Human Hacking as Social Engineering

Carina Franca posted on April 25, 2013 08:00

By **Patric Reynolds**, Information Technology at Adventist Risk Management®, Inc.

Knowledge is power. This is especially true when you are trying to keep personal information safe in a cyber-world where human hacking and social engineering have become the norm.

Social engineering as an act of psychological manipulation had previously been associated with the social sciences, but its usage has caught on among computer professionals.[1] In the context of security, social engineering is understood to be the art of manipulating people into performing actions or divulging confidential information.[2] While it is similar to a confidence trick or simple fraud, it is typically trickery or deception for the purpose of information gathering, fraud, or computer system access. In most cases the attacker never comes face-to-face with the victims.

For the most part, people are trusting and tend to give others the benefit of the doubt before they make judgments of people they meet but do not know. Because of their trusting nature, cyber-criminals take advantage of individuals.

Cyber-attacks can come from a variety of methods, such as in person, through an email system, and over the phone. As an example, imagine a hacker has targeted your business. His reason could be for financial gain, data extraction, or something else. Since the hacker cannot gain physical access into your facility, he chooses to download a virus onto a USB flash drive. He then puts dozens of them in your company parking lot. He patiently waits for one employee, with a curious mind, to pick up the USB drive, take it inside, and insert it into a computer. Companies can spend millions of dollars on the latest perimeter cyber-defense hardware, but still be susceptible to an internal breach, which can literally bypass all that expensive hardware for the cost of a USB flash drive from WalMart.

The simple solution to this complex issue is to ignore any and all things that are in out-of-the ordinary places. Don’t view a USB drive laying in the parking lot as a gift from heaven. The hacker is counting on someone picking up the drive and doing his work for him. The old saying, “If it is too good to be true, it usually is” is valid when discovering things that are out of place. Caution should be the key word of the day when finding something such as a USB drive in an unusual location.

IMPERSONATION

Another popular social engineering attack is called impersonation. This happens when the attacker calls from an outside line and claims to be from the ITS help desk. The hacker will ask pertinent questions of whomever they come into contact with, in order to gain a level of trust and cooperation. When that is achieved, the hacker will escalate the call and ask for personal information, such as passwords and username. When that is achieved, the hacker will gain access into the user's computer and attempt to gain access to sensitive data or servers containing company proprietary information. Then the hacker will sell the information to the company's competitors. They can also use that information for financial gain.

The easiest solution for this kind of attack is first to be familiar with your company's ITS personnel, and know them by facial and voice recognition. Another way to thwart an attack like this is to have a current copy of the office personnel directory. Simply check the number the caller is calling from to see if it is local, or not. Your ITS personnel will always call you from within the organization!

HOAX

Another popular type of social engineering attack is called simply a hoax. This is an email or web-based attack. It has the intention to try to trick the user into completing undesirable actions in order to remove a supposed virus form the user's machine. Many people see these attacks as a pop-up window on their computer screen. The message says your computer has a virus. It says that in order for you to get rid of it, you should click on the link provided and the latest and best anti-virus software will be downloaded to your computer to eliminate the threat. In reality, you have just launched an actual virus into your system and shortly you will notice that your computer will start acting very strangely.

The solution to this type of attack is two-fold and depends on the availability of your network security administrator. You can simply ignore the warning and delete the pop-up and go about your business, knowing that your administrator has installed anti-virus software to always notify him/her when an actual virus attack is in progress on the network. This type of protection would never use a simple pop-up warning. Newer generation anti-virus software programs for enterprise applications are somewhat complex and require constant interaction from an administrator, but they are effective at stopping most malware attacks when properly maintained.

If you want to be pro-active, you simply leave the pop-up on your desktop screen and contact your network administrator and let them investigate the pop-up and determine its intent.

PHISHING

One attack that is becoming very popular today is called phishing (not to be confused with actual fishing) and is a common email-based attack. The suspicious email may look like it is coming from a trusted source, such as a bank or respected institution such as PayPal or Amazon. In reality, it will direct you to some hacker command and control center that is attempting to steal access information for your real bank account. The way to easily identify a phishing email is to simply move your cursor over one of the provided links (but do not click on it). You will most likely see an email address that directs you to somewhere that has nothing to do with the actual institution proclaimed in the email.

The simple solution to this type of social engineering attack is it simply to delete the email. It is advised not to use your company account for personal transactions and purchases. This helps avoid the problem of hackers accessing your email information through the company that you made the purchase from.

THE HUMAN FACTOR

What are some human factors that can be overlooked when considering social engineering attacks on a company? Shoulder surfing is where a person gains access into a company and then simply walks around and casually peers over cubicle walls. While you are accessing sensitive information, the individual gets your password and username visually. The solution to shoulder surfing is vigilance. This requires all users to be observant and to take notice if someone that you have never seen before is walking among the office cubicles. Call security and advise them. Let them deal with the individual. If the person is in the building for a legitimate reason, he/she will not mind being checked by security, in a professional and courteous manner.

Another human vulnerability is the age-old art of dumpster diving. Although this is self-explanatory in nature, be careful what you throw away. Always shred sensitive information.

Do not forget the stealthy art of tailgating (not to be confused with the parking lot version for football parties). A tailgating attacker simply slips into a secure access point with an actual employee who has a badge. The employee may not pay attention or just doesn’t care who else enters with him/her through the access point. Suddenly, the attacker is now inside your facility and can wreak havoc on your company!

Again, due diligence is to be the order of the day for any employee entering his/her place of work. Check around you and especially behind you to see if you know the person entering with you. See if they have their ID card out and ready to use. If you do not know the individual and security is not in place, take the time to wait and see where they go after entering the building.

Beware and be cautious!

There are those around us who want our information and will go to any means to obtain it. Whether the attack comes from the inside or outside, social engineering is costing the business community billions of dollars in lost revenue, data loss, and money spent on hardware as mentioned earlier. Many of the attacks that occur can be circumvented when employees act with caution and common sense. Employers should provide current information to their employees about cyber-risks. Employees should be diligent in their responsibilities of helping to keep information as secure as possible. Use your knowledge of cyber-attackers to gain power over them today!

By **Patrick Reynolds,**
Information Technology at Adventist Risk Management®, Inc.

References:

[1]Anderson, Ross J. (2008). Security engineering : a guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6. Chapter 2, page 17

2Goodchild, Joan (11 January 2010). "Social Engineering: The Basics". csoonline. Retrieved 14 January 2010.