Email Security

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 cybercriminal 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.

In most cases, simply opening an email 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 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 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.

- 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 accidently end up emailing an old friend. 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.

SANS Securing the Human

Email Security

“If you spend more on coffee than on IT security, you will be hacked. What’s more, you deserve to be hacked.”

— Richard Clarke

From the ISO’s Desk

For December, our Awareness topic is Email Safety. Statistically speaking, many of the more recently publicized major information breaches such as Target, Sony, and Home Depot were initiated by an internal employee or a contractor that responded to a phishing email. Careful scrutiny of an email that comes from nowhere is an important step in keeping from having yours or Loyola’s information stolen or leaked. When we get junk mail in our postal mailbox, we can generally easily tell by looking that each item whether it is junk or not. Sometimes we don’t even waste our time opening the envelope. We should all educate ourselves in the same way when it comes to electronic mail. If you would like to know more about our awareness activities, please check out Inside Loyola or go to our web page: http://www.luc.edu/uiso

Jim Pardonek
Information Security Officer
Spear 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.

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.

Soft Phishing

Our December topic is “Email & Messaging”, which will be live on December 1st.

Please visit: http://www.luc.edu/uiso/awareness/loyola_aware.shtml for further instruction.

If you have any questions in regarding to Loyola Aware, please contact the data security team by email (datasecurity@luc.edu) or call x87373 (703-508-7373)