Protect Yourself from the Next Internet Scam

July 15, 2026

Fraud has become one of the fastest-growing financial threats in America.

In 2024, consumers reported losing more than $12.5 billion to fraud, according to the Federal Trade Commission. In 2025, the FBI's Internet Crime Complaint Center reported more than $20.8 billion in losses connected to internet crime. And because many scams are never reported, the true number is likely much higher.

If it feels like you are getting more scam calls, fake text messages, suspicious emails, and urgent alerts than ever before, there is a reason. Fraud has become a massive business. Every call, message, pop-up, and email is designed to get someone to act quickly, emotionally, and without verifying the details first.

While fraud affects people of all ages, older adults are often targeted more aggressively. In 2025, people age 60 and older reported more than $7.7 billion in losses to the FBI, the highest reported loss amount of any age group.

That does not mean older adults are careless. It means criminals are strategic. They often target people who may have accumulated savings, own a home, receive Social Security or pension income, or are less comfortable navigating rapidly changing technology. In some cases, scammers also exploit loneliness, trust, fear, or declining cognitive ability.

Some of the most common fraud categories include:

Investment scams
These often involve promises of unusually high returns through cryptocurrency, foreign exchange trading, private investments, or "exclusive" opportunities.

Tech support scams
A pop-up, email, or phone call claims there is something wrong with your computer, bank account, or device and urges you to call a support number immediately.

Government impersonation scams
Someone claims to be from the IRS, Medicare, Social Security, law enforcement, or another government agency and says you owe money, need to verify information, or are at risk of legal trouble.

Non-payment or non-delivery scams
These may include fake missed delivery notices, unpaid tax notices, online purchases that never arrive, or requests to resolve a payment issue.

Extortion and blackmail scams
A criminal threatens to expose personal information, damage your reputation, or cause harm unless you send money.

Romance scams also deserve special mention. These often begin as online relationships with someone the victim has never met in person. Over time, the scammer builds trust and eventually asks for money, often tied to an emergency, medical issue, travel problem, or investment opportunity.

I recently attended a Seniors Against Financial Exploitation, or S.A.F.E., event put on by the Napa County District Attorney's Office in partnership with Napa County Health & Human Services, Molly's Angels, Monarch Justice Center, the Napa County Commission on Aging, Providence, and Napa Valley College.

The morning session was designed for seniors and focused on education, prevention, and available resources. I attended the afternoon session, which was geared toward financial professionals and emphasized what we can do to help educate and protect the people we serve.

Perhaps the most unsettling takeaway was how far criminals are willing to go. This is no longer limited to suspicious emails or poorly written messages. Scammers can spoof phone numbers, clone voices with artificial intelligence, impersonate family members, create fake websites, and even send couriers to someone's home to collect cash, gold, or other valuables.

Here are a few practical steps that can help protect you and your loved ones:

Review financial accounts regularly.
Check bank, credit card, and investment statements each month for unusual activity. The sooner something is identified, the better the chance of stopping further damage.

Never send money to someone you do not know personally.
Be especially cautious with wire transfers, cryptocurrency, gift cards, payment apps, or requests for cash. These methods are often difficult or impossible to reverse.

Slow down when something feels urgent.
Scammers rely on pressure. They want you to act before you think. If someone says you must act immediately, that is often the first warning sign.

Practice good cyber hygiene.
Do not click on links from unknown senders. Use strong passwords. Turn on two-factor authentication when available. Keep software and security updates current.

Verify through a separate channel.
If you receive a call, text, or email from someone claiming to be a family member, bank, government agency, or business, do not rely on the number or link they provided. Hang up, close the message, and contact the person or organization using a phone number or website you already know is legitimate.

This is especially important now that artificial intelligence can be used to mimic voices and images. A phone call may sound like someone you know. A text may come from a familiar-looking number. An email may look official. But a few extra minutes spent verifying can make all the difference.

For families, one simple idea is to create a family code word. Choose something unique, such as a favorite vacation spot, an inside joke, or a word that would be hard for someone outside the family to guess. If a loved one ever calls asking for urgent financial help, especially under unusual circumstances, ask for the code word before taking action.

It is also worth having a broader family conversation, especially with aging parents or grandparents. This does not need to feel intrusive or uncomfortable. It can be framed simply: “We’ve been hearing more about scams targeting families and older adults. Can we talk about what we would do if one of us received a suspicious call or message?”

That one conversation may prevent a devastating financial mistake later.

Fraud prevention is becoming an important part of financial planning. Protecting wealth is not only about investments, taxes, insurance, or estate documents. It is also about helping families build safeguards around the assets they have worked so hard to accumulate.

At 5T, part of our role is to help protect clients not only from market risk, but also from the growing risks that can threaten their financial security. We have internal procedures designed to help verify unusual requests, especially those involving money movement, changes to account information, or activity that seems inconsistent with a client's normal behavior. Just as importantly, we try to be a trusted resource clients can call before they act. Sometimes the most valuable thing we can do is help someone pause, verify, and avoid making a rushed decision under pressure.

If you have aging parents, grandparents, relatives, neighbors, or friends, consider sharing this with them. A simple conversation today could help protect someone you care about tomorrow.

For more information or to report internet-related fraud, visit the FBI's Internet Crime Complaint Center at IC3.gov. You can also report fraud to the Federal Trade Commission at ReportFraud.ftc.gov.

If you would like to stay informed about future local S.A.F.E. events, you can sign up for news from the Napa County District Attorney's Office through the DA's Newsline newsletter.

Sincerely,

Colton Maher
Financial Planner and Advisor
5T Wealth, LLC
Main (707) 224-1340
Cell (707) 815-0843
Colton@5twealth.com

5T Wealth, LLC
TIME | TEMPERAMENT | TALENT | TECHNOLOGY | TEAM

The opinions expressed are those of the author and are subject to change without notice. The opinions referenced are as of the date of publication and are subject to change due to changes in the market or economic conditions and may not necessarily come to pass. Any opinions, projections, or forward-looking statements expressed herein are solely those of the author. They may differ from the views or opinions expressed by other areas of 5T and are only for general informational purposes as of the date indicated.

5T has presented information in a fair and balanced manner. 5T is not giving tax, legal, or accounting advice.

Past performance should not be considered an indicator of potential future performance. If you do not consider yourself suitable, either emotionally or financially, to experience volatility and/or losses in financial markets, you should not invest. The portfolio managers at 5T do not guarantee investment results.

Charts, displays and graphs may be used as illustrations. They are not intended to be used by themselves to determine which securities to buy or sell, or when to buy or sell them. Such charts and graphs offer limited information and can’t be used on their own to make investment decisions.

Your Financial Roadmap does not represent the opinions of Fidelity, Fidelity Institutional Brokerage Group, NFS or anyone employed by Fidelity in any capacity. Neither Fidelity, Fidelity Institutional Brokerage Group, nor NFS, nor anyone employed by Fidelity in any capacity has participated in the creation of Your Financial Roadmap and they are not responsible for the contents or distribution of Your Financial Roadmap.

Your Financial Roadmap does not represent the opinions of Charles Schwab Corporation, Schwab Advisor Services or anyone employed by Schwab in any capacity. Neither Charles Schwab Corporation nor Schwab Advisor Services, nor anyone employed by Schwab in any capacity has participated in the creation of Your Financial Roadmap and they are not responsible for the contents or distribution of Your Financial Roadmap.

The investment objectives of various strategies mentioned in Your Financial Roadmap may be substantially different from one another. Therefore topics or investments mentioned in Your Financial Roadmap may or may not apply to specific managed accounts and/or strategies. If you are unsure which strategies your accounts are invested in please ask a representative of 5T to clarify that for you.

The assets held in managed accounts at 5T may include stocks, bonds, cash, commodities, foreign exchange, mutual funds or exchange traded funds (ETF's), money market accounts or limited partnerships that represent the same. They are subject to market fluctuation and the potential for losses. The assets are not insured. The value and income produced by these investment products may fluctuate, so that an investor may get back less than they initially invested.