ISSUE: 12-2 YEAR: 2015

University Information Security Office Newsletter

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.

— Richard Clarke

LOYOLA UNIVERSITY CHICAGO

Email Security

SANS Securing the Human

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 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 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.
- 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 Email address into your browser. 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 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.

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's 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

Loyola Email Policy

Created by Grace Meng

Electronic mail (e-mail) has become a ubiquitous service greatly enhancing communication both internally within the Loyola community and externally to Users, including prospective students, alumni, and the public at large. The purpose of this policy is to describe the appropriate use of University E-mail Facilities, associated responsibilities, and rights of all Users of University E-mail Facilities and Official University E-mail Accounts.

Permissible Uses of Electronic Mail

Loyola provides electronic and voice mail to its faculty, students, and staff for educational, research, health care, and internal business purposes. Members of the Loyola community should limit their use to these purposes. Persons outside the Loyola community may be given access to Loyola electronic and voice mail on a case-by-case basis by special authorization from Information Technologies and under certain conditions, including adherence to this and other applicable policies.

Confidentiality of Electronic Mail

Loyola cannot guarantee the confidentiality or privacy of electronic mail messages and makes no promises regarding their security. Decisions as to what information to include in such messages should be made with this in mind.

Limitation on Disclosure

Any third-party disclosure of the contents of electronic mail obtained according to this policy will be limited unless such disclosure is required to protect the integrity of Loyola's systems or to comply with a legal obligation.

Violations

The use of electronic mail services is a privilege offered to Loyola faculty, staff, and students. Loyola University Chicago reserves the right to revoke this privilege for violations of this policy.

For the complete version of E-Mail-Voice Mail Use Policy please visit: http://www.luc.edu/its/itspoliciesguidelines/policy_email_voicemail.shtml

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.

Loyola Aware

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 regrading to Loyola Aware, please contact the data security team by email (datasecurity@luc.edu) or call x87373 (703-508-7373)

Contact Information

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM
Some Material © SANS Institute 2015