Be Aware, Stay Aware

Expand all   Collapse all

Overview

The section defines what phishing is and information on how to protect your accounts.

Email & Phishing

Email is a powerful way to communicate, but it also is one of the most common attack methods used by cyber attackers today. Use common sense. If an email seems odd, suspicious or too good to be true, it is most likely an attack.

Email is one of the primary ways we communicate. We not only use it every day for work, but we use it to stay in touch with our friends and family. In addition, email is how most organizations provide the products or services we depend on, such as confirmation of an online purchase or the availability of your online bank statements. Since so many people around the world depend on email, email attacks (commonly called phishing) have become one of the primary attack methods used by cyber attackers. In this newsletter, we explain what phishing is and the steps you can take to protect yourself.

Phishing was a term originally used to describe email attacks that were designed to steal your online banking username and password. However, the term has evolved and now refers to almost any email-based attack. Phishing uses social engineering, a technique where cyber attackers attempt to fool you into taking an action. These attacks begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store. Their goal is to trick you into taking an action, such as clicking on a malicious link, opening an infected attachment or responding to a scam. Cyber criminals craft these emails to look convincing, sending them out to literally millions of people around the world. These attackers do not have a specific target in mind, nor do they know exactly who will fall victim. They simply know the more emails they send out, the more people they may be able to fool.

Protecting Yourself

In most cases, simply opening an email or reading a message is safe. You have to do something after reading the message for most phishing attacks to work, such as opening the attachment or clicking on a link. To protect yourself, keep the following in mind:

- Just because a message appears to come from a friend or someone you know does not mean the message is safe. Cyber attackers may have infected their computer, hacked their account or spoofed their “From” address. If you are suspicious about a message from someone you know, call the person to verify if he or she really sent it.
- Be suspicious of messages that claim to be from an official organization but have grammar or spelling mistakes. Most organizations have professional writers and do not make these mistakes.
- Before you click on a link, hover your mouse cursor over it. This will display the true destination of where it will take you. Confirm that the destination displayed matches the destination in the email and make sure it is going to the organization’s legitimate website. Even better, type the proper website address into your browser. For example, if you get an email from your bank asking you to update your bank account, type your bank’s website into your browser, then log into the website directly. On a mobile device? No problem. Simply hold your finger down on the link and you should see the true destination appear in a pop-up window.
- Be careful with attachments and only open those you were expecting. Many of the infected attachments sent today can bypass most anti-virus programs.
- Remember that sometimes you are the greatest risk to your email. Always double check that you are emailing the correct person before sending one, especially when sending something sensitive. For example, with email features like autocomplete, you may try to email someone in finance, but accidentally end up emailing an old friend.
- Be skeptical of any message that requires “immediate action,” creates a sense of urgency or threatens to shut down your account.
- Be suspicious of any email directed to “Dear Customer” or some other generic salutation.

Using email safely is ultimately about common sense. If a message sounds suspicious or too good to be true, it is most likely an attack. Simply delete the message. If you get a message and you are not sure if it is an attack, contact your help desk or information security team.

Spear Phishing

The attacks we have discussed so far are generic emails designed to attack as many people as possible. However, attackers have developed an even more dangerous email attack called Spear Phishing. Instead of sending out millions of emails to random people, this attack targets only a few people within our organization.

These targeted attacks are more dangerous because of the extensive research the attackers do. They begin by analyzing who works in our organization, then target specific employees (such as you) and collect as much information as possible through sites such as LinkedIn or Facebook. Once they have learned as much as possible about you, they create a highly customized phishing email designed to fool you into clicking on an infected attachment or malicious link.+

This newsletter is published by Tennessee Tech University Office of Information Security.

For more information, please contact us at: 931-372-3913, 931-372-6859, or by email at ocisо@tntech.edu.

How helpful was this information?

Your Rating: ☆☆☆☆☆ Results: ★★★⯪☆ 113 rates