Online Security
Scam Awareness & Prevention

SIGNS IT'S A SCAM

Scammers PRETEND to be from an Organization You Know.

Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the FTC, Social Security Administration, 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.

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.

Some scammers say there's a problem with one of your accounts and that you need to verify some information.

Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

Scammers PRESSURE You to Act Immediately.

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.

Scammers Tell You to PAY in a Specific Way.

They often insist that you can only pay by using cryptocurrency, wiring money through a company like MoneyGram or Western Union, using a payment app, or putting money on a gift card and then giving them the numbers on the back of the card.

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

HOW 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.

Honest 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.

Honest 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 that you can only pay with cryptocurrency, a wire transfer service like Western Union or MoneyGram, a payment app, or a gift card. And never deposit a check and send money back to someone.

◊ Stop and talk to someone you trust.

Before you do anything else, tell someone — a friend, a family member, a neighbor — what happened. Talking about it could help you realize it's a scam.

Report Scams to the FTC

If you were scammed or think you saw a scam, tell the FTC at ReportFraud.ftc.gov