OUCH! May 2021


# Vishing – Phone Call Attacks and Scams

## Overview

When you think of a cyber criminal you probably think of an evil mastermind sitting behind a computer, launching sophisticated attacks over the internet. While some of today's cyber criminals do use advanced technologies, many simply use the phone to trick their victims. There are two big advantages to using a phone: Unlike other attacks, there are fewer security technologies that can detect and stop a phone call attack; also, it is much easier for criminals to convey emotion and build trust over the phone, which makes it easier to trick their victims. Let's learn how to spot and stop these attacks.

## How Do Phone Call Attacks Work?

First, understand that these criminals are usually after your money, information, or access to your computer (or all three). They do this by tricking you into doing something you should not do, a technique called "social engineering." Cyber criminals often create situations that feel very urgent and realistic on the call. Some of the most common examples include:

- The caller pretends they are from the government and informs you that you have unpaid taxes. They explain that if you don't pay your taxes right away you will go to jail, then pressure you to pay your taxes with your credit card over the phone. This is a scam. The government will send official tax notifications only by regular mail.
- The caller pretends to be from a company such as Amazon, Apple, or Microsoft Tech Support and explains that your computer is infected. Once they convince you that your computer is infected, they pressure you into buying their software or giving them remote access to your computer.
- An automated voicemail informs you that your bank account or credit card has been canceled, and you have to call a number back to reactivate it. When you call, you get an automated system that asks you to confirm your identity as well as 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 a phone call attack is yourself. Keep these things in mind:

- Anytime anyone calls you and creates a tremendous sense of urgency or pressure, be extremely suspicious. They are attempting to rush you into making a mistake. Even if the phone call seems OK at first, if it starts to feel strange, you can stop and say "no" at any time
- Be especially wary of callers who insist that you purchase gift cards or prepaid debit cards.
- Never trust Caller ID. Bad guys will often spoof the 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 they can infect your computer.
- Unless you placed the call, never give the other party information that they should already have. For example, if the bank called you, they shouldn't be asking for your account number.
- If you believe a phone call is an attack, simply hang up. If you want to confirm that the phone call was legitimate, go to the organization's website (such as your bank) and call the customer support phone number directly yourself. That way, you really know you are talking to the real organization.
- 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, on many phones you can enable this by default with the "Do Not Disturb" feature.

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

## Guest Editor

Jen Fox holds the DEF CON 23 black badge for Social Engineering and provides security awareness education as a Security Program Specialist at Domino's. Find Jen on Twitter as @j_fox.

## Resources

**Social Engineering:** https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
**Messaging / Smishing Attacks:** https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
**Personalized Scams:** https://www.sans.org/security-awareness-training/resources/personalized-scams
**Report a Phone Scam (in the US):** https://www.reportfraud.ftc.gov

**Translated for the Community by**: