Is It a Scam?

Understanding Scammers' Tactics

How did they contact you?

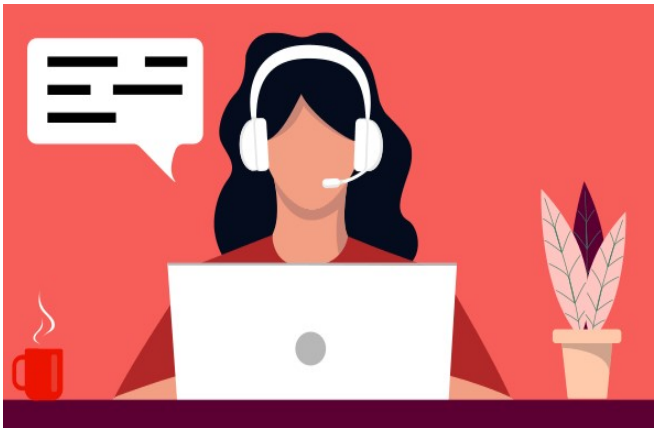
- **Phone?** Only answer calls when you are absolutely certain who is calling. If uncertain, let the caller leave a message, and take time to consider whether it may be a scam before reacting.
- **Email?** Don't assume that an email is from the person or company that it appears to be. Hover your mouse over the name to view the sender's email address or contact information.
- **Social media?** That message from a friend? Scammers may have hacked their account. Reach out another way to confirm they sent the message.
- **Text message?** Don't click links.
- **In-person?** Take a stand against door-to-door sales calls – don't open your door to strangers.
- **Traditional mail?** Treat with suspicion any mail announcing lottery winnings or unanticipated debt collections.

Who did they say they were?

- **Law enforcement?** They never require immediate payment for anything.
- **A government agency?** They typically first contact you by mail unless you have existing business with them.
- **Tech support about a virus on your device?** It's a scam.
- **Amazon?** It's a scam; they don't make calls.
- **Your bank?** Hang up and call back using a number you know to be valid, from a recent statement, for example.
- **A family member in trouble?** Hang up and contact them or someone who can confirm they are safe.
- **Lottery?** It's a scam if you're asked to pay upfront fees.
- **Love interest you've only met online claiming to be in the military or on business abroad?** This is a romance scam.
- **Job opportunity?** Share no sensitive information when applying for a job.

What did they ask for?

Be wary of anyone who contacts you and claims you need to share sensitive information or payment of some sort.



Is It a Scam?

The answers to these questions may provide clues.

How did they contact you?

- O Phone
- O Email
- O Social media / online
- O Text
- O In-person
- O Mail

Who did they say they were?

- O Law enforcement
- O Government agency
- O Computer technician
- O A retailer such as Amazon
- O A utility company
- O A family member in need
- O Someone you met online who claims to be in the military or working abroad
- O A potential employer

What did they ask for?

- O Cash/ gift cards/ peer-to-peer payments/ wire transfer/ credit cards/ cryptocurrency
- O Personal information such as bank account info, Social Security number, Medicare number, or birth date
- O Payment to address a problem, such as taxes owed
- O Payment to receive lottery winnings
- O Money to help a loved one in urgent need

Any check marks above indicate a possible scam. Take these steps:

- **Disengage immediately.**
- **Contact the AARP Fraud Watch Network Helpline (877-908-3360) to talk to a trained specialist.**
- **If they deceived you into paying for some obligation using a debit or credit card, contact your financial institution immediately using a number from a statement or the back of your card.**
- **If they deceived you into sharing sensitive information such as your Social Security number, go to identitytheft.gov and follow the guidance.**
- **If they deceived you into sharing your Medicare number, contact Senior Medicare Patrol at 877-808-2468.**
- **If you lost money or experienced identity fraud, contact local police and state you are a victim of a financial crime and you need to file a police report.**