What is “Vishing”? 

By now, many people have heard of the term, “phishing,” but the term “Vishing” may not be as familiar. Vishing is similar to phishing but instead of using the Internet and email, thieves primarily use the telephone to carry out their scams. Below is information to help you recognize Vishing and tips for what to do if you think you’re being targeted.

What is Vishing?
The term, Vishing is short for voice phishing, and like phishing, the goal is to trick consumers into revealing confidential information that will allow thieves access to your identity and money. They are usually searching for account numbers, passwords, Personal Identification Numbers (PINs), Social Security Numbers, etc. Here are some common Vishing scams:

> Thieves may send an email indicating there has been a problem with your account or requesting information and directing you to call a phone number. When you call that number, a prerecorded message takes you through a series of prompts and leads you to reveal critical information by recording the information after a tone.

> You may receive a pre-recorded phone call where you are again taken through prompts and asked to enter important numbers via your phone’s touch pad.

> A live person may call explaining your account has been compromised or indicating that you need to update your information. They attempt to solicit information directly from you.

What Should You Do?

These attacks are on the rise in the U.S. and the techniques used by thieves are becoming very sophisticated, making legitimate calls from your credit union and attempts at theft more difficult to differentiate. Thieves are even able to manipulate how their name appears on your caller ID box, adding to the appearance that the call is actually coming from your financial institution or credit card company.

Here are some tips to keep in mind and some precautions to follow so your personal information remains protected.

> Whenever you call your credit union or credit card company, always use the phone number found on a previous account statement, in the phone book or through another trustworthy source. Do not call numbers found in unsolicited emails or on web sites that were sent as a link in an unsolicited email.

> Never provide account numbers, passwords, PINs, credit card security codes, Social Security Numbers or other confidential information over the phone unless it is in a phone call that you initiated by calling a telephone number you’re certain is valid. Keep in mind that your credit union already has this information about you and would not need to contact you to ask for it.
> If a caller already has some bit of your personal information, don’t assume the call is well-intentioned. Sometimes thieves will already have your credit card account number and are asking for your security code or other piece of crucial information. This makes the call appear more legitimate, but providing the information they’ve requested can lead to more damage.

> When in doubt, hang up the phone and contact the company yourself. If the call was genuine, they will understand your concerns and still be able to resolve the problem. If the call was a scam, you will be protected and you will have alerted the company to the scam. You may even be helping to stop others from being exploited.

Remember, it’s always better to be safe than sorry. So, be a cautious and informed consumer, and question any attempts made to access your personal and financial information.