Business Impersonator Scams

Here's how they work:

You get a call, email, text, or message on social media that looks like it's from a business you know. It says there's a problem with your account, or you won a prize. It tells you to call a number or click a link.

But the message isn't really from a familiar business, it's from a scammer. If you call, they'll tell you to send payment or give personal information. They'll insist you can only pay with gift cards or cryptocurrency, or by wiring money or using a payment app, which no honest business will do. Or they'll ask for your Social Security number or access to your computer.

But it was never really that business contacting you, there wasn't a problem, and there was never a prize.

Here's what to do:

1. **Stop.** If you get an unexpected call, email, text, or message on social media — even if it looks like it's from a business you know — don't click any links. And don't call phone numbers they give you. These are often scams.

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

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

Your report can help protect other people. By reporting fraud, you can help alert law enforcers across the country who investigate and bring cases against scammers. Your report makes a difference.

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

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.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

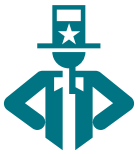
FEDERAL TRADE COMMISSION

August 2023

ftc.gov/PassItOn

Government Impersonator Scams

Here's how they work:



You get a call, email, or text message from someone who says they're from the Social Security Administration or Medicare. They say something alarming — like your Social Security number has been suspended. Or maybe you'll miss out on a government benefit. To fix it, they say you must pay, give them your personal information, or put your money on gift cards and read them the PIN numbers off the back of the cards.

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 government calling?

No. The government doesn't call people out of the blue with threats or promises of money. Caller IDs can be faked, so if you're not sure, contact the agency at a phone number you know to be true (not the one they called you from).

Here's what to do:

1. **Stop. Don't send money to anyone who calls, emails, or texts and says they're with the government.** Don't send them cash or pay them with gift cards, wire transfers, cryptocurrency or a payment app. The government won't demand payment that way — and once you pay, it's hard to get your money back. If you want to reach a government agency, find contact information at **USA.gov.**

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

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

Your report can help protect other people. By reporting fraud, you can help alert law enforcers across the country who investigate and bring cases against scammers. Your report makes a difference.

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

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.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

have you HEARD about...

Health Insurance Scams

Here's how they work:

You get a call or see an ad offering you big discounts on health insurance. Or maybe someone contacts you out of the blue, says they're from the government, and asks for your Medicare number to issue you a new card.

Scammers follow the news. When it's Medicare open season, or when health insurance is a big story, scammers get busy contacting people. They want to get your Social Security number, financial account numbers, or insurance information.

Think about these questions. Is that discount insurance plan a good deal? Is that "government official" really from the government? Do you really have to get a new health insurance card? The answer to all three is almost always: No.

Here's what to 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.

2. **Pass this information on to a friend.** You probably know about these scams. But you might know someone who could use a friendly reminder.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

Home Repair Scams

Here's how they work:

Someone knocks on your door or calls you. They say they can fix your leaky roof, put in new windows, or install the latest energy-efficient solar panels. They might find you after a flood, windstorm, or other natural disaster. They pressure you to act quickly and 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 got you to sign a bad financing agreement that puts your house at risk.

Here's what to do:

1. **Stop. Check it out.** Before making home repairs, ask for recommendations from people you trust and check that the companies have licenses and insurance. Get three written estimates. Don't start work until you have reviewed and signed a written contract. And don't pay someone who insists you can only pay with cash, a payment app, or wire transfers.

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

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

Identity Theft

Here's how it works:

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

Here are signs that someone is using your identity: You get bills for things you didn't buy or services you didn't use. Your bank account has withdrawals you didn't make. You don't get bills you expect. Or you check your credit report and find accounts you never knew about.

Here's what to do:

1. **Protect your information.** Shred documents before you throw them out, give your Social Security number only when you must, and use strong passwords online.

2. **Check your monthly statements and your credit.** Read your account statements and explanations of benefits. Be sure you recognize what they show. 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 bureau. If you see something you don't recognize, deal with it right away.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Identity Theft

If you suspect identity theft, please report it to the Federal Trade Commission.

- Go online: **IdentityTheft.gov**
- Call the FTC at 1-877-ID-THEFT (1-877-438-4338)
  or TTY 1-866-653-4261

Visit **IdentityTheft.gov** to report identity theft and get a personal recovery plan. It will walk you through the steps to take.

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

Investment Scams

Here's how they work:

You see an infomercial, or an ad online, saying you can learn how to make lots of money. It sounds quick, easy, and low risk — and it might involve investing in financial or real estate markets.

The company says their system is "proven" and they even have testimonials from people who've used their system and gotten rich. But those people could be paid actors and their reviews could be made up.

All investments have risks. No one can guarantee a specific return on an investment. And nobody can guarantee that an investment will be successful. Anyone who does promise you a guaranteed return at low or no risk is a scammer.

Here's what to do:

1. **Stop. Take time to research the offer.** Scammers want to rush you into a decision. Slow down. Search online for the name of the company and words like "review," "scam," or "complaint."

2. **Pass this information on to a friend.** You may not have gotten an offer like this, but chances are, you know someone who has.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

Job and Money-Making Scams

Here's how they work:

You see an ad saying you can earn big money, even working from home. Another ad offers help starting an online business — with a proven system to make money. Maybe you uploaded your resume to a job search website, and someone contacts you for an interview — but first, they want your driver's license and bank account numbers.

If you respond to these opportunities to work from home, you'll get requests for money — for training or special access — but you'll never get the job. If you buy the proven system, you'll get pressure to pay more for extra services. But you won't get anything that really helps you start a business or make money. And if you give the caller your driver's license and bank account numbers, they might steal your identity or your money.

Here's what to do:

1. **Stop. Check it out.** Never pay money to earn money. And don't share personal information until you've done your research. Search online for the company name and the words "review," "scam," or "complaint."

2. **Pass this information on to a friend.** You probably know how to keep your money and information safe. But you may know someone who could use a friendly reminder.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

Romance Scams

Here's how they work:

Someone contacts you on social media — and they're interested in getting to know you. Or maybe you meet someone special on a dating website or mobile app. Soon the person wants to write to you directly or start talking on the phone. They say it's true love, but they live far away — maybe because of work, or because they're in the military.

Then they start asking for money. Maybe it's for a plane ticket to visit you. Or emergency surgery. Or something else urgent.

Scammers of all ages, genders, and sexual orientations make fake profiles, sometimes using photos of other people — even stolen pictures of real military personnel. They build relationships — some even pretend to plan weddings — before they disappear with your money.

Here's what to do:

1. **Stop. Don't send money.** Never send cash, or send money using gift cards, wire transfers, cryptocurrency, or a payment app to an online love interest. Once you pay this way, it's hard to get your money back.

2. **Pass this information on to a friend.** You may not have gotten tangled up with a romance scam, but chances are, you know someone who will — if they haven't already.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

Tech Support Scams

Here's how they work:

You get a call or message from someone who says they're a computer technician. Or a number appears in a pop-up message on your screen. Or maybe you're looking for tech support and call a number you find in a search engine. The person on the phone says they're from a well-known company like Microsoft or Apple. And they tell you about viruses or other malware on your computer. Maybe they'll ask you for remote access to your computer or say you must buy new software to fix it.

But are they someone you can trust? Judging by reports to the Federal Trade Commission, no. Tech support scammers will try 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 (including your account passwords).

Here's what to do:

1. **Hang up.** If you get an unexpected call from someone saying there's a problem with a computer — hang up, it's a scam. If you need tech help, go to someone you know and trust — and call them at a phone number you know to be true (the ones that show up in your search engine aren't always legit).

2. **Pass this information on to a friend.** You might know these are scammers, but chances are, you know someone who doesn't.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

Unwanted Calls and Text Messages

Here's how they work:

You pick up the phone and hear a recorded message — a robocall — or a live person selling something. Maybe it's not who your caller ID said it was. Or you get an unexpected text message saying you won a prize, have a package waiting, or must contact your bank.

Recorded sales calls are illegal unless you give a business written permission to robocall you. If your number is on the Do Not Call Registry, you're not supposed to get any recorded or live sales calls. But scammers ignore the rules about when and how they can call you.

Scammers use technology to make any name or number show up on your caller ID: the IRS, a business you know, or even your own number. You can't trust caller ID because phone numbers can be faked. Scammers send text messages to trick you into clicking links and giving personal information.

Here's what to do:

1. **Hang up on unwanted calls and ignore unexpected texts.** Don't press any numbers or click on links. Blocking services might reduce unwanted calls and texts. Ask your phone carrier about call and message blocking. Read expert reviews about your options. Learn more at **ftc.gov/calls**.

2. **Pass this information on to a friend.** You may know what to do about unwanted calls and texts, but you probably know someone who doesn't.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

Please Report Scams

If you get scam calls, illegal robocalls, or unwanted text messages, please report them to the Federal Trade Commission.

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn

“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 insist you can only pay with cash, gift cards, wire transfers, cryptocurrency, or a payment app.

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 pay anyone who insists you send cash or can only pay with cash, gift cards, wire transfers, cryptocurrency, or a payment app.
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.

Want to know more?
Sign up for Consumer Alerts
at **ftc.gov/ConsumerAlerts**.

...Pass it ON

Please Report Scams

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

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

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

FEDERAL TRADE COMMISSION
August 2023

ftc.gov/PassItOn