When you receive a call on your phone from a number unknown to you, it’s hard to guess who’s calling. It could be someone vishing you.

Vishing is a term derived from “phishing” and “voice” – or in simpler terms, voice phishing. Just like phishing is done through emails, vishing is a phone scam that is designed to compel you to give your personal information.

Here’s what you need to know about vishing scams, and how you can identify and avoid them.

## Vishing Explained

When a scammer makes a vishing call, they use social engineering techniques to make you share your personal and financial information, such as passwords and account details. They may use different tactics such as saying that your account is compromised, claiming to be from law enforcement or your bank, or offering help in installing a software program which is probably malware.

Vishing is a form of phishing – which is any message via email, chat, text or phone call from a reliable source – and aims to steal your money or identity.

With vishing, its comparatively much easier to contact many people. A scammer can make hundreds of calls at one time using Voice over Internet Protocol (VoIP) and spoof the caller ID in order to show the caller identity as a trusted source, for instance, your bank.

## Some Common Vishing Scams

Here are some common vishing scams used by criminals to take personal information from their victims.

### A Compromised Credit Card or Bank Account

The scammer will either call you personally or send a recorded message that tells you that there is an issue with your payment. They will then proceed and either ask you for login details to fix the issue or request you to make a new payment. Rather than giving out your information, call your financial institution directly on their publicly available number.

### An Unsolicited Investment or Loan Offer

A person will call you with an offer that seems too good to be true. For instance, they will tell you that you can earn millions of dollars on a small investment, get your student loans waived off or pay your debt with a quick fix. Typically, you will be asked to act fast to avail the offer by paying a small fee. If money is involved, don’t fall for it. A legitimate investor or lender never calls out of the blue with such types of offers.

### Social Security or Medical Care Scam

This technique is usually targeted at older adults or senior citizens. An individual poses as a medicare representative and tries to get information from the victim – such as their medicare number or bank account number. They then either steal their bank money or use their medical benefits. They may also claim that they are calling from the Social Security and will suspend the victim’s Social Security Number if they don’t share their information.

### IRS Tax Scam

This scam has many variations to it, but typically, there’s a prerecorded message that tells you about an issue in your tax returns. It further says that if you don’t respond, you will be arrested. The call is usually from a spoofed ID which makes the call look like it’s from the IRS.

## How to Identify a Vishing Scam

Being vigilant and staying updated is the key to spotting a vishing scam. However, here are some tell-tale signs that can instantly help you identify them.

* There is a sense of urgency in the caller’s message. A scammer will try to develop fear by using threats or mentioning undesirable consequences in case of nonaction. If you receive any of such calls, stay calm and never give out your personal information. Always hang up and try to do your own investigation by calling a publicly available number of the institution.
* Caller asks for your personal information. They may ask you personal questions such as your name, identity number, birth date, address, social security number[, credit card](http://www.cardzgroup.com/ContactLessSmartCard.html) details, and bank account information. To prove themselves legitimate, they may provide you your information they already have in hand. Their goal is to get remaining details about you that they don’t yet have.
* You will receive a call from a number that does not seem like an official number. When a real representative calls you from an institute, they call from their official UAN number or a landline extension. Scammers may call you from a VoIP number or a personal mobile phone number, which is a clear indication of a vishing scam.
* You receive an unsolicited call from a person claiming to be a representative. Unless you are expecting someone to call from your bank or Social Security Administration, or unless you have requested yourself, none of these agencies will call you to ask for your personal information over the phone.

## How To Avoid Vishing Scams?

Apart from staying knowledgeable about how vishing works, you can also do the following:

* **Don’t pick up calls from unknown numbers.** Though you may be tempted to pick up every call, you can simply let it go to voicemail. A caller ID can be faked, so you can never be sure who is calling. Voicemail will help you avoid acting in haste. Listen to the message first and then decide whether you should call the person back.
* **Hang up at once**. The moment you suspect that it’s a scammer making a vishing call, hang up. You don’t owe it to them to carry on a polite conversation.
* **Verify the identity of the caller.** If a person gives you a number to call back on, don’t do it. Instead, search for official number and call on that number to verify.
* **Don’t respond to prompts.** In case of an automated message, you may be asked to press buttons and respond to a number of questions. For example, the message might ask you to “press 1 to talk to operator”. Such tricks are used to identify potential targets for future calls, or for recording your voice to use it for your voice-automated accounts.

## What can you do as an Organization?

To protect your organization and employees from falling victim to vishing scams, take proactive steps and include vishing as a necessary part of your security awareness trainings. There are also several vendors that offer simulated vishing platforms to help you discover how vulnerable your staff’s attitude is towards scammers, while also demonstrating to the employees the nature of the threats they might face.