to Mitigate Phishing Attacks

Have you ever received a mail that tells you to click a link and put your information urgently? This could be a **phishing attack**. Phishing is basically a scheme used by most scammers to get your information through the internet.

This article discusses ways of mitigating phishing attacks. However, before we get to it, you need to know what phishing is all about. Phishing is the use of fraudulent email or electronic communication to get a person to perform an action. Continuous vigorous monitoring can be used to detect vulnerabilities in a system and protect systems from such attacks.

What Is Phishing?

Phishing is a type of social engineering attack in which a fraudulent message is sent to a target to trick the victim into handing over sensitive information or create an entry for installing viruses or ransomware.

Hackers can use different methods to carry out phishing attacks. They are known to most commonly use emails and **smishing (SMS**). There is also a new way for hackers to attack via phone call, which is called vishing, in which they use social media or “maladvertize” the use of digital advert software.

Types of Phishing Attacks

Email Phishing

In email phishing or **deceptive phishing**, the hacker/fraudster tries to impersonate a legitimate company or a person within a company to steal their victims' personal and financial information by making them click a link and enter a password. The goal is to get personal information and damage the victim's computer.

Spear Phishing

These are well-researched, highly targeted attacks that are aimed at government officials, corporate executives, and other wealthy targets. This is similar to deceptive email phishing, but much more targeted.

In this type of phishing, the scammer has already gathered some information about you, such as your name, job title, company, and phone number. They use the information to respond to questions like, "We already know this about you. Confirm to add this data to an existing data set."

Whaling

Whaling attacks are more targeted than spear phishing. The target aims at the CEO/CFO and other executives. They are professionally designed based on a solid understanding of the business language and tone.

These emails are believable as they seem to come from trusted suppliers/partners. Thus, hackers can obtain confidential information by tricking victims to click a link or download an attachment, send out employee information, and also transfer funds.

Angler phishing

This is also called social media phishing. The hacker sends out emails that appear to come from social media or post a message on your social media with a link/attachment. They also pretend to be a customer service agent to lure victims into handing over confidential information.

Smishing

This refers to phishing that uses an SMS (e.g. text message) to deliver malicious short links to smartphones. Users often disguise them as account notices, price notifications, and political messages.

Vishing

This type of attack uses voice calls. It involves a scammer making a malicious call, claiming to be from the banking sector. They use sophisticated scare tactics and emotional manipulation to cause employees to surrender sensitive information.

Pharming

Pharming targets your server and also focuses on providing fake websites that resemble the original website as much as possible. In pharming, attackers redirect website traffic to fake websites controlled by them to collect sensitive information or install malware. The scammers create look-alike e-commerce and digital banking websites to collect your credentials.

Attackers manipulate information on your machine or compromise the DNS servers by re-routing the target from its intended IP address to the one controlled by the hacker. This is usually done by compromising the

victims' machine and changing the configuration files on the device, which redirects the user the next time they try to access the site.

10 Ways to Mitigate Phishing Attacks

Now that we know what phishing is all about, let's see how to avoid/control phishing attacks.

First, when you are on the internet, **avoid pop-ups** and do not click on links immediately. Always hover your mouse pointer over links to see if the destination is the correct one.

Next, keep **your browser and apps up to date**. This is because they contain patches and new features provided by the manufacturer, which, when installed, upgrade your security and prevent your PC from being breached by cyber attackers.

Do not give your information to an unsecured site. One has to be sure of the type of site being clicked. Always check and confirm that whatever link you click on contain HTTPS or has a padlock at the beginning of URL, as this shows that the link is secured.

Use a browser that enables you to use **anti-phishing add-ons** as this will detect and alert you about a phishing site. Additionally, **do not sign up and put your email on sites or forms** when you do not have to. Most spam and junk received results from people signing up to websites.

Always be aware of the content of the email that is sent to you. Never press or click on suspicious links. And finally, always check to make sure that the site is verified by checking the actual email address sent to you, not just its display name.

Phishers sometimes use scare tactics. They usually work by threatening to suspend some service until you update information. Always be on alert not to give important information. Most users have to apply common sense to defend themselves from these scammers

Adapted from: https://cybersecuritynews.com/ways-to-mitigate-phishing-attacks-a-detailed-guide/