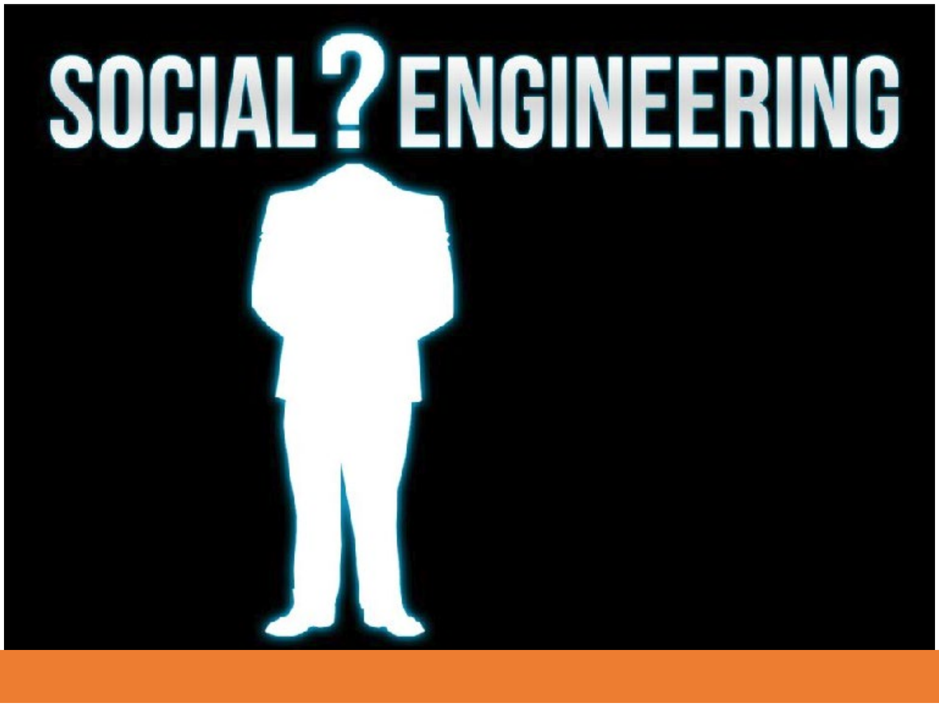

UTHSC G.U.A.R.D.

Fall 2018

Social Engineering Can Happen to Anyone

by Chris Madeksho, Information Security Coordinator

Social engineering is the art of human manipulation. It is someone asking someone else for information, or getting them to do something they normally wouldn't do. It happens to everyone…even me.

Here is my confession. I work in Information Security. I know better. I teach people to know better. But when my daughter's friend asked me what year my daughter was born, I told her. I wasn't paying attention as to what she was doing at the time, or ask her why she wanted to know. I just told her.

Ten seconds later, friend announced that she just hacked into my daughter's phone by guessing her passcode. Guess what the passcode was. Bet you can figure it out.

Who is at fault? The friend for hacking, me for giving away information, or my daughter for having a passcode that is easily guessed? How about all three? Each is a vulnerability for getting into a system that has sensitive information.

Here are five tips to keep in mind about social engineering. (Remember – I teach people to know better.)

- Don't click on links in emails or text messages, especially those asking for sensitive information. Go directly to the source.
- Don't respond to verbal requests asking for personal or financial information.
- Don't overshare on social media. Details shared there can provide hackers with information that can be used against you.
- Be aware of your surroundings. Make sure you know who should and shouldn't be in your building or area.
- Slow down. Most attacks convey a sense of urgency, so pause and think about if what the person is asking for is legitimate.

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

IN THIS ISSUE

Innocent scams?

Read some tip reminders on social engineering

Patching Devices

Learn why you need to keep all your devices up-to-date

Pumpkin Patching? … No Just Patching…

by Tom Coffy, IT Administrator, University of Tennessee Knoxville

Scary cyber criminals are constantly looking for a way into your accounts. This often happens one of two ways: phishing, or an attacker exploiting an existing vulnerability in some program running on your computer. While we continue to warn about the danger of phishing and how you can spot the danger, there are other ways to make sure your device does not become compromised. Luckily, you don't have to put in nearly as much effort to stay safe as cyber criminals need to put in in order to compromise you. Protecting yourself by updating software installed on your computer is one of the easiest ways to keep your device safe.

Every program you run on your machine can add potential vulnerabilities. Unpatched vulnerabilities are akin to leaving your door ajar in a spooky neighborhood: it's an inviting target that can make a criminal's job much simpler. Updating your software regularly, besides adding new features, will often patch existing vulnerabilities, shutting and locking the door to attackers. This makes staying up to date on software patches a priority.

If your application has an option to check for updates automatically, you should always select this option. Your program will check for updates regularly without you having to remember to check. For other applications, you'll have to check yourself, typically in the program's settings. If you are unsure about how to update one or more of your applications, how to configure a program to update automatically if the option exists, or how to check if you are up to date, contact the UTHSC HelpDesk (448-2222).

While staying up to date is critical, don't be tricked into downloading malware disguised as a bogus update to a commonly used application. NEVER click on an unsolicited link in an email or while browsing the web that claims to be an update (i.e. Adobe Flash or Microsoft Office). If you believe you need to update, navigate that application's update interface or go to the company's official website.

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

Additional comment from the UTHSC Information Security Team – certain updates, especially Windows updates, require a restart of your computer to take effect. Routinely restart your computer to make sure that it stays updated. Perhaps make it an "end of week" habit to restart before you leave on Friday.