

Scams

Advance Fee Scams: Scammers may promise you some kind of benefit: a loan, a prize like a foreign lottery, a government grant, an inheritance, an opportunity to work from home, or more. The catch is, they want payment up front before you can receive your benefit. Sometimes they will ask for a payment by wire transfer, online payment, or even gift cards. Stop and think – why are you having to pay to receive this benefit? Are you being asked by a source you know and trust? Do your research to avoid these scam artists!

Tech Support Scams: Out of nowhere, you receive a call or a screen pops up on your computer – maybe from a reputable company like Microsoft or an anti-virus company. They tell you that you have a virus or an error, and they can fix it before you lose all of your data. But first, you have to call the number on your screen allow them access to your computer, and/or pay them a sum of money. Sometimes they will use a “scan” of your computer to try to convince you there is something wrong. **Don’t believe them!**

Don’t give access to your computer! If you do, the scammer can look on your computer for your personal or financial information, or add malware that really will infect your computer, or add spyware so they can get your information in the future.

Instead, you can try exiting the internet, restarting your computer, or manually pressing the “off” button. Or try contacting a reputable source for help. Be careful though when searching for businesses on the internet – sometimes illegitimate services have paid for ads that might lead you to think they are the real thing!

Remember: real tech support or other computer companies don’t just contact you out of the blue.

Phishing Scams: If someone calls, texts, emails, or mails you asking for your personal information—e.g., social security number, credit card number, bank account info, passwords—**DO NOT GIVE IT TO THEM.** Even if they appear to be a known company or claim to be from a trusted source, they may be scamming you in order to steal your identity or money. This is known as phishing. Make sure to carefully consider whether the link you have been sent is authentic. You may want to independently reach out to the business or agency on your own terms using a known phone or website instead of accepting the unsolicited contact. Most legitimate companies will not contact you this way asking for personal information.

Emergency Scams: Sometimes called Grandparent Scams, these scams involve calls or emails from someone claiming to be your friend or family member in dire need. They are trying to prey on your emotions by inventing a situation that you must respond to immediately – with your money. They convince you by disguising their voice, showing a familiar phone number on your caller ID using a practice called “spoofing”, and using information available on the Internet. For instance, they say they may sound different because they are crying, sick, or injured. They reference specific names of family members or locations to make their story seem plausible. Then, they try to keep you from confirming their story by begging you not to tell anyone since they are embarrassed or scared in their situation.

Stop and think: no matter how dire the situation is, you can wait a few minutes before giving away your money. To confirm they are who they say, consider asking specific personal questions that would be difficult to know from the Internet or social media about you or your family. Or even better, use contact information you know for that person to reach out to them separately to confirm the story, or that of their family members.

IRS or Government Imposter Scams: An IRS agent contacts you and tells you that you owe back taxes and must pay immediately. If you don't, they say they will have the police come and send you to jail. There are variations of this scam, such as local law enforcement contacting you with a warrant because you missed jury duty, but almost always you will be asked to pay immediately via wire transfer or even gift cards, and will be told to stay on the phone throughout the entire payment process (including driving to the store!). Or you may be asked for your personal information to confirm your innocence or to receive a tax refund. Do not fall for it! Most likely you are not communicating with a government agent.

If you think you really may owe on your taxes, go to the official IRS website to find a real IRS phone number to contact to confirm. You probably would have received letters from them first if you really owe money. Also, the IRS won't immediately send you to jail – there would be a process you would be aware of prior to any criminal punishment.

Counterfeit Cashier's Checks: This may also be called an “*overpayment scam*.” It looks like the real thing: A cashier's check drawn on a familiar bank is as good as gold, right? Wrong. The counterfeit checks in circulation today are high-quality forgeries. They might even fool your bank at first. You are asked to deposit their cashier's check into your bank, keep some of the funds, and wire back the rest of the payment you owe – for a job, sweepstakes fees, online transaction, or more. Sometimes the excuse is they “accidentally” paid you too much and so need a refund.

Counterfeit cashier's checks can be used in combination with many of the other scams on this page where the victim is skeptical that there really is a pot of money to be gained. Always beware of large cashier's checks from strangers. The victim who deposits the forged check could be charged with a crime. It happens!

Bogus Debts: You receive a threatening letter that demands payment on a debt you've never heard of. Don't pay it! Scammers will demand payment on fake debts because a few people will be scared into paying. Real, legitimate creditors will be able to produce proof that a debt exists in the first place. If the debt is real and you weren't aware of it, you may be the victim of identity theft.

Home repair Scams: Beware of unsolicited door-to-door home improvement offers. If it is a one-time offer—"available only today!"—or a special deal on materials left over from another job, be very cautious. If your home needs repairs, your best bet is to call a few home repair companies in your area and then check their references.

Business Opportunities or Employment Scams: Jobs that require you pay upfront for training or equipment, or send you checks to deposit, are often scams — especially if you don't have any independent information on the company. See the above counterfeit check scams and be suspicious if you are “accidentally” overpaid and then asked to send or wire the difference back to the company. Here's a tip: If the job is easy to get, such as if you didn't even have a legitimate interview, pays extremely well and requires very little work ("In the comfort of your own home!"), you should be suspicious. It's probably too good to be true.

Shopping Sprees: You get a phone call, offering you a "\$500 shopping spree" (or other amount). They say they're from a well-known company or a government agency. Then, the caller asks for your bank account number in order to collect a small fee. They say the fee is for shipping and handling of your vouchers. It's a scam! Never disclose financial information to unsolicited callers *for any reason whatsoever*. Shopping spree promotions are usually fake.

5 Signs of a Scam

If you spot any of these tactics, stop and walk away. You're probably being scammed.

1. *They contacted you*

When you contact a business, you know who's on the other end of the line. But when someone contacts *you* first, you can't be certain they're telling the truth. You don't know if they are whom they say they are. And remember, email addresses and caller ID information can be faked.

2. **They dangle bait—usually money**

Let's face it: People simply don't give away large sums of money easily. If someone dangles bait in front of you—a big prize, a shopping spree, an easy loan — for nothing, they're probably lying.

3. **They want your personal information**

Anytime *anyone* asks for your personal information — bank accounts, social security number, etc. — you should be on alert. Don't give it away quickly or easily, especially to someone you don't know. You may become a victim of [identity theft](#).

4. **You have to pay them first**

If someone offers you a [prize](#), [debt relief](#), or employment — but first you have to pay an [upfront fee](#) to get it —you're probably being scammed.

5. **You have to wire money or send gift cards**

If you're about to [wire money or send gift cards](#) to someone in order to receive a prize, or pay off a debt collector that contacts you ... **STOP!** This may be a scammer trying to take your money.

Don't Scam the Scammer

Trying to scam your scammer — to get "revenge" — is a terrible idea. Don't do it. You won't fool them, and you may end up getting scammed after all.

If you feel you're the subject of a scam, simply cut off communication and go to the [ftc.gov](https://www.ftc.gov) website and contact your local law enforcement.