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...

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.

How can you tell what charity is legitimate and what's a scam? Scammers want your money quickly. Charity scammers often pressure you to donate right away. They might ask for cash, and might even offer to send a courier or ask you to wire money. Scammers often refuse to send you information about the charity, give you details, or tell you how the money will be used. They might even thank you for a pledge you don't remember making.

Here's what you can do:

1. **Take your time.** Tell callers to send you information by mail. For requests you get in the mail, do your research. Is it a real group? What percentage of your donation goes to the charity? Is your donation tax-deductible? How do they want you to pay? Rule out anyone who asks you to send cash or wire money. Chances are, that's a scam.

2. **Pass this information on to a friend.** It's likely that nearly everyone you know gets charity solicitations. This information could help someone else spot a possible scam.

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.

have you HEARD about...

Paying Too Much

Here's how it works:

Everyone pays all kinds of bills. Some are higher than you think they should be. Sometimes, unexpected charges appear on your bill – or sometimes, you might see a fee for a service you don't recall ordering. Are you paying more than you should?

You are your own best advocate. How often does a company figure out that you've overpaid – and refund your money? It could happen – but you're more likely to get money back if you spot the error and point it out.

It means keeping track of what you normally pay, and what the charges are for. You also can ask for a better deal: call to see if there's a promotion you qualify for and how long it will last, or if they can lower your interest rate. They might say no – but if you don't ask, you don't get.

Here's what you can do:

1. **Read every statement, every time.** Does something look wrong or unfamiliar? Call the company and ask. If you don't like the response you get, ask for a supervisor. And keep written records of your calls.

2. **Pass this information on to a friend.** Not paying more than you need to might come easily to you. But you probably know someone who could use some friendly encouragement.

have you HEARD about...

“You’ve Won” Scams

Here’s how they work:

You get a card, a call, or an email telling you that you won! Maybe it’s a trip or a prize, a lottery or a sweepstakes. The person calling is so excited and can’t wait for you to get your winnings.

But here’s what happens next: they tell you there’s a fee, some taxes, or customs duties to pay. And then they ask for your credit card number or bank account information, or they ask you to wire money.

Either way, you lose money instead of winning it. You don’t ever get that big prize. Instead, you get more requests for money, and more promises that you won big.

Here’s what you can 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 wire money to anyone who asks you to.
2. **Pass this information on to a friend.** You probably throw away these kinds of scams or hang up when you get these calls. But you probably know someone who could use a friendly reminder.

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...

Grandkid Scams

Here's how they work:

You get a call: "Grandma, I need money for bail." Or money for a medical bill. Or some other kind of trouble. 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, to make it seem more real. And they'll pressure you to send money before you have time to think.

Here's what you can do:

1. **Stop. Check it out.** Look up your grandkid's phone number yourself, or call another family member.

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...

IRS Imposter Scams

Here's how they work:

You get a call from someone who says she's from the IRS. She says that you owe back taxes. She threatens to sue you, arrest or deport you, or revoke your license if you don't pay right away. She tells you to put money on a prepaid debit card and give her the card numbers.

The caller may know some of your Social Security number. And your caller ID might show a Washington, DC area code. But is it really the IRS calling?

No. The real IRS won't ask you to pay with prepaid debit cards or wire transfers. They also won't ask for a credit card over the phone. And when the IRS first contacts you about unpaid taxes, they do it by mail, not by phone. And caller IDs can be faked.

Here's what you can do:

1. **Stop. Don't wire money or pay with a prepaid debit card.** Once you send it, the money is gone. If you have tax questions, go to irs.gov or call the IRS at 800-829-1040.

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

have you HEARD about...

Tech Support Scams

Here's how they work:

You get a call from someone who says he's a computer technician. He might say he's from a well-known company like Microsoft, or maybe your internet service provider. He tells you there are viruses or other malware on your computer. He says you'll have to give him remote access to your computer or buy new software to fix it.

But is the caller who he says he is? Judging by the complaints to the Federal Trade Commission, no. These scammers might want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything on your computer.

Here's what you can do:

1. **Hang up.** Never give control of your computer or your credit card information to someone who calls you out of the blue.
2. **Pass this information on to a friend.** You might know these calls are fakes, but chances are you know someone who doesn't.

have you HEARD about...

Online Dating Scams

Here's how they work:

You meet someone special on a dating website. Soon he wants to move off the dating site to email or phone calls. He tells you he loves you, but he lives far away — maybe for business, or because he's in the military.

Then he asks for money. He might say it's for a plane ticket to visit you. Or emergency surgery. Or something else urgent.

Scammers, both male and female, make fake dating profiles, sometimes using photos of other people — even stolen pictures of real military personnel. They build relationships — some even fake wedding plans — before they disappear with your money.

Here's what you can do:

1. **Stop. Don't send money.** Never wire money, put money on a prepaid debit card, or send cash to an online love interest. You won't get it back.

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.

Want to know more? Sign up for scam alerts at ftc.gov/subscribe.

...Pass it ON

Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.