SCAMS

There are thousands of new scams every year, and it's challenging to keep up with all of them. However, if you can just remember these ELEVEN TIPS, more than likely, 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 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. If you receive a call, stop, get off the phone or the computer, and file a complaint with the Federal Trade Commission (FTC.gov) and report the activity to BBB Scam Tracker (BBB.org).

2. **Avoid clicking on links or opening attachments in unsolicited emails.** Links, if clicked, will download malware onto your computer, smart phone, tablet or whatever electronic device you're using at the time allowing cyberthieves to steal your identity. Be cautious even with email that looks familiar; it could be fake. Instead, delete it if it looks unfamiliar and block the sender. Email by itself is harmless, but hackers use attachments and downloads to embed viruses on your computer. Links embedded within phishing messages direct you to fraudulent websites. **Do not reply to the sender**. Ignore any requests the sender may solicit and do not call phone numbers provided in the message. Report it.

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.

4**. Double check your online purchase is secure before checking out.** Look for the "https" in the URL (the extra s is for "secure") and look for 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.

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.

SCAMS

6. Hang **up the phone**. It is okay to hang up the phone or disconnect the conversation. Call the company back that you are dealing with and verify it is really them. Close the browser on your computer and even shut the computer down. Do not open any attachments or click on any links which may enable them to take control of your computer.

7**. Never share personally identifiable information** with someone who has contacted you unsolicited, whether it's over the phone, by email, on social media, and even at your front door. This includes banking and credit card information, your birthdate, and Social Security/Social Insurance numbers.

8**. Resist the pressure to act immediately.** Shady actors typically try to make you think something is scarce or is a limited time offer. They want to push victims to make a decision right now before you can think through it, or have time to ask family members, friends or a financial advisor. Sometimes, they'll advise you to avoid contacting anyone and to just trust 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 with anyone.

9. **Use secure and traceable transactions.** Do not pay by wire transfer, prepaid money cards, gift cards, or other non-traditional payment methods (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 the small print on the contract and make sure to understand what the terms are.

10. **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.

11**. 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 family member because they know so much about you. Then, update and change passwords to passphrases on a regular basis on all online accounts.

Report any suspicious activity to BBB.org/ScamTracker and learn more about the different types of common scams on BBB.org/scamtips. You can also sign up for Scam alerts.

SCAMS

How to Identify Spam

- Check for typos or strange phrasing. This can be indicative of a spam email…
- Check for strange or unfamiliar links. ...
- Check for context. ...
- Be wary of emails asking for personal information. ...
- Check to make sure the From and Reply To address match. ...
- Does it sound too good to be true? If so, it is a scam!
-

Five simple ways you can take to help eliminate spam emails.

- Mark as spam. ...
- Delete spam emails. ...
- Keep your email address private. ...
- Use a third-party spam filter. ...
- Change your email address. ...
- Unsubscribe from email lists.

www.BBB.org/ScamTracker - to report a scam and to access information on numerous scams.

www.AARP.org/Money/Scams-Fraud Fraud Resource Center. Call the Help Line if you suspect a scam 1-877-908-3360

The FTC collects complaints about hundreds of issues from **data security and false advertising to identity theft and Do Not Call violations**. These complaints are used to bring cases and share with law enforcement agencies worldwide for follow-up.
The Federal Trade Commission (FTC) is the main agency that collects scam reports. Report the scam to the FTC online, or by phone at 1-877-382-4357 (9:00 AM - 8:00 PM, ET)

The real FTC will never contact you and ask for money or for information like your Social Security, bank account, or credit card number. Scammers will impersonate your local sheriff's office or a court official.

(Information obtained from the BBB and FTC websites.)

"KEEP SAFE BY BEING PREPARED"

Revised April 2025