SCAMS and Info

The following information on scams was taken directly from the FTC (www.ftc.gov). See their website for more information.

SCAMS and Info addressed on this page:

1. IRS Calls
2. Computer Virus/Tech Support Calls
3. Phishing (fake e-mails/texts/calls)
4. Social Security Scams
5. Phony online car sales
6. Gift Card Scams targeting worshipers
7. Charity Scams
8. Imposter Scams
9. Grandkid Scams
10. Online Dating Scams
11. "You've Won" Scams
12. Home Repair Scams
13. Health Care Scams
14. Money Mule Scams
15. Work at Home Scams
16. Job Scams
17. Money Wiring Scams
18. Unwanted Calls
19. Scams Against Immigrants
20. Identity Theft
21. Recovering from Identity Theft
22. Fraud Alerts and Credit Freezes
23. Placing a Fraud Alert
24. Equifax Data Breach: Beware of Fake Settlement Websites

Those (not really) IRS calls (IRS Imposter Scam)

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.

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.

Keep tech support strangers out of your computer

If you need tech help with your computer, where do you go? Most of us probably search online. But your online search can lead you straight to scammers who scare you into thinking your computer is in dire need of repair...and then sell you costly security software that you don't need.

Or you get a pop-up or other urgent message from someone saying your computer is infected. It might seem like the message comes from a well-known company like Microsoft or Apple, or maybe your internet service provider. It tells you there are viruses or other malware on your computer. It says you have to call a number or risk losing your personal data.
But is this threat – or their problem – real? Judging by reports to the Federal Trade Commission, no they are not real. These are scammers who 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**. Stop.** Don't call a phone number or click a link. Don't send money, give your credit card number, or give control of your computer to anyone who contacts you.
2. **Pass this information on to a friend.** You might know these pop-ups are fake, but chances are you know someone who doesn't.

- If you're looking for tech support, go to a company you know and trust, or get help from a knowledgeable friend or family member. If you search online for help, search on the company name plus "scam," "review," or "complaint."
- If you get a phone call you didn't expect from someone who says there's a problem with your computer, hang up.
- **Never give control of your computer or your credit card information to someone who calls you out of the blue. Also do not write them checks or get them gift cards as payment.**
- Never call a number in a pop-up that warns you of computer problems. Real security warnings will never ask you to call a phone number.
- If you think there's a problem with your computer, update its security software and run a scan.

If you spot a tech support scam, tell the FTC: www.ftc.gov/complaint. And learn more at www.ftc.gov/techsupportscams.

Phishing: Don’t take the bait

Phishing is when someone uses fake emails or texts – even phone calls – to get you to share valuable personal information, like account numbers, Social Security numbers, or your login IDs and passwords. Scammers use this information to steal your money, your identity, or both. They may also try to get access to your computer or network. If you click on a link in one of these emails or texts, they can install ransomware or other programs that lock you out of your data and let them steal your personal information.

Scammers often use familiar company names or pretend to be someone you know. They pressure you to act now – or something bad will happen.

The FTC’s new infographic, developed with the American Bankers Association Foundation, offers tips to help you recognize the bait, avoid the hook, and report phishing scams.

Please share this information with your school or family, friends and co-workers.

Want to avoid the latest rip-offs? Sign up for free consumer alerts from the FTC at ftc.gov/subscribe.

Social Security Scams

Earlier this month, we told you about a growing scam: people pretend to be from the Social Security Administration (SSA) and try to get your Social Security number or your money. That scam is now growing exponentially. To compare: in 2017, we heard from 3,200 people about SSA imposter scams, and those people reported losing nearly $210,000. So far THIS year: more than **35,000 people have reported the scam**, and they tell us **they've lost $10 million**.

Scammers are saying your Social Security number (SSN) has been suspended because of suspicious activity, or because it's been involved in a crime. Sometimes, the scammer wants you to confirm your SSN to reactivate it. Sometimes, he'll say your bank account is about to be seized – but he'll tell you what to do to keep it safe. (Often, that involves putting your money on gift cards and giving him the codes – which, of course, means that your money is gone.)

Oh, and your caller ID often shows the real SSA phone number (1-800-772-1213) when these scammers call – but they're faking that number. It's not the real SSA calling.

Here's what to know:

- Your Social Security number is not about to be suspended. You don't have to verify your number to anyone who calls out of the blue. And your bank accounts are not about to be seized.
- SSA will never call to threaten your benefits or tell you to wire money, send cash, or put money on gift cards. Anyone who tells you to do those things is a scammer. Every time.
- The real SSA number is 1-800-772-1213, but scammers are putting that number in the caller ID. If you're worried about what the caller says, hang up and call 1-800-772-1213 to speak to the real SSA. Even if the wait time is long, confirm with the real SSA before responding to one of these calls.
- Never give any part of your Social Security number to anyone who contacts you. Or your bank account or credit card number.
- If you get a robocall, DO NOT PRESS 1. Instead just hang up and remember:
    - Your Social Security number is not about to be suspended.
    - The real Social Security Administration will never call to threaten your benefits.
    - The real SSA will never tell you to wire money, send cash, or put money on a gift card.

If you get one of these calls, tell the FTC at ftc.gov/complaint.

Put the brakes on phony online car sales

You can buy practically anything online, including used cars. But before you shell out any hard-earned cash, here's a warning about scammers trying to sell cars they don't have or own.

Here's how the scam works:

Criminals post ads on online auction and sales websites, like eBay Motors, for inexpensive used cars (that they don't really own). They offer to chat online, share photos, and answer questions. They may even tell you the sale will go through a well-known retailer's buyer protection program. Recently, sellers have been sending fake invoices that appear to come from eBay Motors and demanding payment in eBay gift cards. If you call the number on the invoice, the scammer pretends to work for eBay Motors. Trusting buyers have lost hundreds of thousands of dollars over the past year alone.

So how can you tell if an online car sale is fake?

- **You find bad reviews online.** Check out the seller by searching online for the person's name, phone number and email address, plus words like "review," "complaint" or "scam."
- **Sellers try to rush the sale**. Resist the pressure. Scammers use high-pressure sales tactics to get you to buy without thinking things through.
- **They can't or won't meet in person or let you inspect the car.** Scammers might have an excuse, like a job transfer, military deployment, or divorce, for why you can't see them or the car. But experts agree that you should have an independent mechanic inspect a used car before you buy it.
- **They want you to pay with gift cards or by wire transfer.** If anyone tells you to pay that way, it's a scam. Every time.
- **The sellers demand more money after the sale** for "shipping" or "transportation" costs.
- **The Vehicle Identification Number (VIN) doesn't match** the VIN for the car you're interested in. A vehicle history report can help you spot such discrepancies.

For more tips, check out ftc.gov/used cars and Online Auction Buyers. Want to avoid the latest rip-offs? Sign up for free consumer alerts from the FTC at ftc.gov/subscribe.

If you spot a scam, report it at ftc.gov/complaint.

Worshipers targeted by gift card scam

We're seeing a new spin on gift card scams. This time, scammers are pretending to be a pastor, rabbi, priest, imam, or bishop. They're asking worshipers for gift card contributions for a worthy cause. Appeals are often made by email, but we've heard people are also getting texts and phone calls, too.

The bogus emails often include the name of the local pastor and a legitimate looking email address. But a closer look should raise some red flags. For example, the email address isn't the one normally used by the church, and the service provider is different, too. The message may begin with a simple "Hi," but doesn't include a recipients' name. There also may be spelling errors, including the pastor's name.

The imposter asks you to buy a popular gift card — frequently, iTunes, Google Play, or Amazon — and then asks for the gift card number and PIN on the back of the card. Those numbers let the scammer immediately get the money you loaded onto the card. And once that's done, the scammer and your money are gone, usually without a trace.

If you or someone you know paid a scammer with a gift card, report it as soon as possible. Call the card company and tell them the gift card was used in a scam. Here is contact information for some of the gift card companies that scammers use most often.

Then, tell the FTC about it at ftc.gov/complaint. Your reports may help law enforcement agencies launch investigations that could stop imposters and other fraudsters in their tracks.

Report gift card scams

Amazon

- Call 1 (888) 280-4331
- Learn about Amazon gift card scams here.

Google Play

- Call 1 (855) 466-4438
- Report gift card scams online here.
- Learn about Google Play gift card scams here.

iTunes

- Call Apple Support at 1 (800) 275-2273, then say "gift card" to be connected to a live representative.
- Learn about iTunes gift card scams and how to report them here.

Steam

- If you have a Steam account, you can report gift card scams online here.
- Learn about Steam gift card scams here.

MoneyPak

- Call 1 (866) 795-7969
- Report a MoneyPak card scam online here.

Before giving to a Charity

You want your donations to count. That's why it's important to ask questions whenever you're asked to give — whether over the phone, in direct mail, or online. Do some research before donating. You should know, for example, exactly how much of your donation goes to the program you want to support. Don't donate until you're sure it will make a difference. Here are some things you can do to make sure your donations get where they'll do good — and help you avoid donating to a scam.

If you want to give to charity:

- Search online for the cause you care about — like "hurricane relief" or "homeless kids" — plus phrases like "best charity" or "highly rated charity." Once you find a specific charity you're considering giving to, search its name plus "complaint," "review," "rating," or "scam." If you find red flags, it might be best to find another organization.
- Check out the charity's website. Does it give information about the programs you want to support, or how it uses donations? How much of your donation will go directly to support the programs you care about? If you can't find detailed information about a charity's mission and programs, be suspicious.
- Use one of these organizations to help you research charities: BBB Wise Giving Alliance, Charity Navigator, CharityWatch, and GuideStar.
- See what your state's charity regulator has to say about the charity. Don't know who that is? Look it up at nasconet.org.
- Before you donate through an online portal that lets you choose from a list of charities, read the article *Donating Through an Online Giving Portal*, available at FTC.gov/Charity. It explains how these online giving portals work.

If you get a call from a fundraiser:

- You don't have to give over the phone. Don't let any caller pressure you. A legitimate charity will be happy to get your donation at any time, so there's no rush. Take time to do the research.
- Ask the fundraiser for the charity's exact name, web address, and mailing address, so you can confirm it later. Some dishonest telemarketers use names that sound like large well-known charities to confuse you.
- Ask how much of your donation will go directly to the program you want to help. Then, call the organization directly and ask them, too, or see if the information is on their website. What else does the charity spend money on? Some fundraising can be very expensive, leaving the charity with little money to spend on its programs.
- Ask if your donation will be tax-deductible. Not every call seeking a donation is from a charity. Some calls might be from Political Action Committees or other groups where donations are not deductible. You can make sure that your donation is to a charity and tax-deductible by looking up the organization in the IRS's Tax Exempt Organization Search.
- Check to see if the fundraiser and charity are registered with your state's charity regulator (if that's required in your state).

Charity (continued page 2)

If you get a donation request through social media or a crowdfunding site:

- Keep in mind that crowdfunding sites often have little control over who uses them and how donations are spent. Research any charity before you give. Also, if tax deductions are important to you, remember that donations to individuals are not tax deductible.
- The safest way to give on social media or through crowdfunding is to donate to people you know who contact you about a specific project. Don't assume solicitations on social media or crowdfunding sites are legitimate, or that hyperlinks are accurate — even in posts that are shared or liked by your friends. Do your own research. Call your friends or contact them offline to ask them about the post they shared.
- You can always go directly to a charity's website and donate directly that way.

If you're ready to donate:

- Be careful how you pay. If someone asks you to pay by giving them the numbers from a gift card, or by wiring money, don't do it. That's how scammers ask you to pay. It's safest to pay by credit card or check — and only after you have done some research on the charity.
- If someone wants you to leave your donation in cash under your doormat, be suspicious. You're probably dealing with a scammer.

After you've donated:

- Review your bank account and credit card statements closely to make sure you're only charged the amount you agreed to donate — and that you're not signed up to make a recurring donation.
- It's a good practice to keep a record of all donations.

How to avoid donating to a sham charity:

- Don't let anyone rush you into making a donation. That's something scammers do.
- Don't feel pressured to donate. Scammers will say anything to get you to give them money. They may say you already pledged to make the donation, or that you donated to them last year. They may even send you a mailer that says you already pledged. Don't let that pressure you into paying what could be a scammer.
- Don't trust your caller ID. Technology makes it easy for scammers to have caller ID say the call comes from anywhere, including your local area code, or from a particular name. In reality, the caller could be anywhere in the world. If you want your donation to help your local community,

Charity (continued page 3)

- ask questions about where your donation will be used and how much of your donation will be spent there.
- Check out the name of the charity, especially if it sounds like a well-known organization. Some scammers use names that sound a lot like other charities to trick you.
- Watch out for solicitations that give lots of vague and sentimental claims, but give you no specifics about how your donation will be used.
- If someone is guaranteeing you sweepstakes winnings in exchange for a contribution, that's a scam.

How to handle calls from telemarketers:

Even if your number is on the National Do Not Call Registry, the Telemarketing Sales Rule lets fundraisers asking for charitable solicitations to call you until you tell them to stop. To do that, ask to be placed on the charity's do not call list.

Fundraisers who call you have to follow other rules too:

- They can't call you before 8 a.m. or after 9 p.m.
- They have to tell you the name of the charity they're calling for and tell you if the purpose of the call is to seek a donation.
- They can't deceive you or lie about:
    - The fundraiser's connection to the charity.
    - The mission or purpose of the charity.
    - Whether a donation is tax deductible.
    - How a donation will be used, or how much of the donation actually goes to the charity's programs.
    - The charity's affiliation with the government.
- They can't use a robocall or prerecorded message to reach you unless you have supported the charity in the past.
- The caller ID on your phone has to show the name of the charity or fundraiser, along with a number that you can call to ask to be placed on the charity's do not call list.

If a fundraiser breaks any of these rules, that's a red flag. Do some more research before you donate to them. If you think you've been contacted by a scam charity, or a fundraiser that is not following the rules, please tell the FTC: FTC.gov/Complaint. It's most helpful to tell the FTC the name of the charity or fundraiser and why you think it was a scam.

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.

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.

Grandkid Scams

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.** 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.

Please Report Scams

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

- Report a scam online
- or call the FTC at 1-877-FTC-HELP

(1-877-382-4357) or TTY 1-866-653-4261.

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, 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. 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.

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.

“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.

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 scammers and stop them before they can get someone’s hard-earned money. It really makes a difference.

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.

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 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

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.

Please Report Scams

If you spot a health care 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 scam artists and stop them before they can access to a friend's hard-earned money. It really makes a difference.

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.

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 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.

Work at Home Scams

Here's how they work:

You see an ad saying you can earn big money at home. Or one that offers help starting an online business – with a proven system to make money online. Or maybe your resume is on a job search website and someone calls: they want your driver's license and bank account numbers before they interview you.

What happens next?

If you answer the ad to work from home, they'll ask you for money for training or special access. But there'll be no job. If you buy that "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 that caller your driver's license and bank account numbers, they might steal your identity or your money.

Here's what you can 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.

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 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.

Job Scams

Scammers might promise you a job, lots of money, or work you can do at home. But they make you pay them before they help you. If you pay them, you will lose your money and will not get a job.

How do I spot a job scam? Look for these signs of a scam. Scammers might:

- promise you a job
- promise you a government job
- offer you the secret to getting a job
- promise that you will make lots of money by working at home
- offer you a certificate to improve your chances of getting a job

Scammers always will ask you to pay first. That is the biggest sign of any scam. Never pay in advance. Someone might say you cannot lose. It is not true. You will lose money.

How can I avoid a job scam?

- Never deal with anyone who promises you a job. No one can promise you a job.
- Do not pay in advance for information about a job. Even if there is a money-back guarantee.
- Do not deal with anyone who says you have to act fast.
- Ignore promises to make thousands of dollars working in your own home. Those promises are lies.

What if I already paid someone but I did not get anything?

If you sent money and did not get help finding a job, report it to the Federal Trade Commission (FTC).

- Call the FTC at 1-877-382-4357
- Go online: ftc.gov/complaint

The FTC uses complaints to build cases against scammers. Any information you can give helps investigators.

Money Wiring Scams

Wiring money is like sending cash. Do not wire money to people you do not know.

How do I spot a money wiring scam?

Most money wiring scams look like this:

- Someone you do not know asks you to wire money.

A scammer might use different ways to convince you to wire money. The scammer might say:

- you won a prize, or inherited money, but you have to pay fees first.
- you won the lottery, but you have to pay some taxes first.
- a friend or family member is in trouble and needs you to send money to help.
- you need to pay for something you just bought online before they send it.
- you got a check for too much money and need to send back the extra.

These are all tricks. When you hear stories like these, you have spotted a money wiring scam.

How do I avoid a money wiring scam?

Scammers are good at being friendly. They are also good at fooling people. Here is how you can stop a scammer:

- Never wire money to someone you do not know.
- Never wire money because someone contacted you:
    - even if you feel like you know the person
    - even if the person says he is your friend or related to you

What if I already wired money to someone?

If you sent money to someone who contacted you, report it to the Federal Trade Commission (FTC).

- Call the FTC at 1-877-382-4357
- Go online: ftc.gov/complaint

The FTC uses complaints to build cases against scammers. Any information you can give helps investigators.

Unwanted Calls

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. It's frustrating, and you just want it to stop.

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 sales calls — live or recorded. But scammers ignore the rules about when and how they can call you.

Scammers can use technology to make their calls look like they come from anywhere: the IRS, a business you know, a neighbor, or even your own number. Because phone numbers can be faked, you can't trust your caller ID. So now what?

Here's what you can do:

1. **Hang up. Don't press a number.** Just hang up the phone on unwanted calls. Consider call-blocking services to reduce the number of unwanted calls you get. Ask your phone carrier about call blocking and 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, but chances are you know someone who doesn't.

Please Report Scams

If you get scam calls or illegal robocalls, please report them 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 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.

Scams Against Immigrants

There are scams that target people who are trying to immigrate to the U.S. You can lose money in those scams. These scams also can hurt your chance to immigrate. Learn how to avoid a scam.

How can I avoid scams in the immigration process?

- Do not go to a notario, notario público, or a notary public for legal advice. In the U.S., notarios are not lawyers. They cannot give you legal advice.
- Never pay for government forms from the U.S. government. Government forms are free.
- Get immigration information from U.S. government websites. You might see a website that looks like it is from the government. Make sure that the website address includes .gov. That means the website is from the U.S. government.

What else can I do to protect myself?

- Never sign a form that is blank. Never sign a form that has false information in it.
- Do not let anyone keep your original documents, like your passport or birth certificate.
- Keep a copy of every document you turn in. Keep a copy of every letter you get from the U.S. government.
- You will get a receipt when you turn in your forms. The United States Citizenship and Immigration Service (USCIS) will give it to you. Keep the receipt. You will need it to check on your application.

How can I get help with immigration?

Immigration can be complicated. It can feel frustrating until you find the right kind of help.

- Get free immigration forms: at visit uscis.gov/forms or by calling USCIS at 1-800-870-3676
- Learn who can help you and where to find help:
- Order the free brochure from the Federal Trade Commission (FTC), *I Need Immigration Help. Who Can Help Me?*
- find the brochure online at ftc.gov/immigration
- call the FTC at 1-877-382-4357 to get a free copy sent to you

What if I paid someone who did not help me?

Immigration scams are illegal. Report what happened to the Federal Trade Commission (FTC).

- Call the FTC at 1-877-382-4357
- Go online: ftc.gov/complaint

The FTC uses complaints to build cases against scammers. Any information you can give helps investigators.

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.

Please Report Scams

If you spot a scam, 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.

Recovering from Identity Theft

If someone stole your identity, act fast. Acting fast can help reduce the damage identity theft can cause.

What should I do if someone steals my identity?

- First, call the companies where you know fraud happened.
    - Explain that someone stole your identity.
    - Ask them to close or freeze your accounts.
- Then change your password or personal identification number (PIN). Then visit IdentityTheft.gov or call 1-877-438-4338.
- Answer questions about what happened to you.
- Get a recovery plan that's just for you.
    - You can create an account on the website.
        - The account helps you with recovery steps.
        - The account also helps you tracks your progress.

What happens when I get my recovery plan?

You will want to call one of the credit bureaus. Ask the credit bureau for an initial fraud alert. It is free and lasts for 90 days. The fraud alert makes it harder for thieves to open accounts in your name. That credit bureau has to tell the other two.

Then you can ask all three credit bureaus for a credit report. If someone stole your identity, your credit report is free. Look at your credit report for things you do not recognize.

Fraud Alerts and Credit Freezes

UPDATE: As of September 21, 2018, the law says credit freezes are free for everyone, and alerts now last one year (not 90 days). Read more here.

What is a credit freeze?

Also known as a security freeze, this free tool lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

Does a credit freeze affect my credit score?

No. A credit freeze does not affect your credit score.
A credit freeze also does not:

- prevent you from getting your free annual credit report
- keep you from opening a new account. But to open one, you'll need to lift the freeze temporarily. It's free to lift the freeze and free to place it again when you're done accessing your credit.
- keep you from applying for a job, renting an apartment, or buying insurance. The freeze doesn't apply to these actions so you don't need to lift it.
- prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Does a credit freeze stop prescreened credit offers?

No. If you want to stop getting prescreened offers of credit, call 888-5OPTOUT (888-567-8688) or go online. The phone number and website are operated by the nationwide credit bureaus. You can opt out for five years or permanently. However, some companies send offers that are not based on prescreening, and your federal opt-out right will not stop those kinds of solicitations.

As you consider opting out, you should know that prescreened offers can provide many benefits, especially if you are in the market for a credit card or insurance. Prescreened offers can help you learn about what's available, compare costs, and find the best product for your needs. Because you are pre-selected to receive the offer, you can be turned down only under limited circumstances. The terms of prescreened offers also may be more favorable than those that are available to the general public. In fact, some credit card or insurance products may be available only through prescreened offers.

Can anyone see my credit report if it is frozen?

Certain entities still will have access to it.

- your report can be released to your existing creditors or to debt collectors acting on their behalf.
- government agencies may have access in response to a court or administrative order, a subpoena, or a search warrant.

How do I place a freeze on my credit reports?

Contact each of the nationwide credit bureaus:

Fraud Alerts and Credit Freezes (continued page 2)

Equifax
Equifax.com/personal/credit-report-services
800-685-1111
Experian
Experian.com/help
888-EXPERIAN (888-397-3742)
Transunion
TransUnion.com/credit-help
888-909-8872

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze?

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

What's the difference between a credit freeze and a fraud alert?

A credit freeze locks down your credit. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. For example, if you provide a telephone number, the business must call you to verify whether you are the person making the credit request. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Three types of fraud alerts are available:

Fraud Alert. If you're concerned about identity theft, but haven't yet become a victim, this fraud alert will protect your credit from unverified access for one year. You may want to place a fraud alert on your file if your wallet, Social Security card, or other personal, financial or account information is lost or stolen.

Extended Fraud Alert. For victims of identity theft, an extended fraud alert will protect your credit for seven years.

Active Duty Military Alert. For those in the military who want to protect their credit while deployed, this fraud alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. Also see "Placing a Fraud Alert".

Placing a Fraud Alert

A fraud alert can make it harder for an identity thief to open more accounts in your name. You can place a fraud alert by asking one of the three nationwide credit bureaus. It has to put the alert on your credit report and tell the other two credit bureaus to do so. The alert lasts one year.

Why Place a Fraud Alert

Three nationwide credit bureaus keep records of your credit history. If someone has misused your personal information – or even if you're concerned about identity theft, but haven't yet become a victim – you can place a fraud alert. For example, you may want to place a fraud alert if your wallet, Social Security card, or other personal, financial or account information is lost or stolen. You also may want to place a fraud alert if your personal information was exposed in a data breach. A fraud alert is free. The credit bureau you contact must tell the other two about your alert.

A fraud alert can make it harder for an identity thief to open more accounts in your name. When you have an alert on your report, a business must verify your identity before it issues credit, so it may try to contact you. The alert stays on your report for one year. You can get a new one after one year. It allows you to order one free copy of your credit report from each of the three credit bureaus. Be sure the credit bureaus have your current contact information so they can get in touch with you.

How to Place a Fraud Alert

1. **Contact one credit bureau.**
    - Ask it to put a fraud alert on your credit report.
    - The credit bureau you contact will then contact the other two credit bureaus. Placing a fraud alert
    - Be sure the credit bureaus have your current contact information so they can get in touch with you.
2. **The credit bureau will explain that you can get a free credit report and other rights you have.**
3. **Mark your calendar.**
   The fraud alert stays on your report for one year. You can get a new one after one year.

Credit Bureau Contact Information

Contact the national credit bureaus to request fraud alerts, credit freezes (also known as security freezes), and opt outs from pre-screened credit offers.

Equifax
Equifax.com/personal/credit-report-services
800-685-1111

Experian
Experian.com/help
888-EXPERIAN (888-397-3742)

Transunion
TransUnion.com/credit-help
888-909-8872

Equifax Data Breach: Beware of Fake Settlement Websites

You may go to the www.ftc.gov/Equifax to find out if your information, like your Social Security Number, was exposed in the September 2017 Equifax data breach. At that same website, you can also start a claim for benefits available under the settlement that the FTC and others reached with Equifax.

But, wouldn't you know it? People may have already started putting up **fake websites** meant to look like the official Equifax settlement claims website. To be sure you're going to the right place, **start at the FTC's page: ftc.gov/Equifax.**

A couple more things to remember:

- You'll never have to pay to file a claim for these benefits.
- And anyone who calls and tries to get you to file a claim is almost certainly a scammer.