Four Warning Signs of a Scam

Recognizing the tactics scammers use can help protect you and others from fraud. Here are four common signs that indicate a potential scam:

1. Impersonation of Trusted Organizations

Scammers often pose as representatives of well-known organizations, such as government agencies (e.g., the IRS, Social Security Administration, Medicare), utility companies, technology firms, or charitable organizations. They may use real names or invent official-sounding ones to gain your trust. They frequently manipulate caller ID information to make it appear as though the call is coming from a legitimate source. Be cautious—what you see on your screen may not be accurate.

2. Claims of a Problem or a Prize

Scammers may tell you:

- You're in trouble with the government.
- You owe money or face legal action.
- A family member is in an emergency.
- Your computer has a virus.
- You've won a prize or lottery—but must pay a fee to claim it.

These claims are designed to provoke fear or excitement and prompt quick action.

3. Urgent Pressure to Act Immediately

Fraudsters often create a sense of urgency to prevent you from thinking critically or seeking advice. They may:

- Insist you stay on the phone.
- Threaten arrest, license revocation, or deportation.
- Claim your computer or accounts are at immediate risk.

Legitimate organizations will never pressure you to act without time to consider your options.

4. Unusual Payment Requests

Scammers typically demand payment through unconventional methods, such as:

- Cryptocurrency
- Wire transfers (e.g., MoneyGram, Western Union)
- Payment apps
- Gift cards (by asking for the numbers on the back)

Some may send fake checks and ask you to deposit them and send money back—this is a common scam tactic.

How to Protect Yourself

- Block unwanted calls and texts. Use tools and settings on your phone to reduce spam.
- Never share personal or financial information in response to unexpected requests.
- Avoid clicking links in unsolicited emails or texts.

 Instead, visit the organization's official website or call a verified number.
- Resist pressure to act quickly. Scammers rely on urgency—take time to verify.
- Understand legitimate payment methods. No trustworthy organization will demand payment via cryptocurrency, wire transfer, or gift cards.
- Talk to someone you trust. Discuss suspicious messages or calls with a friend, family member, or colleague before taking action.

Report Scams

If you've encountered a scam or suspect fraudulent activity, report it to the Federal Trade Commission (FTC) at ReportFraud.ftc.gov.