ISSUE: 10-9 YEAR: 2015

University Information Security Office Newsletter

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

-Bill Watterson

From the ISO's Desk

October is National Cyber Security Awareness Month (NCSAM), conducted every October since 2004, this national public awareness campaign is intended to encourage everyone to protect their computers and our nation's critical cyber infrastructure. Cyber security requires vigilance 365 days per year. However, the Department of Homeland Security (DHS), the National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the primary drivers of NCSAM, coordinate to shed a brighter light on what home users, schools, businesses and governments need to do in order to protect their computers, and data. This year, the LUC Information Security Staff will be launching a new awareness video series, Loyola Aware. Each month we will release a new video generally 4 minutes in length on a different topic. This month's topic is "You Are The Target" Please see page 2 for instructions on how to access the modules. If you would like to know more about our NCSAM activities, please check out Inside Loyola or go to our web page https://www.luc.edu/uiso

Jim Pardonek
Information Security Officer

University Information Security Office

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

Introducing Loyola Aware

Created by Cai Wang

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. Beginning in this month, ITS will release a series of training modules, distributed by the University Information Security Office, that can be accessed via Sakai. 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. The training modules contain a variety of topics which include: social engineering, email & messaging, browsing and many others.

To Access Loyola Aware

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

2) All current LUC employees should already be enrolled in Loyola Aware. If the course does not appear at the top of the page, please click on "More Sites" to check. If you believe you are not enrolled in Loyola Aware, please email 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 first, watch the monthly video and second complete the associated assessment.

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

For additional question or assistance, please contact the University Information Security Office: DataSecurity@luc.edu

You Are the Target

SANS Securing the Human

Many people mistakenly believe that their computer or information has no value and cyber attackers would never target them. In reality, individuals like you are a target. You and your computer are under attack almost every day. The first step to protecting yourself is realizing you are a target.

Many people mistakenly believe that cyber attackers only target our databases or web servers. In reality, they also target individuals like you. While these attackers use a variety of sophisticated tools, they have learned that the simplest way to hack into an organization like ours is to target people like you. Let's take a look at how a group of cyber attackers might hack into our organization.

While the following story did not happen, it illustrates common methods used to hack into an organization like ours. Several months ago, a team of cyber attackers decided to target our organization. We are not sure what their motivation was. Perhaps they wanted to steal our sensitive information, make a political statement or gain access to one of our partners. All we know is that they began searching our website several weeks ago, learning everything they could about us. This included who we are, how we operate and the identities of our employees and staff. They then began to harvest employees' personal information from websites such as Facebook, YouTube, LinkedIn, Instagram and public forums.

You are the Target—Cont.

Unfortunately, several employees had posted too much information about themselves and our organization. As a result, the attackers were able to build a complete picture of our organization and learn details about key members of our staff. Armed with this information, they launched their attack. Seven employees at our organization received emails that appeared to come from a package delivery service we commonly use. While these emails appeared to be legitimate, they were actually phishing emails created by the attackers. Each message contained an infected email attachment designed to bypass our anti-virus software and silently infect our computers.

Unfortunately, two of the targeted employees fell victim to the phishing emails by opening the attachments. Since their computers were not patched, they were quickly infected, giving the cyber attackers complete control. The attackers then installed keylogging software on the computers, enabling them to capture all of the employees' keystrokes.

On one of the hacked computers, an employee was using a login and password they had shared with their coworkers. The attackers quickly harvested this information and were able to log into other systems throughout our organization. Because the attackers were using stolen, legitimate passwords, our security team did not detect them.

Over the next seven days, the attackers scanned the hard drives of numerous compromised systems, stealing every document, spreadsheet and presentation they could find. They soon transferred over 150 Gigabytes of confidential information out of our organization, including a key project we had been working on for over three months. Fortunately, an alert employee noticed several suspicious programs running on their computer and reported it. As a result, the attackers were finally detected and blocked from causing any more harm.

While this story is only an example, it demonstrates why we have security policies and controls. They are carefully designed to protect you and our organization, while also ensuring that we are compliant with important standards and regulations. This is why it is so important that you understand and follow our security policies. You may not realize it, but you are also under attack when you and your family connect to the Internet at home. To help protect yourself, your family and our organization, always remember some core principles:

• Always be cautious and assume you are a target. You may not think you or your information has value, but it does.

• Attacks are a constant threat on the Internet. If something seems suspicious or too good to be true, it most likely is.

Help Us Celebrate Cyber Security Awareness Month by Attending One of Our Awareness Events

Security and Donuts Sessions

- Thursday October 8, 9:00AM-10:00AM LSC Damen 214
- Thursday October 15, 9:00AM-10:00AM WTC Corboy 602
- Tuesday October 20, 9:00AM-10:00AM LSC Damen 214

Host Firewalling

Created by Chris Campbell

While several anti-virus vendors have developed firewalls that are integrated into their products, most major operating systems come with firewall capabilities that are more than sufficient. A host firewall is a piece of software running on your computer that dictates what programs and services are allowed to communicate with your computer on a network. Firewalls are operated on the principle of least access, which means that only connections that are necessary for that particular device will be allowed. This helps prevent potentially vulnerable services on your device from being targeted by remote attackers.

Windows

Windows machines handle the majority of firewall functionality for you. If you have seen a pop-up window after installing a new application that asks which networks it should be allowed to communicate on, you have configured your Windows firewall. Check "Control Panel\All Control Panel Items\Windows Firewall" for a useful summary of your current protection.

Items to look for under both Private and Guest or Public networks include "Windows Firewall state" set to On, and "Incoming connections" displaying the following: "Block all connections to apps that are not on the list of allowed apps".

Mac

Mac OS X has a powerful firewall capability as well, which is unfortunately disabled by default. Turn on your Mac's firewall by navigating to "System Preferences > Security & Privacy > Firewall" and click "Turn On Firewall". Next, select "Firewall Options" and add any applications that you need to be available over the network (such as Remote Desktop, if you use it).

If you do not have any need for incoming connections (such as remote access or file sharing), I recommend checking the box next to "Block all incoming connections". This will lock your Mac down to the fullest extent possible, and prevent the vast majority of network-based attacks.