OUCH! | July 2018

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for Everyone

Phone Call Attacks & Scams

Overview

When you think of cyber criminals, you probably think of an evil mastermind sitting behind a computer launching sophisticated attacks over the Internet. While many of today's cyber criminals do use technologies like email or instant messaging, bad guys are also using the phone to trick their victims. There are two big advantages to using a phone. First, unlike email, there are fewer security technologies that monitor phone calls and can detect and stop an attack. Second, it is much easier for bad guys to convey emotion over the phone, which makes it more likely they can trick their victims. Let's learn how to spot and stop these attacks.

How do Phone Call Attacks Work?

First, you have to understand what these attackers are after. They usually want your money, information, or access to your computer (or all three). They do this by tricking you into doing what they want. The bad guys call people around the world, creating situations that seem very urgent. They want to get you off-balance by scaring you so you won't think clearly, and then rush you into making a mistake. Some of the most common examples include:

The caller pretends that they are from a government tax department or a tax collection service and that you have unpaid taxes. They explain that if you don't pay your taxes right away you will go to jail. They then pressure you to pay your taxes with your credit card over the phone. This is a scam. Many tax departments, including the IRS, never call or email people. All official tax notifications are sent by regular mail.

The caller pretends they are Microsoft Tech Support and explain that your computer is infected. Once they convince you that you are infected, they pressure you into buying their software or giving them remote access to your computer. Microsoft will not call you at home.

You get an automated voicemail message that your bank account has been canceled, and that you have to call a number to reactivate it. When you call, you get an automated system that asks you to confirm your identity and asks you all sorts of private questions. This is really not your bank, they are simply recording all your information for identity fraud.

Protecting Yourself

The greatest defense you have against phone call attacks is yourself. Keep these things in mind:

- Anytime anyone calls you and creates a tremendous sense of urgency, pressuring you to do something, be extremely suspicious. Even if the phone call seems OK at first, but then starts to feel strange, you can stop and say no at any time.
- If you believe a phone call is an attack, simply hang up. If you want to confirm if the phone call was legitimate, go to the organization's website (such as your bank) and get the customer support phone number and call them directly yourself. That way, you really know you are talking to the real organization.
- Never trust Caller ID. Bad guys will often spoof the caller number so it looks like it is coming from a legitimate organization or has the same area code as your phone number.
- Never allow a caller to take temporary control of your computer or trick you into downloading software. This is how bad guys can infect your computer.
- If a phone call is coming from someone you do not personally know, let the call go directly to voicemail. This way, you can review unknown calls on your own time. Even better, you can enable this by default on many phones with the "Do Not Disturb" feature.

Scams and attacks over the phone are on the rise. You are the best defense you have at detecting and stopping them.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Jen Fox *provides security awareness, social engineering, and risk assessment services as a Sr. Security Consultant at All Covered. Find Jen on Twitter as @j_fox.*

Resources

Consumer Information about Identity, Privacy, & Online Security:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
Report a Phone Scam (in the US): https://www.ftccomplaintassistant.gov/#crnt
Social Engineering: https://www.sans.org/u/Fi5