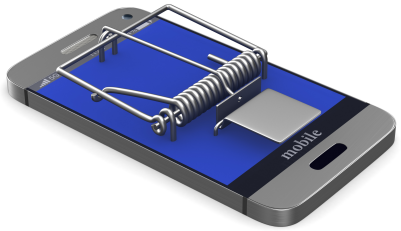

Hold the phone!

Beware of the phone number that displays when you receive a call. That number can easily be faked to look like a government agency, your employer, a family member, or even your phone number! And in many cases, it's legal!

Scammers use this tactic, called "vishing," to get information about you or your employer. Here's what you should know.

- Don't assume callers are who they claim to be. Software for spoofing phone numbers is inexpensive and easy to find.
- After you answer the phone, if there is a 1-2 second delay before someone responds, the call is either a sales call or a scam.
- Allow calls that show up as "unknown" to go to voicemail. If it's a legitimate call, they'll leave a voicemail.
- Make sure your voicemail is protected by a password. It's easy for a scammer to spoof your phone number and access the messages.
- Wondering if the call is really from your bank, government agency, employer, or another familiar source? Call them back using the phone number you have for them or the contact number on the website, not the number that shows up on your phone.
- If a caller instructs you to press a number to continue, hang up.
- If you suspect the call is a scam, hang up immediately. The longer you remain on the line and answer questions, the more apt you are to give information you shouldn't.
- Consider downloading and subscribing to a caller ID app to prevent sales and scam calls from getting through. Respected brands include HiYa, RoboKiller, Mr. Number, NoMoRobo, and Truecaller.
- There's not much you can do to prevent spoofed, sales, or scam calls made to a landline. Contact your phone provider and look into getting a call-blocking device.
- **Moves that aren't very effective:**
  - Blocking numbers one at a time.
  - Reporting vishing calls to the government.
  - Changing your phone number.

Resources: FTC, Applavia, Gadget Hacks, Android Authority, MakeUseOf, Fortinet

XTREME I.C.E.