The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- What Is Social Engineering?
- Detecting/Stopping Social Engineering Attacks

Social Engineering

Overview

A common misconception most people have about cyber attackers is that they use only highly advanced tools and techniques to hack into people's computers or accounts. This is simply not true. Cyber attackers have learned that often the easiest way to steal your information, hack your accounts, or infect your systems is by simply tricking you into making a mistake. In this newsletter, you will learn how these attacks, called social engineering, work and what you can do to protect yourself.

Guest Editor

James Lyne (@jameslyne) is a certified SANS instructor and Global Head of Research at Sophos. He unpicks and reverse engineers the latest and greatest creations from cyber criminals. He is also an author of the Metasploit (SEC580) and Social Engineering (SEC567) classes at SANS.

What Is Social Engineering?

Social engineering is a psychological attack where an attacker tricks you into doing something you should not do. The concept of social engineering is not new; it has existed for thousands of years. Think of scammers or con artists, it is the very same idea. What makes today's technology so much more effective for cyber attackers is you cannot physically see them; they can easily pretend to be anything or anyone they want and target millions of people around the world, including you. In addition, social engineering attacks can bypass many security technologies. The simplest way to understand how these attacks work and protect yourself from them is to take a look at two real-world examples.

You receive a phone call from someone claiming to be from a computer support company, your ISP, or Microsoft Tech Support. The caller explains that your computer is actively scanning the Internet. They believe it is infected and have been tasked with 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 if you have certain files on your computer and walk you through how to find them. When you locate these files, the caller assures you that these files prove that your computer is infected, when in reality they are common system files found on almost every computer in

Social Engineering

the world. Once they have tricked you into believing your computer is infected, they pressure you into buying their security software or giving 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 it, not only have they fooled you into infecting your computer, but you just paid them to do it. If you give them remote access to your computer, they are going to take it over, steal your data, or use it for their bidding.

Common sense is your most powerful defense in identifying and stopping most social engineering attacks.

Another example is an email attack called CEO Fraud, which most often happens at work. This is when a cyber attacker researches your organization online and identifies the name of your boss or coworker. The attacker then crafts an email pretending to be from that person and sends the email to you. The email urgently asks you to take an action, such as conducting a wire transfer or emailing sensitive employee information. Quite often, these emails pretend there is an emergency that urgently requires you to bypass standard security procedures. For example, they may ask you to send the highly sensitive information to a personal @gmail.com account. What makes targeted attacks like these so dangerous is the cyber attackers do their research beforehand. In addition, security technologies like anti-virus or firewalls cannot detect or stop these attacks because there is no malware or malicious links involved.

Keep in mind, social engineering attacks like these are not limited to phone calls or email; they can happen in any form, including text messages on your phone, over social media, or even in person. The key is to know what to look out for--you are your own best defense.

Detecting/Stopping Social Engineering Attacks

Fortunately, stopping such attacks is simpler then you may think—common sense is your best defense. If something seems suspicious or does not feel right, it may be an attack. The most common clues of a social engineering attack include:

- Someone creating a tremendous sense of urgency. They are attempting to fool you into making a mistake.

Social Engineering

- Someone asking for information they should not have access to or should already know, such as your account numbers.
- Someone asking for your password. No legitimate organization will ever ask you for that.
- Someone pressuring you to bypass or ignore security processes or procedures you are expected to follow at work.
- Something too good to be true. For example, you are notified you won the lottery or an iPad, even though you never even entered the lottery.
- You receive an odd email from a friend or coworker containing wording that does not sound like it is really them. A cyber attacker may have hacked into their account and is attempting to trick you. To protect yourself, verify such requests by reaching out to your friend using a different communications method, such as in person or over the phone.

If you suspect someone is trying to trick or fool you, do not communicate with the person anymore. If the attack is work related, be sure to report it to your help desk or information security team right away. Remember, common sense is often your best defense.

Security Awareness Training for Developers

Ensure your team can properly build defensible applications from the start by conducting security awareness training for developers, architects, managers, testers, business owners, and partners. https://securingthehuman.sans.org/u/nwb

Resources

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO Fraud:	https://securingthehuman.sans.org/ouch/2016#july2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Archives:	https://securingthehuman.sans.org/ouch/archives

License