UTHSC G.U.A.R.D.

Summer 2018

IN THIS ISSUE

Vacation Getaway!!! – with Cyber Security

by Chris Madeksho, Information Security Coordinator

When traveling, people tend to get out of their security norms. What you might never do at home becomes something that is OK at a resort or airport. Stay cyber security aware during planning and traveling will protect you and your devices. Here are some tips.

Preparing for your trip:

- **Password protect:** Use a passcode or security feature like a finger swipe pattern or fingerprint to lock your mobile device. Also set your screen to lock after a short period of time by default.
- **Think before you use that app:** While new apps are tempting, it is important to always download new apps from only trusted sources.

While traveling:

- **Public Wi-Fi:** Do not transmit personal info or make purchases on unsecure or public networks. For laptops/tablets, it is easy to use your phone as a personal hotspot to surf more securely using carrier data. Also, never use a public computer or device to shop, log in to accounts, or do anything personal.
- **Turn off Wi-Fi and Bluetooth when idle:** Only enable Wi-Fi and Bluetooth when required, and disable your Wi-Fi auto-connect features.
- **Be careful what you post:** Think twice before posting pictures that signal you are out of town. Knowing you are away from home is a great piece of information for a criminal to have and they may target your home for physical crime.
- **Keep an eye on your devices:** Laptops, smartphones, and tablets are all portable and convenient, making them perfect for a thief to carry away! It is more likely that you device will get lost than stolen. Also load a reputable app that will locate your device if lost or stolen.
- **Know your destination's laws:** If you are heading out of the country, check up on any specific laws on internet and device usage.

For more information, contact the UTHSC Information Security Team at (901) 448-1880 or itsecurity@uthsc.edu.

Traveling?

Read some tips on how to stay cyber secure during vacations.

Phone Call Scams

Social Engineering doesn't come just from email. Phone call scams are on the rise.

Phone Call Attacks & Scams

by Jen Fox, Guest Editor, SANS OUCH! Newsletter

When you think of cyber criminals, you probably think of an evil mastermind sitting behind a computer launching sophisticated attacks over the Internet. While many of today's cyber criminals do use technologies like email or instant messaging, bad guys are also using the phone to trick their victims. There are two big advantages to using a phone. First, unlike email, there are fewer security technologies that monitor phone calls and can detect and stop an attack. Second, it is much easier for bad guys to convey emotion over the phone, which makes it more likely they can trick their victims. Let's learn how to spot and stop these attacks.

How do Phone Call Attacks Work?

First, you have to understand what these attackers are after. They usually want your money, information, or access to your computer (or all three). They do this by tricking you into doing what they want. The bad guys call people around the world, creating situations that seem very urgent. They want to get you off-balance by scaring you so you won't think clearly, and then rush you into making a mistake. Some of the most common examples include:

- The caller pretends that they are from a government tax department or a tax collection service and that you have unpaid taxes. They explain that if you don't pay your taxes right away you will go to jail. They then pressure you to pay your taxes with your credit card over the phone. This is a scam. Many tax departments, including the IRS, never call or email people. All official tax notifications are sent by regular mail.
- The caller pretends they are Microsoft Tech Support and explain that your computer is infected. Once they convince you that you are infected, they pressure you into buying their software or giving them remote access to your computer. Microsoft will not call you at home.
- You get an automated voicemail message that your bank account has been canceled, and that you have to call a number to reactivate it. When you call, you get an automated system that asks you to confirm your identity and asks you all sorts of private questions. This is really not your bank, they are simply recording all your information for identity fraud.

Protecting Yourself

The greatest defense you have against phone call attacks is yourself. Keep these things in mind:

- Anytime anyone calls you and creates a tremendous sense of urgency, pressuring you to do something, be extremely suspicious. Even if the phone call seems OK at first, but then starts to feel strange, you can stop and say no at any time.
- If you believe a phone call is an attack, simply hang up. If you want to confirm if the phone call was legitimate, go to the organization's website (such as your bank) and get the customer support phone number and call them directly yourself. That way, you really know you are talking to the real organization.
- Never trust Caller ID. Bad guys will often spoof the caller number so it looks like it is coming from a legitimate organization or has the same area code as your phone number.
- Never allow a caller to take temporary control of your computer or trick you into downloading software. This is how bad guys can infect your computer.
- If a phone call is coming from someone you do not personally know, let the call go directly to voicemail. This way, you can review unknown calls on your own time. Even better, you can enable this by default on many phones with the "Do Not Disturb" feature.

Scams and attacks over the phone are on the rise. You are the best defense you have at detecting and stopping them.

For more information, contact the UTHSC Information Security Team at (901) 448-1880 or itsecurity@uthsc.edu.