Spear phishing scammers want more from you

From the Federal Trade Commission

"I'm calling from (pick any bank). Someone's been using your debit card ending in 1234 at (pick any retailer). I'll need to verify your Social Security number - which ends in 5678, right? - and full debit card information so we can stop this unauthorized activity..."

So the caller ID shows the name of your bank. And the caller knows some of your personal details. Does that mean it's legit? No. It's a scam — and scammers are counting on the call being so unsettling that you might not stop to check your bank statement.

Authorities have started hearing about phone scams like this, which combine two scammer tricks: spear phishing and caller ID spoofing. In a phishing attempt, scammers may make it look like they're from a legitimate company. And when they call or email with specific details about you — asking you to verify the information in full (things like your Social Security number or address) — that's called spear phishing.

The other nasty wrinkle in this scam is caller ID spoofing. That's when scammers fake their caller ID to trick you into thinking the call is from someone you trust.

Some scammers call and claim to be computer techs associated with well-known companies like Microsoft or Apple. Other scammers send pop-up messages that warn about computer problems. They say they've detected viruses or other malware on your computer. They claim to be "tech support" and will ask you to give them remote access to your computer. Eventually, they'll diagnose a non-existent problem and ask you to pay for unnecessary – or even harmful – services.

Here's how you can avoid these scam tactics:

- Don't assume your caller ID is proof of whom you're dealing with. Scammers can make it look like they're calling from a company or number you trust.
- If you get a phone call, email or text from someone asking for your personal information, don't respond. Instead, check it out using contact information you know is correct.
- Don't trust someone just because they have personal information about you. Scammers have ways of getting that information.
- If you get an unexpected pop-up, call, spam email or other urgent message about problems with your computer, stop. Don't click on any links, don't give control of your computer and don't send any money.
- If you think you did give a scammer your information, go to IdentityTheft.gov. You'll learn what to do if the scammer made charges on your accounts.

Even if you didn't give personal information to the scammer, report the scam to the Federal Trade Commission. Your reports help them understand what's happening and can lead to investigations and legal action to shut scammers down.