What is Vishing?

A new scam that is popping up is called **"vishing".** Like the "phishing" scams that are now familiar to most Internet users, **vishing** is designed to trick consumers into giving out account numbers. But instead of using e-mail, **vishing** uses telephone calls generated from automated random callers.
Here's how it works: someone calls and says that your credit card has been used illegally. The caller gives you an 800 number to call to "verify" the theft of your card information and "confirm" your account number. Of course, the 800 number will be answered by an accomplice who will use your account information fraudulently.

What you need to know:

- These phone calls are becoming more common.
- The caller may be very persuasive or intimidating.
- It is not rude to hang up if you think you are being scammed.
- You cannot rely on Caller ID. It's easy for people to "spoof" their Caller ID information.

In most cases, our credit union will contact you by phone or mail to discuss anything relating to your account information. We will not contact you by e-mail. If you are unsure whether you are talking to a credit union representative, hang up and stop into your favorite branch to follow up on the information requested.

Go to www.consumer.gov/idtheft to learn more on protecting yourself from vishing and other scams.

Here's an example of a recent phone scam taking place in Northwest Ohio as reported by the Better Business Bureau:

BOGUS PHONE CALLS ASKING PRIVATE INFORMATION ARE HITTING THE AREA NOW! BEWARE of bogus phone calls claiming that your checking account numbers (or other personal information) are on the Internet. The BBB has been receiving a number of reports that unknown callers claiming to be from **"Nationwide Security" or "Nationwide Verification" (or other names)** are calling consumers – often in the evening. In one situation, the caller claims to have discovered your checking account number on the Internet, and warns that anyone can obtain it. She offers the "good news" that her company can "fix this" and remove your number. She then asks you to verify your checking account number. Often she will say, "I'll wait while you go and get your checkbook." Consumers who suspect a scam and refuse to cooperate are subjected to abusive language and treatment. IN OTHER CASES the caller claims to be working for "the government and several banks." She tells you that your checking account information has been "misdirected" and they need to correct the problem. Those who have called their banks have confirmed that this is nonsense. Some consumers tried to get the return number of the caller, but the caller ID was incorrect. We assume that these callers use "spoof" software to hide their return numbers. They may not even be in the United States. (Some callers have heavy foreign accents.) Obviously the BBB WARNS consumers to NEVER give out their personal bank account numbers or credit card numbers to anonymous callers. **These con artists can use your numbers to withdraw money from your bank account or even steal your identity.**

Anyone with more details on who is doing this is asked to call the BBB at (419) 578-6000 or 800-542-5539.