Caller ID Spoofing

Your phone rings. You recognize the number, but when you pick up, it’s someone else. What’s the deal?

Scammers are using false caller ID information to trick you into thinking they are someone local, someone you trust – like a government agency or police department – or a company you do business with – like your bank or cable provider. The practice is called caller ID spoofing, and scammers don’t care whose phone number they use. One scammer recently used the phone number of an FTC employee.

Don’t rely on caller ID to verify who’s calling. It can be nearly impossible to tell whether the caller ID information is real. Here are a few tips for handling these calls:

- If you get a strange call from the government, hang up. If you want to check it out, visit the official (.gov) website for contact information. Government employees won’t call out of the blue to demand money or account information.
- Don’t give out, or confirm to the caller, your personal or financial information.
- Don’t wire money or send money using a reloadable card. In fact, never pay someone who calls out of the blue, even if the name or number on the caller ID looks legit.
- Feeling pressured to act immediately? Hang up. That’s a sure sign of a scam.

Want more tips for avoiding scams? Check out 10 Ways to Avoid Fraud.

If you’ve received a call from a scammer, with or without fake caller ID information, report it to the FTC and the FCC.

Resource: https://www.consumer.ftc.gov/blog/2016/05/scammers-can-fake-caller-id-info