ISSUE: 2-3 YEAR: 2016

University Information Security Office Newsletter

"A password is like a toothbrush. Make sure you choose a good one, never share it with anyone, and change it occasionally."
— Unknown

Mobile Device Security

SANS Securing the Human

Mobile devices, such as smartphones and tablets, have become incredibly powerful. Not only can you call anyone in the world, but you can also watch movies, read your email, bank online and even install apps. These combinations of factors make mobile devices very useful; however, they also can put you at great risk. To protect yourself, we recommend the following:

- Just like with your computer, install only apps that you need and make sure that you download them from trusted sources. Criminals can create apps that look real, but are actually malicious programs designed to quietly take control of your devices. In addition, do not install apps that request excessive permissions, such as the ability to silently send text messages or copy your address book.
- Just like with your computer, backup your mobile device on a regular basis. This way, if something happens to the device, your information is not lost.
- Make sure you update your mobile device and apps on a regular basis. Cyber attackers can more easily exploit your devices if you are running outdated software. If your mobile device is old and no longer supported, consider purchasing a new one that can support the latest version of the operating system and security updates.
- Never jailbreak or hack your own mobile device. Not only may your device no longer be supported, but this usually cripples or disables many of the security features designed to protect you and your information.
- If you have security software installed, such as anti-virus or a firewall, then make sure they are enabled and updated with the latest version.
- Remember that many of the attacks you find in email can also happen via texting on your mobile device. For example, cyber criminals can text you messages asking you to connect to malicious websites, download infected apps or ask you for private information, such as your bank account. If a text message seems suspicious or too good to be true, simply delete it.
- Be careful when using Wi-Fi. Many mobile devices will automatically connect to Wi-Fi networks without asking you, putting your device at risk. Disable Wi-Fi if you are not using it.
- Attackers can also take advantage of your Bluetooth capabilities. Just like Wi-Fi, disable Bluetooth when you are not using it. It is also important to turn off Bluetooth discoverable mode features.
- Do not access or store work email or other data from our organization on your mobile device unless you have been authorized to do so and the appropriate security safeguards are in place. Finally, when you lose a mobile device, anyone can access all of your information, including your emails, pictures or contact lists, unless it is protected.
- Protect your devices with a hard-to-guess password or PIN. If your device supports encryption, we recommend you use it. Also, consider enabling remote wiping if it's available. This means that if your mobile device is lost or stolen, you can erase all of your information remotely.
- If you lose a device issued to you by our organization or a device that contained any organizational information, notify the help desk or information security team immediately.

From the ISO's Desk

Our February Awareness topic is Mobile Device Security. Mobile devices, such as your smartphone and tablet, have become some of the most powerful means of communicating. In many ways, they have replaced computers. By following the steps in this newsletter as well and watching the video in Loyola Aware, you can be well on your way to making sure that the device that you expose the most to public threats is as safe and secure as possible.

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

Safe Computing to you all!

Jim Pardonek, Loyola's Information Security Officer

Does iPhone Malware Exist?

Although iPhone apps are some of the safest around, during the last part of 2015 the Apple app store contained several applications that contained embedded malware. This malware was named XcodeGhost.

What's XcodeGhost?
XcodeGhost is the malicious version of Xcode; Apple's official tool for developing apps for IOS and OS X. The tool was used by a handful of iOS developers to develop games and other applications that were then uploaded into the app store. iOS apps infected with the malware are capable of collecting information on devices, such as the current time, an infected app's name, the current device's name and type, the current system's language and country, and the current device's user information.

Which apps and devices are affected?
There were more than 50 iOS apps were infected. Some of the more popular apps included WeChat, NetEast Cloud Music, Tailway 12306, and Angry Birds. However, there is no complete list of the infected applications. Apple has identified these applications and has replaced them with fixed versions or is removing them from the App Store until the issue is resolved.

What can the University Information Security Office do to help?
One of our services has the ability to detect traffic from your iPhone and determine if any applications contain XcodeGhost. Although we cannot determine the exact app that is infected, if the UISO receives notifications from our monitoring service, we will reach out to the user and bring it to their attention.

If you get a notice from the Information Security Office;

- Step 1: Check your device for any infected applications that were listed on the notification's attachment.
- Step 2: Delete infected applications and re-download them from the App Store

If you are not able to determine which app is infected, feel free to send us a list of the apps installed on your device. We will do our best to determine which apps have been affected.

If you have additional questions or concerns in regarding to iOS Malware XcodeGhost, please email us at datasecurity@luc.edu

Disposing Your Devices

New mobile devices with must-have features are coming out every month. As a result, many people replace their smartphones or tablets almost every year. However, what happens to your old device when you dispose of it? More importantly, what happens to all of your private information? After using your devices every day for so long, it has accumulated an amazing amount of very private data. Before you dispose of any mobile device, ensure that you wipe all information on it. Most mobile devices now have a reset feature that wipes all the data from your mobile device. Be sure to use these built-in features to wipe your device. In addition, be sure to remove the SIM and any flash cards from the device before disposing of it. If your mobile device was issued to you by our organization, make sure you contact the help desk or information security team so they can tell you how to dispose of it.

Loyola Aware

Our Feburary awareness topic is " Mobile Device Security", which will be live on February 8th.

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

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