

How to Avoid Scams

Don't fall for a fake

Imposters can come in all different forms, from banks, real estate and utility companies, to family members and government agencies. These fraudsters use pressure tactics to create a false sense of urgency. They may tell you they'll disconnect your electricity, you'll be arrested, or your account will be suspended if you don't act now.

If it sounds too good to be true, it probably is

Beware of anyone promising you unreasonably high returns, low risk and "golden" savings opportunities. Take the time to ask questions and be skeptical to help guard against getting scammed.

Monitor your accounts

Keep a close eye on your accounts, respond to fraud alerts, and report unauthorized transactions quickly. Consider placing a "freeze" on your data held at the big three credit bureaus so someone cannot open a new line of credit without your authorization.

Avoid grandparent scams

If someone claims to be a family member, verify with that family member by calling them directly. If you think your grandchild needs help, contact them directly, not by email, social media or text, or call their parents before sending money or gift cards unintentionally to a scammer.

Ensure the website is authentic

Beware of fraudulent websites that impersonate legitimate companies to take your money or information. Many of these websites look like the real thing, but you can protect yourself by researching the company, checking the website URL, and looking for typos or details that don't feel right. Don't call the phone number on a suspicious website, because you could be unknowingly calling the fraudster.

Watch for phishing

Pay attention to any email claiming to be a bill or a security alert. Delete the message if anything looks odd, such as: misspelled words, your name not appearing correctly, an unusual sender email address, links that don't go to the right place, or requests for you to "verify" personal information.