April 2025 | Issue No. 20

Security is *Everyone's* Responsibility

Signs of a Scam

Summary

Scammers tell all kinds of stories to try to steal your money or information. They may pretend to be a government official saying you owe a fine. Or they may pose as a friend or online love interest who supposedly needs information or money. A scammer might offer you a (fake) job but say you need to pay a fee before you get hired.

Yet though the lies differ, scammers often use the following five tactics:

1. **Contacting you unexpectedly.**

   They're hoping the element of surprise causes you to drop your guard. Don't respond to unexpected calls, emails, texts, or social media messages that request money or personal information. If you're not sure if a call or message is real, look up contact information from a different source and reach out to the business, organization, or person — even if they're claiming to be a friend or relative.

2. **Telling you to hurry.**

   Scammers don't want you to have time to think or check out their story. So slow down and think it over. Talk to someone you trust before providing money or information.

3. **Telling you to pay — and HOW to pay**.

   Scammers want you to pay in ways that are hard to track. Don't pay anyone who contacts you out of the blue and insists you can only pay with cash, a gift card, a wire transfer, cryptocurrency, or a payment app. Those methods make it hard to get your money back, if it's possible at all.

4. **Pretending to be from an organization you know.**

   To earn your trust, scammers often pretend to be contacting you on behalf of a government agency, like the FTC, Social Security Administration, IRS, or Medicare (some even make up a name that sounds official). They may pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations. They often use technology

to change the phone number that appears on your caller ID so the name and number you see is convincing — even though it's not real. Don't pay them until you've checked the source independently, just like you would for any unexpected contact, and see how the organization actually reaches out to people. Many, like the IRS, *never* call people and ask for payment.

5. **Saying there's a problem or a prize**.

   It's a tactic to hook you emotionally. 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. Don't.

It's Easier to Prevent than Recoup

Knowing the signs of a scam helps you see through the stories that scammers tell. Meanwhile, protect yourself from fraud with these defenses:

Block unwanted calls and text messages. The best way to protect yourself from scam calls and texts is not to get them. The easiest way? Block unwanted calls and filter unwanted text messages.

Don't give your personal or financial information to someone you didn't expect to ask for them. Organizations that care about your security don't ask you to report your social security, bank account, or credit card numbers in unsafe ways, like on the phone or via text. Even if you think an email or text message is from a legitimate source, it's still best not to click on any links. Instead, contact the organization 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. Most businesses will give you time to make a payment. People who pressure you for money or your personal information probably do not have your best interests in mind.

Know how scammers want 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 stranger's check and send the money on to someone else — when the check bounces, you're stuck with the loss.

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 think the situation through.

If you've lost money to a scam, reach out to the company that transferred the money right away to see if there's a way to get your money back. Then report the scammer at ReportFraud.ftc.gov.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the

Getting Help

attack to IC3.gov and the police, and file a report with the Federal Trade Commission.

If you identify suspicious activity involving your financial institution, contact them immediately.

TLP WHITE

12120 Sunset Hills Rd, Reston
VA 20190