What is Phishing?

In phishing, individuals are contacted by email, phone, or text message by someone posing as a legitimate institution in order to entice them to disclose sensitive data, such as passwords and banking information.

After the information is obtained, it is used to access important accounts, leading to identity theft and financial loss.

Typical Phishing Features

In order to protect yourself from phishing scams, you should look for a few common features. In spite of the fact that there are several types of phishing, these are some of the most commonly used tactics of scammers.

Too Good- An offer that is too good to be true and eye-catching or attention-grabbing is designed to catch people's attention immediately. The claims may include winning an iPhone, a lottery, or some other lavish reward. Keep an eye out for suspicious emails and don't click on them. Don't believe everything you hear! If it sounds too good to be true, it probably is!

Sense of Urgency- Cybercriminals love to tell you that super deals are only available for a limited time, which creates a sense of urgency. Some of them will even tell you that you have only a few minutes to respond. These types of emails are best ignored. Occasionally, you will be notified that your account will be suspended unless you update your personal information immediately. Generally, trustworthy organizations give patrons ample time to update their personal information before terminating their accounts. If in doubt, visit the source directly rather than clicking a link in an email.

Hyperlinks - A link may not be what it seems. Hovering over a link reveals the URL you'll be directed to when you click it. Perhaps the website is completely different or is a popular one with a misspelling, for example, www.bankofarnerica.com - note the 'r' and 'n'.

Attachments - Do not open email attachments you did not expect or that seem suspicious! It is common for them to contain payloads like ransomware or viruses.

Prevent Phishing Attacks

It is important to keep your organization and yourself protected, even though hackers come up with new techniques constantly. You can apply these tips to a number of situations to help you prevent phishing.

Spam filters are a useful tool for preventing spam emails. To determine if a message is spam, filters evaluate the message's origin, its software, and its appearance. There are times when spam filters block legitimate emails, so they are not always 100% accurate.

If there is a link in an email, hover over the URL first. Secure websites with a valid Secure Socket Layer (SSL) certificate begin with “HTTPS”.

Keep your software and operating system up to date. Windows OS products are often targets of phishing and other malicious attacks, so be sure you are secure and up to date. Especially for those still running anything older than Windows 10.

Safety conscious individuals should use 2FA. Given how easily password and username combinations can be stolen by hackers, it's no wonder that breaches happen regularly. And when they do, two-factor authentication is one of the best ways to protect your sensitive data from theft. Two-Factor Authentication (2FA) works by adding an additional layer of security to your online accounts. It requires an additional login credential – beyond just the username and password – to gain account access, and getting that second credential requires access to something that belongs to you.