

Avoiding Online Scams

What To Do

Know who you're dealing with.

Try to find a seller's physical address (not just 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 internet search for the company name and website, and look for negative reviews. If you find them, you'll have to decide if the offer is worth the risk. After all, it's only a good deal if you actually get a product that works.

Understand 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 family friend in an emergency who wants to keep the request a secret.

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.

Give only to established charities after a disaster.

In the aftermath of a disaster, give to established charities, 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 [**ftc.gov/charityfraud**](https://www.ftc.gov/charityfraud).

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. 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**](#).

When investing, remember there's no sure thing.

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](https://www.ftc.gov).

What Not To Do

Don't send money to someone you don't know.

Not an online seller you've never heard of — nor 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 an 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, **do some research**. 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 now for the promise of a big pay-off later — whether it's for a loan, a job, or a so-called prize.

Don't agree to deposit a check and wire money back.

No matter how convincing the story. 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.

Don't reply to messages asking for personal or financial information.

That goes 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.

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 so tempting. Inevitably, you're asked to pay "taxes," "fees," or "customs duties" to collect your prize. If you send money to collect, you haven't won anything. Indeed, you've lost whatever money you sent. You won't get any money back, either, regardless of the promises.

Report Online Scams

If you think you may have been scammed:

- File a complaint with the **Federal Trade Commission**. If you are outside the U.S., file a complaint at **econsumer.gov**. Complaints are entered into the Consumer Sentinel Network, an online database used by hundreds of law enforcement agencies in the U.S. and abroad.
- Visit **ftc.gov/idtheft**, where you'll find out how to minimize your risk of identity theft.
- Report scams to your **state Attorney General**.

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, give it to your local postmaster.

Where to Learn More

U.S. Federal Trade Commission — The FTC works to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or get free information on consumer issues, visit **ftc.gov** or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a video, **How to File a Complaint**, at **ftc.gov/video** to learn more. The FTC enters consumer complaints into the **Consumer Sentinel Network**, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

The Internet Crime Complaint Center – IC3 was established as a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. Visit **www.ic3.gov**.

U.S. Department of State — The Department of State's mission is to create a more secure, democratic, and prosperous world for the benefit of the American people and the international community. As part of that mission, the Department of State seeks to minimize the impact of international crime, including cross-border internet scams, on the United States and its citizens. To get free information, visit **www.state.gov**.