ISSUE: 11-1 YEAR: 2015

University Information Security Office Newsletter

All this modern technology just makes people try to do everything at once.

-Bill Watterson

Social Engineering

SANS Securing the Human

Cyber attackers have learned that the easiest way to take control of your computer or steal your information is to simply ask. Use common sense. If a person or a message seems suspicious or too good to be true, it may be an attack. One of the main techniques cyber attackers use to compromise your computers and steal your information is called social engineering, also known as the art of human manipulation. This is when attackers pretend to be someone or something you know or trust, such as your bank, a government organization or even a friend or coworker. They then leverage that trust to get what they want, often by simply asking for it. Let's take a look at several examples of real social engineering attacks.

Email —You receive an email from a shipping company saying that they tried to deliver a package to you but had the wrong address. The email looks official; it has professional-looking graphic designs and a real company logo. The email informs you that if you do not respond in the next 24 hours, your package will be returned to sender. It then provides you with a link to click on or an email attachment to fill out so you can receive your package. The problem is this is an attack. A cyber criminal has created an email that looks just like a real shipping company; however, the email is designed to fool you. If you click on the link, you will be taken to a website that the attacker controls. Once your browser connects to the attacker's website, it attempts to silently hack into your browser. If you were to open the attachment, it would silently infect your computer. Be suspicious of any unexpected emails that urge you to click on links or open attachments.

Tech Support Scam —You receive a phone call from someone claiming to be from a computer support company. They believe your computer is infected and have been tasked with investigating the issue and helping you secure your computer. They then ask you if there are specific files on your computer and tell you how to find them. When you locate the files on your computer, the caller confirms your computer is infected. This is really all a lie and your computer is not infected. These files are standard files that every computer has. Once they have you fooled into believing your computer is infected, they will then pressure you into buying their security software. However, this software is really a virus that gives them total control of your computer. In the end, not only has the caller tricked you into infecting your computer for them, but you just paid them to do it.

Social Media —Your friend posts on her Facebook page that she is on vacation in London and has just been mugged. She needs someone to send her money right away so she can get back home. However, this is a lie. Your friend has not been mugged. In fact, she is not even in London. Instead, a cyber attacker has hacked into and taken over her Facebook account, then posted this fake message in an attempt to scam money from her friends. In this case, the best way to protect yourself would be to call your friend on the phone and confirm if she really does need help. Remember, social engineering is nothing more than an attacker building trust with you, then abusing that trust to get what they want. If you get an email, message or phone call that seems odd, suspicious or too good to be true, it may be an attack. Common indicators of a social engineering attack include people asking for information they should not have access to, using a lot of confusing or technical terms or creating a sense of urgency. If you believe someone is attempting to trick or fool you, simply hang up the phone or ignore the email and immediately contact the help desk or information security team.

You Won the Lottery — You receive a text message on your smartphone announcing you have won the lottery. To collect your winnings, you must call the number in the message and provide them your banking information. When you call the phone number, a person explains that you must pay a transaction fee or taxes before you receive your lottery winnings. Once you provide them your financial information and pay the required fees, the cyber criminals disappear with your money and information, never to be seen again. The simplest way to protect yourself against these types of attacks is to be suspicious of any message that sounds too good to be true. In this case, how could you win a lottery that you never even entered or heard of before?

From the ISO's Desk

Our November Awareness topic is based on Social Engineering. These are common techniques that are used by hackers to trick an individual into providing information that may allow them access to other systems so that they can steal corporate secrets. Please see page 2 for instructions on how to access the Social Engineering awareness module. 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

How to access Loyola Aware

Loyola Aware is Loyola's new information security awareness program designed for all faculty and staff. The purpose of the program is to increase employees security awareness by providing short video snippets that bring to light specific topics in information security. By increasing awareness, the program allows everyone to recognize IT Security concerns and respond accordingly.

Starting in October, ITS began releasing a series of awareness training modules, distributed by the University Information Security Office. Our October topic was "You are the target". The November module "Social Engineering" will be available starting November 2nd. Each module contains a brief video followed by five assessment questions. The idea is to reinforce the video content by asking questions about the content. All prior month's topics are also available.

Loyola Aware can be accessed using these steps:

1) Log into your Sakai account with your UVID and password: https://sakai.luc.edu/

2) All current LUC employees are already enrolled in Loyola Aware. If the course does not appear at the top of the page, please contact the UISO via email at DataSecurity@luc.edu.

3) There should be three tabs on the left side of the page: Home, Lessons and Gradebook.

4) To access the training, you can either click the "Click Here" hyperlink on the "Home" page, or you can click on the "Lessons" tab.

5) Once in the lessons tab, it is recommended that you watch the monthly video followed by completing the associated assessment.

6) Assessments are available for unlimited attempts. Users can click on the Gradebook to check their scores and get immediate feedback.

Social Engineering Security

Created by Yuan Liu

Facebook, YouTube, Twitter and LinkedIn are famous common social media applications. We should be careful when we use them for personal or company information. Here are some quick tips on having a safer social media experience.

Please use a secure connection where possible. Regular web (http) traffic is plain text and anyone between your computer and the institution could theoretically read it. The secure (https) traffic is encrypted and only you and the institution can read it.

Limit your contact information on your social networks to friends/ followers. Any information you post publicly on the web can be used against you in online or identity attacks. Therefore setting the privacy as "Only me" or "Friends" is better than "Public".

Facebook, Twitter, and Pinterest allow search engines like Google crawl allow user profiles to be displayed in searches. Turning off this feature further hides you from the public web.

Public searching controls whether people who enter your name in a search engine will see a preview of your Facebook timeline, or Twitter feed. It is always a good idea to turn off the public searching feature of any social media account that you might be using. Because some search engines cache information, some of your timeline information may be available for a period of time after you turn public search off.

Don't Become a Victim

Keep an eye out. Social engineering and this kind of "soft" hacking isn't particularly new, but it's rising in popularity among even untrained and unsophisticated hackers, mostly because it's easy to do, can net a ton of information, and, of course, the human systems set up around our technology are almost always the weakest link in the security chain. A little attention to detail and vigilance goes a long way.

Contact Information

University Information Security Office

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