UTHSC G.U.A.R.D.

March 2018

You are a Target – Yes, I mean YOU!

by Chris Madeksho, Information Security Coordinator

A common misconception people have is that they are not a target for cybercrime: that they or their computers do not have any value. Nothing could be further from the truth. If you have a computer, mobile device, an online account, email address, credit card or engage in other type of online activity, you are worth money to cyber criminals.

Cyber criminals know stealing more credit cards, hacking more bank accounts, or compromising more passwords, the more money they can make. They will attempt to hack anyone connected to the Internet, including you. Hacking millions around the world is surprisingly easy to do with automated tools at their disposal, which requires little effort from the hacker.

Protecting yourself is easy. Just follow some simple guidelines that include:

Yourself: Ultimately, you are the first line of defense against any cyber attackers. Common sense is your best defense: if something seems odd, suspicious or too good to be true, it most likely is an attack.

Updating: Make sure that any computer or mobile device you use is fully updated and has all the latest patches. This is not only important for your operating system, but for any applications or plugins you are using.

Passwords: Use a strong, unique password for each of your accounts.

Credit Cards: Check your financial statements often. As soon as you see any unauthorized transactions on your credit card, report it immediately to your card issuer. If your bank allows you to set email or text message alerts for unusually large or odd transactions, use them for even faster notification of suspicious activity.

Social Media: The more information you post online the more likely you may put yourself at risk. Any information you post may actually identify you as a more valuable target.

If you would like more information, please contact the Information Security Team at itsecurity@uthsc.edu or (901) 448-1880.

Social Engineering: Stop & Think Before You Talk

by Alissa Torres of the SANS Institute

A common misconception people have about cyber attackers is that they only use advanced hacking tools and technology to break into people's computers, accounts and mobile devices. This is simply not true. Cyber attackers have learned that one of the easiest ways to steal your information or hack your computer is by simply talking to and misleading you.

Social engineering is a type of psychological attack where an attacker misleads you into doing something they want you to do. Social engineering has existed for thousands of years; the idea of scamming or conning someone is not new. However, cyber attackers have learned that using this technique on the Internet is extremely effective and can be used to target millions of people. The simplest way to understand how social engineering works is to take a look at a common, real-world example.

You receive a phone call from someone claiming to be from a computer support company, your ISP or perhaps Microsoft tech support. The caller explains they have noticed that your computer is behaving strangely, such as scanning the Internet or sending spam, and they believe it is infected. They have been tasked with investigating the issue and helping you secure your computer. They then use a variety of technical terms and take you through confusing steps to convince you that your computer is infected. For example, they may ask you to check to see if you have certain files on your computer and walk you through on how to find them. When you locate these files, the caller will assure you that these files are a sign that your computer is infected, when in reality, these files are nothing more than common system files found on every computer. Once they have tricked you into believing your computer is infected, they will pressure you into going to a website and buying their security software or ask you to give them remote access to your computer so they can fix it. However, the software they are selling is actually a malicious program. If you purchase and install the software, not only have they fooled you into infecting your computer, but you also just paid them to do it. If you give them remote access to your computer to fix it, in reality, they are going to take over and infect it.

Keep in mind that social engineering attacks like this are not limited to phone calls; they can happen with almost any technology, including phishing attacks via email, text messaging, Facebook messaging, Twitter posts or online chats. The key is to know what to look out for.

The simplest way to defend against social engineering attacks is to use common sense. If something seems suspicious or does not feel right, it may be an attack. Some common indicators of a social engineering attack include:

- Someone creating a tremendous sense of urgency. If you feel like you are under pressure to make a very quick decision, be suspicious.
- Someone asking for information they should not have access to or should already know.
- Something too good to be true. A common example is you are notified you won the lottery, even though you never even entered it.

If you suspect someone is trying to make you the victim of a social engineering attack, do not communicate with the person any more. If it is someone calling you on the phone, hang up. If it is someone chatting with you online, terminate the connection. If it is an email you do not trust, delete it. If the attack is work-related, be sure to report it to your help desk or information security team right away.

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