

11 red flags to help identify scams



1. You're contacted out of the blue.

Unsolicited phone calls should always be treated with caution. If you're in doubt, hang up, or better yet, don't answer. You shouldn't receive a call from tech support if you didn't initiate an interaction. The same goes for winning prizes or money—you can't win a sweepstakes or lottery you never entered.

2. It sounds too good to be true.

If it seems too good to be true, it probably is. If you're approached about a long-lost relative who left you money in their will, an investment with no risk or unusually high returns, or being awarded a loan or grant you don't remember applying for, it's probably a scam. These are the types of tactics scammers regularly use to get their hands on peoples' money and personal information.

3. There's a sense of urgency to act.

Scammers know fear works in their favor. They want you to panic and act quickly without taking time to ask questions, verify information and evaluate the situation with a clear head.

4. Threat tactics are used.

If you receive a phone call, email or text message from someone claiming to be with a government agency, law enforcement organization, utility company, financial institution or health care facility who says you'll face legal action, deportation, immediate disconnection of utilities or arrest if you don't immediately pay or provide your financial information, then you've likely been targeted by a scammer. Scammers use threats to cloud your judgment and prompt you to respond or act quickly.

5. Spelling and grammatical errors are made.

Be very suspicious of "official" documents with misspellings, poor grammar or logos that don't look legitimate. Real entities take time to proofread and review their correspondence. If scammers aren't well educated or don't speak English as their first language, they are likely to have several errors in their correspondence.

6. An upfront investment or payment is required.

Scammers often claim advanced payment of taxes or fees is needed to clear funds or release money you've "won." Never pay fees or taxes in advance, especially if you don't have clear documentation of what the payments are for. Legitimate sweepstakes or lotteries do not request any form of payment in advance to claim your winnings.

7. Untraceable payment methods are requested.

Scammers may avoid traditional banking methods to cover their tracks. They often direct consumers to provide payment in the form of wire transfers, prepaid debit cards, gift cards, cryptocurrency or even gold bars. Another tactic is to request the funds via applications like PayPal, Zelle, Venmo or others. They prefer methods that are nearly untraceable, so once the money is sent, it's gone for good.

8. You're required to provide personal information.

In rare circumstances, banks, government agencies and legitimate companies may ask you to provide personal information to verify your identity, but they generally don't call you to request this information. Scammers, on the other hand, may attempt to impersonate an entity to lure consumers into providing their private information so they can use it to commit fraud. Never provide your private information in response to an unsolicited call, email or text message. Instead, call the entity at a phone number found on its website, on the back of your credit or debit card, or on official correspondence like your monthly utility bill.

9. Pop-ups or links are used.

If you get a pop-up message to call tech support, even if it appears to be from a known company like Microsoft or Apple, ignore it. Some pop-up messages about computer issues are legitimate, but never call a number or click a link that appears in a pop-up message warning you of a computer problem or virus. Close the pop-up and contact tech support via a local or known, trusted channel. Do not give remote access to someone you didn't contact first. Don't share passwords or login information with anyone, not even tech support.

10. They refuse to let you see them.

If you meet a new friend or romantic interest online, take it slowly and ask questions. Watch for inconsistencies in information they share. Look for red flags such as promising to meet in person but later canceling or refusing to appear on camera. If they ask for money so they can visit you or pay for some other emergency—even if they offer to repay you—don't comply. Limit the amount of personal information you provide and talk to family and friends about the person to see if they have concerns.

11. They ask you to keep a secret.

Scammers often use secrecy to prevent you from getting a second opinion from trusted family, friends or other professionals, such as your Thrivent financial advisor, attorney or banker. By keeping things secret, scammers maintain power over you and make it harder to expose the scam. They might even imply that revealing the information could lead to negative consequences, which puts additional pressure on you to stay silent. Always check with someone you trust before acting—especially if it seems too good to be true!



If you think you are being scammed:

- Stop communicating with the scammer. Block their phone numbers and texts, and don't respond to their emails.
- Notify your bank, credit card companies and financial advisor. Consider a credit freeze with the three major credit bureaus: Equifax, TransUnion and Experian.
- Write down as many details as possible, such as the scammer's name, location, email address and phone number.
- Report the scam to:
 - o Your local police department or sheriff's office, especially if you lost money or property or had your identity compromised.
 - o The Federal Trade Commission (FTC) at 877-382-4357 or reportfraud.ftc.gov.
 - o The FBI's Internet Crime Complaint Center at ic3.gov.
 - o The National Elder Fraud Hotline at 833-372-8311.