



Eight Signs That It's a Scam

1. Scammers PRETEND to be from an organization you know.
2. Scammers often pretend to be contacting you on behalf of the government.
 - They might use a real name, like the Social Security Administration, the IRS, or Medicare, or make up a name that sounds official.
 - Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations.
 - They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.
3. Scammers say there's a PROBLEM or a PRIZE.
 - They might say you're in trouble with the government.
 - Or you owe money.
 - Or someone in your family had an emergency.
 - Or that there's a virus on your computer.
4. Scammers say there's a problem with one of your accounts and that you need to verify some information.
5. Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.
6. Scammers PRESSURE you to act immediately.
7. Scammers want you to act before you have time to think.
 - If you're on the phone, they might tell you not to hang up so you can't check out their story.
 - They might threaten to arrest you, sue you, take away your driver's or business license, or deport you.
 - They might say your computer is about to be corrupted.
8. Scammers tell you to PAY in a specific way.
 - They often insist that you pay by sending money through a money transfer company or by putting money on a gift card and then giving them the number on the back.

- Some will send you a check (that will later turn out to be fake), tell you to deposit it, and then send them money.

What You Can Do to Avoid a Scam

- Block unwanted calls and text messages.
- Take steps to block unwanted calls and to filter unwanted text messages.
- Don't give your personal or financial information in response to a request that you didn't expect. Legitimate organizations won't call, email, or text to ask for your personal information, like your Social Security, bank account, or credit card numbers.
- If you get an email or text message from a company you do business with and you think it's real, it's still best not to click on any links. Instead, contact them using a website you know is trustworthy. Or look up their phone number.
- Don't call a number they gave you or the number from your caller ID.
- Resist the pressure to act immediately. Legitimate businesses will give you time to make a decision.
- Anyone who pressures you to pay or give them your personal information is a scammer.
- Know how scammers tell you to pay.
- Never pay someone who insists you pay with a gift card or by using a money transfer service.
- And never deposit a check and send money back to someone.

Other Helpful Sites to Help Detect Scams:

<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

<https://suffolkpd.org/Information-and-Policies/SCAM-Alerts>

https://www.cisa.gov/uscert/sites/default/files/publications/emailscams_0905.pdf