OUCH! | November 2014

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Social Engineering
- Detecting/Stopping Social Engineering Attacks
- Preventing Future Attacks

Social Engineering

Overview

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. In this newsletter, we will learn how these types of human attacks (called social engineering attacks) work and what you can do to protect yourself.

Guest Editor

Alissa Torres is a certified SANS instructor, specializing in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as an incident handler and working on an internal security team as a digital forensic investigator. Alissa can be found on Twitter as **@sibertor**.

Social Engineering

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

Social Engineering

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.

Learning how to prevent, detect and stop social engineering attacks is one of the most effective steps you can take to protect yourself.

Detecting / Stopping Social Engineering Attacks

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.

Preventing Future Social Engineering Attacks

Fortunately, there are precautions you can take to help prevent exposing yourself to future social engineering attacks:

Social Engineering

- Never Share Passwords. No organization will ever contact you and ask for your password. If someone is asking you for your password, it is an attack.

- Don't Share Too Much. The more an attacker knows about you, the easier it is for them to find and mislead you into doing what they want. Even sharing small details about yourself over time can be put together to create a complete picture of you. The less you share publicly, including posts on social media sites, product reviews or public forums and mail lists, the less likely you will be attacked.

- Verify Contacts. At times, you may be called by your bank, credit card company, mobile service provider or other organizations for legitimate reasons. If you have any doubt as to whether a request for information is legitimate, ask the person for their name and extension number. Then find the company's phone number from a trusted source, such as the number on the back of your credit card, the number on your bank statement or perhaps the number on the company's website. (Be sure you type the URL in your browser yourself.) This way, when you call the organization, you know you are really talking to them. Though it seems like a hassle, safeguarding your identity and personal information is well worth the additional step.

Protect Against Phishing Attacks

Phishing has become one of the most common and successful attack vectors for hacking into an organization. Training and testing your employees is a proven way to minimize this risk. Learn more about Securing The Human's Phishing solution at http://www.securingthehuman.org/info/170182.

Resources

Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Social Networking Safely:	http://www.securingthehuman.org/ouch/2013#march2013
Avoid Scams:	http://www.onguardonline.gov/topics/avoid-scams

License