Vishing is a term derived from ‘voice’ and ‘phishing’. It is a type of social engineering attack carried out through a telephone. The attacker intends to phish out information from a target by calling them over the phone. During the phone call, the scammer asks you to share personal information or financial details such as account numbers or passwords. They do this by using social engineering techniques such as claiming to be your bank’s or a law enforcement representative, or offering you to install software for you which may actually be malware.

Vishing is a type of phishing, which is any fake message such as a text, email, chat message or phone call appearing from a trusted source. The goal behind it is to steal the target’s money or identity. Vishing has become very common in recent times. With VoIP technology, it’s now much easier to make hundreds of phone calls to any part of the world. It can also allow scammers to spoof a caller ID and make it appear from a source the target trusts.

**Some Common Vishing Scams**

Let’s look at some common vishing scams that are carried out through social engineering techniques.

**Compromised Credit Card or Bank Account**

It can be an actual person or a prerecorded message that tells you your bank account or credit card is compromised. They may tell you that there is a problem with a recent payment you made and ask you for your login credentials to fix your problem. Rather than giving your information, always hang up and call the financial institute on their official number.

**Unsolicited Investment or Loan Offer**

A scammer will call you with an offer that is too good to be true. For instance, they will lure you into an investment plan by telling you that you can earn millions with a very small investment. They may also tell you that you can pay off all your debt or clear your student loans by investing a small amount into a scheme. Typically, they will ask you to act quick and pay the amount right then for the scheme to work. Never fall for this. A legitimate investor or lender will not make such huge promises or offers.

**Social Security and Medicare Scams**

The top method scammers use to reach older adults is by phone. They often act as medical representatives and try to get financial information from the victims such as their bank account details, social security number or medicare number. They then either use their medicare benefits or steal their money.

These scams keep evolving and scammers continue to come up with new social engineering attacks to get a victim’s information. Therefore, it’s important to never give your personal information to anyone on phone even if you are seemingly talking to a trusted individual.