FAKE CALLER ID: ROANOKE RAPIDS POLICE DEPARTMENT

DON'T FALL FOR SPOOFING SCAMS

Telephone scammers will implement various techniques to get you to answer their call. The elderly can be particularly susceptible to their creative tactics, so it is crucial that caregivers and family members stay up to date on the latest schemes and warn their loved ones.

One technique that has been on the rise is to make it appear that you are receiving a telephone call from your own telephone number. But how is this possible?

The scammers are using a technique called caller ID "**spoofing.**" Spoofing is the practice of forcing a telephone network to display false information on the receiving caller's caller ID. The scammers do not need any complicated tools to do this. They merely need to visit a spoofing website to use the service. A simple Google Search for "caller ID spoofing" will reveal a half dozen or more websites offering such services. While manipulating caller ID is illegal for malicious purposes, it is legal for permissible purposes.

Scammers will use this caller technique to force your caller ID display to show a number from your local area code. They know that most people will only answer telephone calls that originate from local area codes. Remember, scammers are very good at what they do. Caller ID spoofing has been used by con artists pretending to be from your mortgage company, your bank or credit card company. The possibilities are endless, and it is important to be aware of these deceptive tactics.

For instance, you may receive a spoofing telephone call and the caller ID may say the IRS or display a Washington, D.C. area code. When you answer the call, the scammer pretends to be from the IRS stating that there is a problem with your tax return or that you owe money. The call then quickly escalates to the scammer demanding payment or you will be arrested. Their ultimate goal is to get you to send money, provide your credit card information or provide your bank account information. If you get this call, **hang up**. The IRS will not contact you by telephone. If there is a problem with your tax return or if you owe them money, they will contact you by mail.

Another spoofing telephone scam is the Microsoft call. In this instance, the caller ID may say "Microsoft" and the scammer claims to be a representative of the tech company. The scammers say they have detected a problem with your computer and then ask permission to remotely check your device. He will politely provide with instructions on how to grant permission to access your computer. Once this is accomplished, the scammer can access everything on your computer, including sensitive information which could easily be down loaded.

The scammer could install additional software with malicious intent or malware for nefarious reasons. If you get this call**, hang up**. Most people store sensitive information and engage in on line banking and on line shopping with their computers. Opening your device up to a stranger can be extremely risky. Microsoft will never call you. Further, they do not actively monitor computers using Microsoft.

So next time your telephone rings and the caller ID displays your own telephone number or another suspicious number, hopefully your will remember this information. It behooves people of all ages to remain skeptical when accepting calls these days. When it comes to caller ID, perception is not always reality.