have you HEARD about...

"You've Won" Scams

Here's how they work:

You get a call, letter, email, or text saying that you won! Maybe it's a vacation or cruise, a lottery or a sweepstakes. The person calling about your prize is so excited. They can't wait for you to get your winnings.

But here's what happens next. They say there are fees, taxes, or customs duties to pay. Then they ask for your credit card number or bank account information. Or they ask you to pay with cash, gift cards, wire transfers, or cryptocurrency.

If you pay a scammer or share information, you lose. There is no prize. Instead, you get more requests for money, and more false promises that you won big.

Here's what to do:

1. **Keep your money — and your information — to yourself.** Never share your financial information with someone who contacts you and claims to need it. And never send anyone cash or pay with gift cards, wire transfers, or cryptocurrency.

2. **Pass this information on to a friend.** You probably ignore these kinds of scams when you see or hear them. But you probably know someone who could use a friendly reminder.

A call or a message says your computer is

INFECTED.

That's a

SCAM.

Don't call a phone number or click a link.

Don't give control of your computer.

Don't send money.

have you HEARD about...

Money Mule Scams

Here's how they work:

Someone might offer you a job. Or say you've won a sweepstakes. Or start an online relationship with you. Whatever the story, next they want to send you money – and then ask you to send it on to someone else. They often say to wire the money or use gift cards.

But that money is stolen. And there never was a job, a prize, or a relationship – only a scam. That scammer was trying to get you to be what some people call a "money mule."

If you deposit a scammer's check, it might clear. But later, when the bank finds out it's a fake check, you'll have to repay the bank. And if you help a scammer move stolen money – even if you didn't know it was stolen – you could get into legal trouble.

Here's what you can do:

1. **Keep your money to yourself.** Never agree to move money for someone who contacts you, even if they promise a relationship, job, or prize. You could lose money and get in legal trouble.

2. **Pass this information on to a friend.** You may see through these scams. But chances are you know someone who could use a friendly reminder.

have you HEARD about...

Grandkid and Family Scams

Here's how they work:

You get a call: "Grandma, I need money for bail." Or maybe an email from someone claiming to be your brother or a friend who says they're in trouble. They need money for a medical bill. Or some other kind of emergency. The caller says it's urgent — and tells you to keep it a secret.

But is the caller who you think it is? Scammers are good at pretending to be someone they're not. They can be convincing: sometimes using information from social networking sites, or hacking into your loved one's email account, all to make it seem more real. And they'll pressure you to send money before you have time to think.

Here's what to do:

1. **Stop. Check it out.** Look up your family member's phone number yourself and call another family member to check out the story.

2. **Pass this information on to a friend.** You may not have gotten one of these calls, but chances are, you know someone who will get one — if they haven't already.

have you HEARD about...

Charity Fraud

Here's how it works:

Someone contacts you asking for a donation to their charity. It sounds like a group you've heard of, it seems real, and you want to help.

But how can you tell what's a scam? Charity scammers want to get your money quickly. They often pressure you to donate right away. They ask for cash, gift cards, cryptocurrency, or wire transfers. Scammers often refuse to send you information about the charity. They won't answer questions or explain how the money will be used. They might even lie and say you already made a pledge to donate.

Here's what to do:

1. **Take your time.** Don't trust your caller ID. Scammers use technology to make any name or number appear on caller ID. Tell callers to send you information by mail. Do some research. Is the charity real? If callers ask you for cash, gift cards, cryptocurrency, or a wire transfer, it's a scam.

2. **Pass this information on to a friend.** Probably everyone you know gets charity solicitations. This information could help someone else spot a possible scam.

have you HEARD about...

Identity Theft

Here's how it works:

Someone gets your personal information and runs up bills in your name. They might use your Social Security or Medicare number, your credit card, or your medical insurance – along with your good name.

How would you know? You could get bills for things you didn't buy or services you didn't get. Your bank account might have withdrawals you didn't make. You might not get bills you expect. Or, you could check your credit report and find accounts you never knew about.

Here's what you can do:

1. **Protect your information.** Put yourself in another person's shoes. Where would they find your credit card or Social Security number? Protect your personal information by shredding documents before you throw them out, by giving your Social Security number only when you must, and by using strong passwords online.

2. **Read your monthly statements and check your credit.** When you get your account statements and explanations of benefits, read them for accuracy. You should recognize what's there. Once a year, get your credit report for free from AnnualCreditReport.com or 1-877-322-8228. The law entitles you to one free report each year from each credit reporting company. If you see something you don't recognize, you will be able to deal with it.

have you HEARD about...

Imposter Scams

Here's how they work:

You get a call or an email. It might say you've won a prize. It might seem to come from a government official. Maybe it seems to be from someone you know – your grandchild, a relative or a friend. Or maybe it's from someone you *feel* like you know, but you haven't met in person – say, a person you met online who you've been writing to.

Whatever the story, the request is the same: wire money to pay taxes or fees, or to help someone you care about.

But is the person who you think it is? Is there an emergency or a prize? Judging by the complaints to the Federal Trade Commission (FTC), the answer is no. The person calling you is pretending to be someone else.

Here's what you can do:

1. **Stop. Check it out – before you wire money to anyone.** Call the person, the government agency, or someone else you trust. Get the real story. Then decide what to do. No government agency will ever ask you to wire money.

2. **Pass this information on to a friend.** You may not have gotten one of these calls or emails, but the chances are you know someone who has.

have you HEARD about...

Home Repair Scams

Here's how they work:

Someone knocks on your door or calls you. They say they can fix your leaky roof, install new windows, or provide the latest energy-efficient solar panels. They might find you after a flood, windstorm or other natural disaster. They pressure you to act quickly, might ask you to pay in cash, or offer to get you financing.

But here's what happens next: they run off with your money and never make the repairs. Or they do shoddy repairs that make things worse. Maybe they even put you in a bad financing agreement that puts your house at risk.

Here's what you can do:

1. **Stop. Check it out.** Before making home repairs, ask for references, licenses and insurance. Get three written estimates. Don't start work until you have a signed contract. And don't pay by cash or wire transfer.

2. **Pass this information on to a friend.** You may see through these scams. But chances are you know someone who could use a friendly reminder.

have you HEARD about...

Health Care Scams

Here's how they work:

You see an ad on TV, telling you about a new law that requires you to get a new health care card. Maybe you get a call offering you big discounts on health insurance. Or maybe someone says they're from the government, and she needs your Medicare number to issue you a new card.

Scammers follow the headlines. When it's Medicare open season, or when health care is in the news, they go to work with a new script. Their goal? To get your Social Security number, financial information, or insurance number.

So take a minute to think before you talk: Do you really have to get a new health care card? Is that discounted insurance a good deal? Is that "government official" really from the government? The answer to all three is almost always: No.

Here's what you can do:

1. **Stop. Check it out.** Before you share your information, call Medicare (1-800-MEDICARE), do some research, and check with someone you trust. What's the real story?

2. **Pass this information on to a friend.** You probably saw through the requests. But chances are you know someone who could use a friendly reminder.