Scam artists in the U.S. and around the world defraud millions of people each year. They use the phone, email, postal mail, and the internet to trick you into sending money or giving out personal information.

Here are 10 things you can do — or not — to stop a scam.

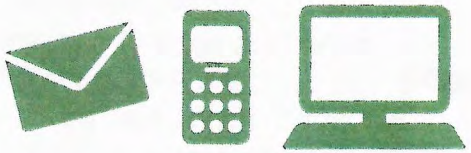
Report Scams

If you think you may have been scammed:

- File a complaint with the Federal Trade Commission at ftc.gov. If you are outside the U.S., file a complaint at econsumer.gov
- Visit ftc.gov/idtheft, where you'll find out how to minimize your risk of identity theft.
- Report scams to your state Attorney General. Visit naag.org.
- If you get unsolicited email offers or spam, send the messages to spam@uce.gov.
- If you get what looks like lottery material from a foreign country through the postal mail, take it to your local postmaster.

FEDERAL TRADE COMMISSION
August 2012

10 Ways to Avoid Fraud



FEDERAL TRADE COMMISSION

1 **Know who you're dealing with.** Try to find a seller's physical address (not a P.O. Box) and phone number. With internet phone services and other web-based technologies, it's tough to tell where someone is calling from. Do an online search for the company name and website, and look for reviews. If people report negative experiences, you'll have to decide if the offer is worth the risk. After all, a deal is good only if you get a product that actually works as promised.

2 **Know that wiring money is like sending cash.** 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 anyone who claims to be a relative or friend in an emergency and wants to keep the request a secret.

3 **Read your monthly statements.** Scammers steal account information and then run up charges or commit crimes in your name. Dishonest merchants bill you for monthly "membership fees" and other goods or services without your authorization. If you see charges you don't recognize or didn't okay, contact your bank, card issuer, or other creditor immediately.

4 **After a disaster, give only to established charities.** In the aftermath of a disaster, give to an established charity, rather than one that has 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. For more donating tips, check out consumer.ftc.gov.

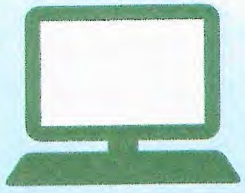
5 **Talk to your doctor before you buy health products or treatments.** Ask about research that supports a product's claims — and possible risks or side effects. In addition, buy prescription drugs only from licensed U.S. pharmacies. Otherwise, you could end up with products that are fake, expired, or mislabeled — in short, products that could be dangerous to your health. Learn more about buying health products online at consumer.ftc.gov.

6 **Remember there's no sure thing in investing.** If someone contacts you with low-risk, high-return investment opportunities, stay away. When you hear pitches that insist you act now, that guarantee big profits, that promise little or no financial risk, or that demand that you send cash immediately, report them at ftc.gov.

7 **Don't send money to someone you don't know.** Not to an online seller you've never heard of — or an online love interest who asks for money. It's best to do business with sites you know and trust. If you buy items through an online auction, consider using a payment option that provides protection, like a credit card.

If you think you've found a good deal, but you aren't familiar with the company, check it out. Type the company or product name into your favorite search engine with terms like "review," "complaint," or "scam." See what comes up — on the first page of results as well as on the later pages. Never pay fees first for the promise of a big pay-off later — whether it's for a loan, a job, a grant or a so-called prize.

8 **Don't agree to deposit a check and wire money back.** By law, banks have to make funds from deposited checks available within days, but uncovering a fake check can take weeks. You're responsible for the checks you deposit: If a check turns out to be a fake, you're responsible for paying back the bank. No matter how convincing the story, someone who overpays with a check is almost certainly a scam artist.

9 **Don't reply to messages asking for personal or financial information.** It doesn't matter whether the message comes as an email, a phone call, a text message, or an ad. Don't click on links or call phone numbers included in the message, either. It's called phishing. The crooks behind these messages are trying to trick you into revealing sensitive information. If you got a message like this and you are concerned about your account status, call the number on your credit or debit card — or your statement — and check on it.

10 **Don't play a foreign lottery.** It's illegal to play a foreign lottery. And yet messages that tout your chances of winning a foreign lottery, or messages that claim you've already won, can be tempting. Inevitably, you have to pay "taxes," "fees," or "customs duties" to collect your prize. If you must send money to collect, you haven't won anything. And if you send any money, you will lose it. You won't get any money back, either, regardless of promises or guarantees.