



[Home](#) > [Latest News](#) > BBB Tip: 10 steps to avoid scams

BBB Tip: 10 steps to avoid scams

By [Better Business Bureau](#). June 21, 2024.

Share



(Getty Images)

There are thousands of new scams every year, and it can be challenging to keep up with them all!

However, if you can just remember these ten tips, you will be able to avoid most scams while protecting yourself and your family.

1. Never send money via gift card or wire transfer to someone you have never met face-to-face. Seriously, just don't ever do it. If they ask you to use a wire transfer, a prepaid debit card, or a [gift card](#); those cannot be traced and are as good as cash. Chances are, you won't see your money again. See the [Federal Trade Commission's video on how scammers try to convince you to pay](#). If someone is trying to convince you to pay this way, stop, get off the phone or the computer, and [file a](#)

[complaint with the Federal Trade Commission \(FTC\)](#). Report the activity to [BBB Scam Tracker](#). Check out the [BBB tip for avoiding online purchase scams](#).

2. Avoid clicking on links or opening attachments in unsolicited emails. Links, if clicked, will download malware onto your computer, smartphone, tablet, or whatever electronic device you're using at the time, allowing cyber thieves to steal your identity. Be cautious even with an email that looks familiar; it could be fake. Instead, delete it if it looks unfamiliar and block the sender. Take a look at the [BBB tip for how to spot a scam email](#).

3. Don't believe everything you see. Scammers are great at mimicking official seals, fonts, and other details. Just because a website or email looks official does not mean that it is. Caller ID is commonly faked. Learn more about [avoiding impostor scams](#).

4. Double-check that your online purchase is secure before checking out. Look for the "HTTPS" in the URL (the extra s is for "secure") and a small lock icon on the address bar. Better yet, before shopping on the website, make certain you are on the site you intended to visit. Check out the company first at [BBB.org](#). Read reviews about the quality of the merchandise, and make sure you are not buying cheap and/or counterfeit goods. Look for a brick-and-mortar address listing on the website itself and a working phone number. Take an extra step and call the number if it is a business you are not familiar with. Learn [how to identify a fake website](#).

5. Use extreme caution when dealing with anyone you've met online. Scammers use [dating websites](#), Craigslist, [social media](#), and many other sites to reach potential targets. They can quickly feel like a friend or even a romantic partner, but that is part of the con for you to trust them.

6. Never share personally identifiable information with someone who has contacted you unsolicited, whether it's over the phone, by email, on social media, or even at your front door. This includes banking and credit card information, your birthdate, and Social Security/Social Insurance numbers. Protect you and your family from [identity theft](#).

7. Resist the pressure to act immediately. Shady actors typically try to make you think something is scarce or a limited-time offer. They want to push victims to make a decision right now before even thinking through it, asking family members, friends, or financial advisors. Sometimes, they'll advise against contacting anyone and just trusting them. While high-pressure sales tactics are also used by some legitimate businesses, it typically isn't a good idea to make an important decision quickly. Know what to look for when [spotting a scam](#).

8. Use secure and traceable transactions. Do not pay by wire transfer, prepaid money card, [gift card](#), or another non-traditional payment method (see number one above). Say no to cash-only deals, high-pressure sales tactics, high upfront payments, overpayments, and handshake deals without a contract. Read all of the small print on the contract and make sure to understand what the terms are. Learn more about your [rights and responsibilities when it comes to payment types](#).

9. Whenever possible, work with local businesses. Ask that they have proper identification, licensing, and insurance, especially contractors who will be [coming into your home](#) or anyone dealing with your money or sensitive information. Review Business Profiles at [BBB.org](#) to see what other people have experienced. Research [BBB Accredited home improvement businesses and contractors](#) before making a final decision.

10. Be cautious about what you share on social media. Consider only connecting with people you already know. Check the privacy settings on all social media and online accounts. Imposters often [get information](#) about their targets from their online interactions and can make themselves sound

like a friend or a family member because they know so much about you. Then, update and change passwords to passphrases on a regular basis on all online accounts. Protect yourself from [fake social media accounts](#)

Learn how to [Spot A Scam](#).

Report any suspicious activities to [BBB Scam Tracker](#) and learn more about the different types of common scams on [BBB.org/scamtips](#).

[Sign up for Scam Alerts](#)

Read more about [BBB Accreditation Standards](#) and [BBB Standards for Trust](#).

Ad

**Look for it.
It's looking out for you.**



**THE SIGN OF A
BETTER
BUSINESS**

LEARN MORE

© 2025, International Association of Better Business Bureaus, Inc., separately incorporated Better Business Bureau organizations in the US and Canada, and BBB Institute for Marketplace Trust, Inc. All rights reserved. *In Canada, trademark(s) of the International Association of Better Business Bureaus, used under License.