THE FTC IS CLOSED DUE TO THE LAPSE IN FUNDING. :

Learn about the status of FTC online services and website information updates during the lapse in funding.

FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Spear phishing scammers want more from you

October 31, 2018
by Lisa Lake
Consumer Education Specialist, FTC

"I'm calling from [pick any bank]. Someone's been using your debit card ending in 2345 at [pick any retailer]. I'll need to verify your Social Security number — which ends in 8190, 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.

We've started hearing about phone scams like this, which combine two scammer tricks: spear phishing and caller ID spoofing. In a phishing (https://www.consumer.ftc.gov/articles/0003-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 (https://www.consumer.ftc.gov/blog/2016/05/scammers-can-fake-caller-id-info). That's when scammers fake their caller ID to trick you into thinking the call is from someone you trust.

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 (https://www.consumer.ftc.gov/articles/0076-phone-scams), email, or text from someone asking for your personal information, don't respond. Instead, check it out using contact info 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 gave a scammer your information, go to IdentityTheft.gov (http://www.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, r (http://www.ftc.gov/consumer)eport the scam to the FTC (http://www.ftc.gov/consumer). Your reports help us understand what's happening and can lead to investigations and legal action to shut scammers down.

Blog Topics: Privacy, Identity & Online Security (https://www.consumer.ftc.gov/blog/privacy%2C-identity-%26-online-security)