

From telemarketing scams to stealing personal information over the internet, there are many ways that your money and identity can be stolen. While the Federal Trade Commission is in charge of fighting these scams, as a Member of Congress, I can share valuable information with you to help you from becoming a victim of fraud. Please use these resources, and always think twice before sharing your personal information.

Below is a list of top ten ways to protect against fraud (courtesy of the Federal Trade Commission). You can also use one the links below to learn more about specific scams that are commonly used by criminals.

[If you think you have been a victim of fraud, you can file a complaint by click here.](#)

[If you'd like to register on the Do Not Call Registry, click here.](#)

More information about specific types of fraud

[Identity Theft & Telemarketing](#)

[Credit & Loan Offers](#)

[Charities & Fundraising Fraud](#)

[Buying Club Memberships](#)

[Government Grant Scams](#)

[Medical Discount Plans](#)

[Reloading Scams](#)

[Robocalls](#)

[Sweepstakes & Lotteries](#)

[Travel Scams](#)

[Work-at-Home & Business Opportunities](#)

Top Ten Ways to Protect Against Fraud

1. Keep in mind that wiring money is like sending cash: the sender has no protections against loss. Con artists often insist that people wire money, especially overseas, because it's nearly impossible to reverse the transaction or trace the money. Don't wire money to strangers, to sellers who insist on wire transfers for payment, or to someone who claims to be a relative in an emergency (and wants to keep the request a secret).

2. Don't send money to someone you don't know. That includes an online merchant you've never heard of — or an online love interest who asks for money or favors. It's best to do business with sites you know and trust. If you buy items through an online auction, consider a payment option that provides protection, like a credit card. Don't send cash or use a wire transfer service.

3. Don't respond to messages that ask for your personal or financial information, whether the message comes as an email, a phone call, a text message, or an ad. Don't click on links in the message, or call phone numbers that are left on your answering machine, either. The crooks behind these messages are trying to trick you into giving up your personal information. If you get a message and are concerned about your account status, call the number on your credit or debit card — or your statement — and check it out.

4. Don't play a foreign lottery. First, it's easy to be tempted by messages that boast enticing odds in a foreign lottery, or messages that claim you've already won. Inevitably, you'll be asked to pay "taxes," "fees," or "customs duties" to collect your prize. If you send money, you won't get it back, regardless of the promises. Second, it's illegal to play foreign lotteries.

5. Don't agree to deposit a check from someone you don't know and then wire money back, no matter how convincing the story. By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. You are responsible for the checks you deposit: When a check turns out to be a fake, it's you who is responsible for paying back the bank.

6. Read your bills and monthly statements regularly—on paper and online. Scammers steal account information and then run up charges or commit crimes in your name. Dishonest merchants sometimes bill you for monthly "membership fees" and other goods or services you didn't authorize. If you see charges you don't recognize or didn't okay, contact your bank, card issuer, or other creditor immediately.

7. In the wake of a natural disaster or another crisis, give to established charities rather than one that seems to have sprung up overnight. Pop-up charities probably don't have the infrastructure to get help to the affected areas or people, and they could be collecting the money to finance illegal activity. Check out [ftc.gov/charityfraud](https://www.ftc.gov/charityfraud) to learn more.

8. Talk to your doctor before buying health products or signing up for medical treatments. Ask about research that supports a product's claims—and possible risks or side effects. Buy prescription drugs only from licensed U.S. pharmacies. Otherwise, you could end up with products that are fake, expired or mislabeled — in short, products that could be dangerous. Visit ftc.gov/health for more information.

9. Remember there's no such thing as a sure thing. If someone contacts you promoting low-risk, high-return investment opportunities, stay away. When you hear pitches that insist you act now, guarantees of big profits, promises of little or no financial risk, or demands that you send cash immediately, report them to the FTC. For more information about investment fraud, visit cftc.gov.

10. Know where an offer comes from and who you're dealing with. Try to find a seller's physical address (not just a P.O. Box) and phone number. With VoIP and other web-based technologies, it's tough to tell where someone is calling from. Do an internet search for the company name and website and look for negative reviews. Check them out with the Better Business Bureau at bbb.org.

PUBLISHED APRIL 25, 2012