

Protect yourself from financial fraud

Key points

- **Financial fraud takes many forms.** Phishing, identity theft, investment scams, and account takeovers are among the most common threats targeting individuals today.
- **Slow down when something feels off.** Urgency, impersonation, and unusual payment requests are classic red flags — pause, verify, and consult your financial advisor before acting.
- **Simple habits offer strong protection.** Strong passwords, multifactor authentication, and regular account monitoring go a long way toward keeping your finances secure.
- **Guard your personal information carefully.** Only share personal details with trusted parties, shred sensitive documents, and secure your devices with strong passwords or biometric logins.
- **Act quickly if you suspect fraud.** Contact a trusted person right away, report to the FBI, FTC, or SEC, change your passwords, and place a fraud alert or credit freeze on your accounts.

Fraudsters are getting smarter, but you can stay a step ahead of them. Protecting your financial information is one of our top priorities. We can work with you to keep your financial information secure by helping you understand common fraud tactics and how to adopt simple habits like safeguarding your personal information, monitoring your accounts, and staying alert.

Here's what to watch for and how to better protect yourself against a range of schemes and scams. When in doubt, always take a moment to verify, and never hesitate to report concerns to your financial advisor.

What are common types of fraud?

Fraudsters use various tactics and schemes to take advantage of people. Below are common types of fraud. Becoming familiar with these schemes can lessen your vulnerability to cyber threats.

Phishing. Using fake emails, texts, or websites to attempt to steal sensitive information

Identity theft. Using personal details (like your name, birthdate, or address) without permission or knowledge to commit fraud, potentially leading to significant financial harm

Credit card fraud. Making unauthorized purchases or withdrawals using credit cards or credit card numbers — warning signs include missing cards, charges you don't recognize, or sudden credit score changes

Account takeover. Fraudulently accessing accounts (email, bank, social media) to carry out unauthorized actions, such as withdrawals, posts, and communications

Investment fraud. Using deceptive practices or schemes that promise unreasonably quick, high returns with little to no risk — examples include Ponzi schemes, fake real estate deals, fraudulent cryptocurrency pitches, investment fraud through social media, and promissory notes carrying false guarantees

Social engineering. Manipulating people into sharing personal information or performing actions, such as money transfers, that are used to commit fraud

How do you recognize fraudulent communications?

Fraudsters are using increasingly sophisticated methods that can be convincing and difficult to detect. They often pretend to be people or companies you know and trust. Know what to look for and follow the tips below to help identify if you're being targeted.

What to look for

- **Imposters.** Scammers often pretend to be someone you trust, like a government official, a family member, a charity, or a familiar company
- **Suspicious emails, calls, or messages.** Look for spelling mistakes, generic greetings, and unrecognized sender addresses or caller IDs. Be wary of requests to respond by WhatsApp, live chat, or a "Contact us" form
- **Sense of urgency or threats.** Be alert for urgent requests or threats (e.g., "your account will be locked"). Often, scammers rush their victims, speak quickly to create confusion, or attempt to gain trust to entice disclosure of personal information
- **Fake websites, attachments, or links.** Some fraudsters use fake or offshore websites or compromised email accounts to appear legitimate. In some cases, fraudsters use a valid email address or website URL that has no ties to a true operating business
- **Financial phone calls.** Scammers may cold call asking for money or personal information

If you encounter any of the above or other communications that raise red flags, pause. Give yourself a moment to think calmly and critically, then consider these suggestions for responding below.

What to do

- **Review emails carefully.** Reread the email to look for any misspellings or poor grammar. Don't act, send money, or give out personal information in response to an unexpected request — whether it comes as a text, a phone call, or an email
- **Move slowly and carefully.** Never let strangers force you into quick decisions. If you're uncertain, don't be afraid to hang up

- **Verify with someone you trust.** If you think the call, email, or message is fraudulent, try calling back using a number you know is genuine such as one printed on a bill or statement, reach out to a trusted contact such as your financial advisor, or contact law enforcement

Never let strangers force you into quick decisions. If you're uncertain, don't be afraid to hang up.

What can you do to prevent fraud?

Safeguarding your personal and financial information is one of the best defenses against fraud. Here are some tips and best practices for fraud prevention:

Staying safe online

- **Use strong and unique passwords.** Create long, complex, and unique passwords for each account
- **Monitor financial accounts.** Conduct a regular, if not daily, review of bank, brokerage, and credit card statements to help identify unusual or unauthorized activity in your accounts
- **Review credit reports.** Frequently review your credit reports for sudden changes in your credit score to identify any suspicious activity. The three major credit reporting bureaus — Experian, Equifax, TransUnion — allow you to check your credit report free once a week. Sign up for alerts with your banks and the credit bureaus to help spot any suspicious activity early
- **Check website URLs.** Use tools like Whois Domain Lookup to help verify a website's owner, as scammers often use typos to mimic legitimate sites
- **Use multifactor authentication.** Gain an extra layer of protection by using multifactor authentication to verify your identity when you log in to websites and applications
- **Review apps before downloading.** Check app ratings and reviews, and be wary of apps that ask you for access to your contacts, camera, or other parts of your phone when it's not clear why it's needed

Protecting personal information

- **Limit sharing personal details.** Only share personal information, including login credentials (e.g., usernames and passwords), with trusted entities
- **Shred documents.** Shred physical documents that contain personal information, such as bank statements, credit card offers, and tax records, once you've reviewed them
- **Secure devices.** Use strong and unique passwords, PINs, or biometric logins (like fingerprint or face recognition) to ensure that only you can access your device and accounts
- **Use encryption.** Send emails containing personal information using encryption tools to provide further protection
- **Stay updated.** Keep your software and security programs current so you have the most up-to-date protections

Guarding money movement and payments

- **Consider how you pay.** Government offices and legitimate companies will not require you to use payment methods like Western Union or MoneyGram nor will they request payment through iTunes, Amazon, or other gift cards
- **Do not pay up front to an unknown party.** Fraudsters generally ask for payment in advance of receiving a service, such as debt relief, a job, or a prize. Be aware — these are normally scams
- **Do not deposit a check and then wire money back.** Scammers may send you a fake check for more than you're owed and ask you to deposit it, then send back the extra money. Not only will you lose the money, but you'll be on the hook to pay any fees associated with the transaction

What can you do if you suspect fraud?

If you think you've been defrauded, follow these steps:

- **Immediately engage a trusted party for help.** Call someone that you trust — a friend, a family member, or your financial advisor — to help guide you on steps to increase your chances of recovering funds
- **File a report.** Filing a report can help stop the fraudster and prevent them from harming others. Consider filing a report with the following:
 - The FBI's [Internet Crime Complaint Center](#)
 - [Commodity Futures Trading Commission fraud reporting](#)
 - [Federal Trade Commission fraud reporting](#)
 - [Securities and Exchange Commission fraud reporting](#)
- **Change your passwords.** Update your passwords and turn on multifactor authentication
- **Notify credit agencies.** Place a fraud alert — or freeze your credit if appropriate
- **Continue monitoring.** Watch your accounts for any new issues

A final reminder

The threat of fraud can feel scary, but if you watch for the signs and check before you respond, you'll go a long way to thwarting fraudsters. Remember, if something feels off, pause and investigate further. Talk it over with someone you trust and verify the request. When in doubt, don't share or send personal information or money, and avoid clicking on unknown links. Your vigilance helps protect your finances — and also your peace of mind.

Call your financial advisor if you have any questions or concerns. We are here to support you and help protect your financial well-being.

About &Partners

&PartnersSM is the enterprise trade/marketing name for Ampersand Partners LLC, a Delaware limited liability holding company, and its subsidiary, &Partners LLC, a Tennessee limited liability company. Securities and advisory services offered through &Partners LLC, member [FINRA](#), [SIPC](#). Please see [FINRA's BrokerCheck](#) for information on our firm and representatives as well as these important [disclosures](#).

AndPartners_PreventingFraudWL_0727026 MR9048105.1.

© 2026 &Partners. All rights reserved.