USE EMAIL SAFELY

The Problem

Email is one of the primary ways we communicate. We not only use it every day for work, but to also stay in touch with our friends and family. In addition, email is how many companies provide the products or services we depend on, such as confirmation of an online purchase or availability of your online bank statements. Since so many people around the world depend on email, email attacks (also called phishing) have become one of the primary attack methods used by cyber criminals. 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. The criminals 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.

Using Email Safely

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

This newsletter is published by
the IT Security Advisory Team.
For more information, please visit
http://www.utc.edu/itsecurity

THE UNIVERSITY of TENNESSEE UT CHATTANOOGA

Protecting Yourself

In most cases, simply opening an email or reading a message is safe. For most attacks to work you have to do something after reading the message, such as opening the attachment, clicking on the link or responding to the request for information. 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 criminals 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 it was truly them that sent it.
- Be suspicious of any email directed to “Dear Customer” or some other generic salutation.
- Be skeptical of any message that requires “immediate action,” creates a sense of urgency or threatens to shut down your account.
- 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 over it. This will display the true destination of where you would go. Confirm that the destination displayed matches the destination in the email and that it is going to the organization’s legitimate website. Typing the website into your browser is even better. For example, if you get an email from your bank asking you to update your bank account, do not click on the link. Instead, type your bank’s website in your browser, then log into the website directly.
- Be careful with attachments and only open those you were expecting. Cyber criminals can send you infected attachments that can potentially bypass your anti-virus.

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 a specific organization.

The reason these targeted attacks are more dangerous is 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, they create a highly customized phishing email designed to fool you into clicking on an infected attachment or malicious link.