



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](https://www.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.





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.





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.





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.





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.





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.





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

...Pass it ON

Please Report Identity Theft

If you suspect identity theft, act quickly. 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

The FTC operator will give you the next steps to take. Visit ftc.gov/idtheft to learn more.





FEDERAL TRADE COMMISSION

IdentityTheft.gov

Is someone using your personal information to open new accounts, make purchases, or get a tax refund? Report it at **IdentityTheft.gov** and get a personal recovery plan.

What To Do Right Away

Step 1: Call the companies where you know fraud occurred.

- Call the fraud department. Explain that someone stole your identity.
- Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.
- Change logins, passwords and PINS for your accounts.

Step 2: Place a fraud alert, and get your credit reports.

- To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.

Equifax.com/CreditReportAssistance
1-888-766-0008

Experian.com/fraudalert
1-888-397-3742

TransUnion.com/fraud
1-800-680-7289

A fraud alert is free. It will make it harder for someone to open new accounts in your name.

You'll get a letter from each credit bureau. It will confirm that they placed a fraud alert on your file.

- Get a copy of your free credit reports from Equifax, Experian, and TransUnion. Go to **annualcreditreport.com** or call 1-877-322-8228.

Did you already order your free annual reports this year? If so, you can pay to get your report immediately. Or follow the instructions in the fraud alert confirmation letter from each credit bureau to get a free report. That might take longer.

- Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.



Step 3: Report identity theft to the FTC.

- Visit **IdentityTheft.gov** and click “Get Started.”
Or call 1-877-438-4338. Include as many details as possible.

Based on the information you enter, IdentityTheft.gov will create your **Identity Theft Affidavit** and **recovery plan**.

If you create an account, we’ll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

If you don’t create an account, you must print and save your Identity Theft Affidavit and recovery plan right away. Once you leave the page, you won’t be able to access or update them.

Step 4: File a report with your local police department.

- Go to your local police office with:
 - a copy of your FTC Identity Theft Affidavit
 - a government-issued ID with a photo
 - proof of your address (mortgage statement, rental agreement, or utilities bill)
 - any other proof you have of the theft (bills, IRS notices, etc.)
 - the FTC’s Memo to Law Enforcement (available at **IdentityTheft.gov**)
- Tell the police someone stole your identity and you need to file a report. If they are reluctant, show them the FTC’s Memo to Law Enforcement.
- Ask for a copy of the police report. You’ll need this to complete other steps.
- Create your Identity Theft Report by combining your FTC Identity Theft Affidavit with your police report.



Your identity theft report proves to businesses that someone stole your identity. It also guarantees you certain rights.

Go to **IdentityTheft.gov** for next steps.

Your next step might be closing accounts opened in your name, or reporting fraudulent charges to your credit card company. **IdentityTheft.gov** can help — no matter what your specific identity theft situation is.