MARCH 2026

BE SAFE | BE INFORMED | BE AWARE

FIGHTING FRAUD with ENOA

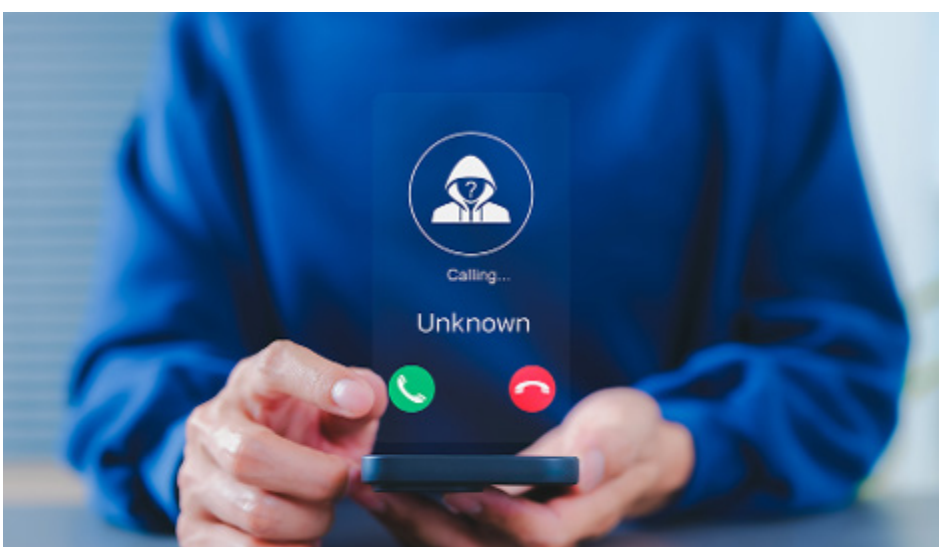
Eastern Nebraska Office on Aging
(402) 444-6536 | Blair (402) 426-9614
enoa.org

Stop Unwanted Robocalls and Texts

Robocalls are more than an annoyance, they are often the preferred tool of fraudsters. Stopping illegal robocalls is the Federal Communication Commission's (FCC) top consumer protection priority.

To restore trust in our phone networks, the FCC is fighting illegal robocalls at every point of a call's journey, from its source to your phone.

This includes empowering carriers to block more illegal robocalls before they reach consumers, giving consumers better tools to distinguish legitimate calls from scams, stepping up enforcement, and disrupting scam calls that originate outside of the United States.



Scammers often use caller ID spoofing to make their calls appear legitimate so you are more likely to answer. If you think the call has been spoofed, don't hang on, hang up!

How to avoid phone scams

Scammers create a false sense of urgency and leverage technology and information they can find online to sound convincing.

- Don't answer calls from numbers you don't know.
- Hang up right away if someone asks for money or personal information.
- If you feel pressured, or a caller asks you to pay with gift cards, it's a scam!
- Never share account numbers, Social Security numbers, passwords, PINs, or other important information over the phone.
- If someone says they're calling from a company or a government agency, hang up and call back using an official phone number from an account statement (if you have one) or their website.
- Don't respond to texts or click on links sent from numbers you don't recognize.
- Set up strong passwords for your voicemail so it doesn't get hacked.
- Talk to your phone company about call blocking tools they may have and check into apps that you can download to your mobile device to block unwanted calls.

Check the FCC Scam Glossary for detailed breakdowns of specific robocall scams. Help us spread the word by talking to your family and friends about phone-based scams.

Robocalls rules

Robocalls are phone calls made using an autodialer or a prerecorded or artificial voice message.

FCC rules require a caller to obtain your prior written consent – on paper or through electronic means, including website forms or a telephone keypress – before they make a prerecorded telemarketing call to your home or wireless phone number. FCC rules also require a caller to obtain your oral or written consent before making an autodialed or prerecorded call or text to your wireless number.

Continued on next page

These rules do not apply to emergency calls about danger to life, safety, or property.

Types of permitted autodialed calls

FCC rules allow market research or polling calls and calls on behalf of tax-exempt non-profit groups to landline numbers. Calls about school closings or flight information are also permitted to your landline.

Opting out of autodialed calls

Prerecorded telemarketing calls must provide an opt-out option at the start of the message. You may opt out of any robocall or robotext at any time and in any reasonable manner, even if you previously gave consent for such calls.

Prerecorded voice messages

All prerecorded voice message calls must include the caller's name, number, and business name at the beginning of the message.

Artificial intelligence and voice cloning

AI-generated voice calls are illegal unless the consumer has agreed to receive them or the caller is exempt.

Telephone solicitations

Telephone solicitations are calls that act as an advertisement. Phone solicitations are permissible with prior express permission or from tax-exempt non-profits. Telemarketing calls based on an established business relationship are not permitted to your landline phone without your advanced permission.

Robotexts

FCC rules ban text messages sent to a mobile phone using an autodialer unless the phone owner previously gave consent to receive the message or the message is sent for emergency purposes.

Commercial texts require written consent; for informational texts, your consent may be oral.

FCC rules apply even if you have not placed your mobile phone number on the National Do Not Call Registry.

Tips for avoiding text scams and spam

- Do not respond to texts from unknown or questionable sources, and never click links in these messages.
- Most mobile carriers let you block spam by forwarding the message to 7726 (SPAM)—check with your provider.
- Be careful about giving out your mobile phone number and personal information.
- Before submitting your number on websites, read the privacy policy and look for opt-out options—often a checkbox.
- Check the policies of the companies you do business with for selling or sharing your information.

Political campaign robocalls & robotexts

The Telephone Consumer Protection Act contains specific rules callers must follow when making campaign calls or sending texts:

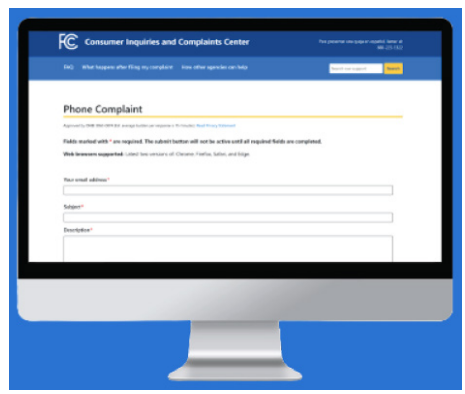
- Landlines: Political robocalls (autodialed or prerecorded) are allowed without prior consent.
- Cell phones: Political calls, texts, or prerecorded messages require the recipient's prior permission—unless sent manually.
- Robotexts: Autodialed political texts need consent; manually sent texts do not.
- Caller Identification: Prerecorded or artificial voice calls must begin with the caller's name, phone number, and the name of the organization they represent (if calling on behalf of a third-party).

Filing complaints about robocalls and texts

FCC Complaints: You can report illegal calls or texts to the FCC. Choose the "unwanted calls" category and note if your number is being spoofed, blocked, or mislabeled.

What Happens Next: The FCC doesn't resolve individual complaints but uses them to guide policy and possible enforcement under the Telephone Consumer Protection Act or the Truth in Caller ID Act. Your complaint may also be shared with other enforcement agencies.

FTC Complaints: Report phone scams or Do Not Call violations to the FTC.



Do Not Call Registry

The National Do Not Call Registry is a list of landline and wireless phone numbers that legitimate telemarketers agree not to call. You can register your numbers for free at donotcall.gov, or by calling 1-888-382-1222 (TTY: 1-866-290-4236). You must call from the phone number you wish to register.

Under FCC rules, telemarketers calling your home must provide their name along with the name, telephone number, and address where their employer or contractor can be contacted. Telemarketing calls to your home are prohibited before 8 a.m. and after 9 p.m., and telemarketers must comply immediately with any do-not-call request you make during a call.

Continued on next page

Other do-not-call lists

Many states now have statewide do-not-call lists for residents. Contact your state's public service commission or consumer protection office to find out if your state has such a list and how you can sign up.

FCC actions to protect consumers

- Issued hundreds of millions of dollars in enforcement actions against illegal robocallers.
- Empowered phone companies to block suspected illegal calls.
- Allowed phone companies to block numbers not on a customer's contact list or "whitelist" when the customer opts in.
- Required caller ID authentication to reduce illegal spoofing.
- Mandated blocking of illegal international robocall traffic.

If you spot a scam, report it to the ***FTC*** @ ReportFraud.ftc.gov.

6 Common Types of Investment Fraud and How to Identify Them

Learn the red flags for financial scams from these recent criminal cases

By Cheryl Winokur Munk

Older Americans have lost an alarming amount of money to investment scams in recent years. In 2023, people 50 and older reported more than $900 million in investment-related fraud to the Federal Trade Commission — far more than the combined reported losses to romance, tech support and online shopping scams. The median investment loss was at least $9,500. (For more on the ongoing war against all types of fraud, see the April AARP Bulletin.)

Although these scams come in many varieties, they often share the same red flags:

- Investment strategies are hard to understand (as is often the case with cryptocurrency, for instance).
- Risk-free returns are promised.
- It's insisted that you act soon or lose your chance for a big payout.

To put you on alert, here's a roundup of fraud alleged by prosecutors and regulators, along with a guide to some of the reddest flags.

Cryptocurrency

Crypto-related fraud is rampant, often in the form of criminals touting sure bets on cryptocurrency investments, using bogus websites to demonstrate (fake) profits.

Continued on next page

Recent case: From October 2020 to August 2023, a group known as Fundsz promised investors no-sweat annual profits of 365 percent through cryptocurrency trading and other "healthy and sustainable" sources of income, alleges a complaint filed by the Commodity Futures Trading Commission (CFTC). "Make Money While You Sleep" and "Passive Income With ZERO Effort on Your Part," reads one Fundsz marketing slide included in the complaint. An alleged ringleader touted a "proprietary algorithm" but declined to reveal "the secret to our sauce." A court-appointed receiver calculated that more than 9,000 investors lost a total of $15.7 million.

Foreign exchange

Similar to the crypto scams noted above, these involve scammers promising easy gains for investments in foreign exchange markets. They often keep the ruse going by delivering payouts Ponzi scheme–style.

Recent case: In late 2022, the Securities and Exchange Commission alleged that Houston resident John Fernandez had fraudulently raised more than $4.3 million from about 175 investors, promising "guaranteed interest every month" from trading in currency markets. Rather than investing in foreign exchange markets, he sent investors computer screenshots of fabricated gains from trades, the SEC said. He paid out some money, but that was mostly a Ponzi scheme — a fraud in which the illusion of a successful operation is created by paying investors fake "profits" that are simply money paid in by other deceived investors. When that venture failed, Fernandez blamed a "tax blowback" and asked investors to move their money to a new investment, described as a "legitimate financial company." This second venture, which promised annual returns of 5 to 100 percent, failed as well.

Guaranteed buyback

These scams promise the benefits of entrepreneurship with none of its risks. All you need to do is buy something from the scammer, who promises to buy it back from you once it's ready for market. Variations on this pitch have included "you buy our seedlings, and we'll buy your plants" and "buy our earthworm farm equipment, and we'll buy your worms."

Recent case: Since 2021, a company called Agridime has raised $191 million from more than 2,100 investors in what the SEC says is a Ponzi scheme. The company allegedly agreed to sell investors beef calves for $2,000 apiece, then buy back the same animals at a higher price after a year, guaranteeing a return of at least 15 percent and allowing participants "to become a part of providing fellow Americans with the highest-quality farm-fresh beef available." Instead, the SEC says, the company acquired far fewer cattle than it sold to investors, had less than $1.5 million in cash as of last September, and made at least $58 million in Ponzi payments to investors. In its advertising, the company acknowledged, "We know it sounds too good to be true."

Precious metals

In these illegal operations, salespeople persuade victims that they should move their savings out of safe, traditional investments and into gold and silver coins. These coins, the scammers say, will keep your hard-earned money safe when the economy (or the environment or the health system) inevitably collapses.

Recent case: In a settlement announced last October, the CFTC and regulators from 30 states alleged that precious metals dealer Safeguard Metals had deceived more than 450 investors by selling them $66 million in fraudulently priced silver coins. According to the settlement, the company pushed older Americans, most of whom were inexperienced investors, to empty their retirement accounts for silver purchases by preying on their fears and misrepresenting the safety of traditional retirement accounts. Sales representatives told one investor that the stock market was going to crash and the government would confiscate people's IRAs and repeatedly called another to say "hurry up" and "make a decision." Despite telling customers that it typically sold them silver 4 to 23 percent above its own costs, Safeguard's markups actually averaged 71 percent up until 2021, according to the CFTC.

Commodities trading

This is another example of scammers taking advantage of the fact that most people don't know much about many forms of investment.

Recent case: Phillip Galles was found by a judge last November to have fraudulently obtained $5.3 million from 65 people for a pool of money to invest in commodities, then to have used that money instead for expenses including luxury car rentals and purchases at a jeweler, Macy's and Best Buy. Among Galles' false claims, the judge found: that he had an investment return of 238 percent in 2020; that he managed $1.7 billion in offshore entities and had just raised $3 billion to invest; and that he employed at least five different automated trading models, including "algorithmically determined 'inflection points' [that] are filtered using order book dynamics/market microstructure analysis to profit from price movements in either direction around these areas." When one client asked to withdraw some of his money, Galles put him off with a series of excuses for why he couldn't, including bank mix-ups that prevented withdrawals and a visit to the emergency room: "A pill opened up in my throat by accident and closed my throat for 2 full minutes. I thought that it was an onion and tried to get it back up. It didn't go so well."

Real estate

Whenever you deal with big-ticket items — including real estate — you're going to find scammers looking for a way in. Sometimes they offer a homeowner quick cash in exchange for a promise to use a certain real estate agent if the owner decides to sell their home, as described in this episode of AARP's The Perfect Scam. In some cases, homeowners aren't aware that the contract locks them in for years and that the real estate agent can take out a mortgage on their home. Or, like the case alleged below, a scammer will pitch real estate investments that offer high returns, then take off with the principal.

Recent case: Wilson Baston pleaded guilty to mail fraud and wire fraud in 2008 in a real estate scheme that cost an estimated 185 people more than $22 million. The SEC accused him last June of launching a similar scheme not long after he was released from prison in 2017. This time around, the SEC says, he persuaded people to invest more than $10 million in several real estate deals (which he didn't identify) by promising to repay their principal, with interest up to 25 percent, within days or weeks. Baston, who allegedly hid his past by using the alias "Chanon Gordon," touted his ability to flip undervalued properties, but he often used fresh investments to make Ponzi payments to other investors, according to the federal accusations. After Baston failed to repay one investor — he had used that person's money to pay off someone else — he persuaded the first investor not only to "roll over" the purported principal and interest into a new transaction but also to pay an additional $4,000, the SEC says. Baston fended off requests for repayment by citing obstacles such as moving his office, not having his phone and dealing with multiple bouts of COVID-19, according to the complaint.

How to avoid these scams

Before you invest:

1. Check credentials. Brokercheck.finra.org, adviserinfo.sec.gov and nfa.futures.org/basicnet show finance pros' records and licenses. "Most scams involve unregistered entities, people and products," says Melanie Devoe of the CFTC.

2. Look for transparency. Be wary if you can't independently verify financial statements. One advantage of mutual funds is that you can easily find their price, performance and holdings from multiple sources.

3. Take your time. Don't rush to invest because you're told you'll lose out unless you act soon. "If it's a legitimate investment, it's going to be available tomorrow," says Claire McHenry, president of the North American Securities Administrators Association.

Continued on next page

4. Get a reality check. Run a proposed investment past someone who's not involved with the venture — maybe just a levelheaded friend. That move "can melt away the halo of excitement that comes with a sales pitch," Devoe says.

5. Know your limitations. Can you afford to lose all or part of your investment? Do you really understand what you're getting into? If an investment opportunity is confusing or vague, it's probably not a great strategy for you, McHenry says.

That text or email about your "tax refund" is a scam

Tax season is approaching, and if you're getting a refund, scammers are looking to steal it before you've had a chance to claim it. So, before you respond to a text or email about a "tax refund" — especially one that asks you to click a link — know that this could be a scam designed to get your personal information and steal your tax refund.

These scams often start with a text or email that looks like it's from the IRS or a state tax office saying they've "processed" or "approved" your tax refund claim. (Note: that's not how you find out about a real tax refund.) To "verify your identity" and "send you money," they ask you to click a link to enter details like your Social Security and bank account numbers — but it's a phishing scam. If you click and share your info, the scammer might steal your personal information to get your tax refund or even steal your identity to open other accounts.

If you get a message like this:

- Know that the real IRS and state tax offices won't reach out by text, email, or on social media to get your information. Only scammers will.
- Don't respond or click any links. To check the status of a pending tax refund, never use the link from the message. Instead, visit USA.gov to learn how to find out if you're really getting a federal or state tax refund.
- Report and delete the message. Use your phone's "report junk" option or forward unwanted texts to 7726 (SPAM) and mark unwanted emails as spam or junk. Once you've checked it out and reported it, delete the message.

Visit IdentityTheft.gov/steps to learn how to protect yourself before identity theft happens. And if you spot a scam, tell the FTC at ReportFraud.ftc.gov.

How To Spot, Avoid, and Report Tech Support Scams

Tech support scammers try to scare you into believing there's a problem with your computer. They tell lies to get your financial information or remote access to your computer. Their goal is to steal your money, or worse, steal your identity.

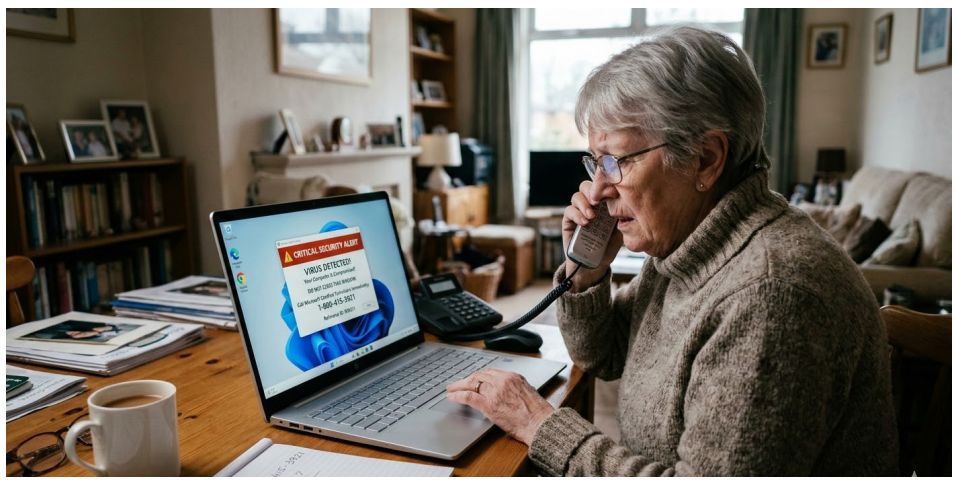
How a Tech Support Scam Works

Tech support scammers use different tactics to trick you into believing there's a virus or other issue with your computer.

Tech support scams often start with a bogus warning about a problem with your computer. It could be a fake pop-up warning that looks like it's from a well-known company and urges you to call a phone number to get help. Other tech support scams might start with a call or text message from a scammer who pretends they're a computer technician from a well-known company.

Tech support scammers might also try to get their websites to show up in online search results for tech support or run their own display ads online. The scammers are hoping you'll call the phone number to get help.

If one of these tech support impersonators gets you on the phone, they ask for remote access to your computer and pretend to scan it for viruses. They claim to find a malicious program and offer to remove it for a fee.



They often insist that you pay with gift cards, a wire transfer, a bank transfer, cryptocurrency, or a payment app. They want you to pay in one of these ways because it's like using cash — once you pay, it's hard to get your money back.

Other Types of Tech Support Scams

Serious crimes and bogus helpers

Sometimes, the fake tech support specialist with remote access to your computer pretends to scan it for viruses and claims to discover that someone hacked your accounts. Or that your name is linked to serious crimes, like money laundering or drug trafficking.

That's when the tech support impersonator transfers you to someone who supposedly works for the government and can help you. That's a lie. This person is a scammer who may give you a badge number or open a case number. Both are fake. How can you know? Because of what comes next. He says your money is at risk and you have to protect it immediately. He might say to

- withdraw money from your account to "protect it,"
- deposit money in a "federal safety locker," or
- buy gold or get cash and give it to someone.

And that's how you know it's a scam. ***Because someone who works for the government will never say you must transfer your money to "protect it."***

Continued on next page

Someone who works for the government will never tell you to put your money in a federal safety locker. There's no such thing.

Someone who works for the government will never demand payment. Not in cash. Not in gold.

Fake invoices and subscription renewals

In another type of scheme, scammers send notices about automatic renewals for tech support subscriptions. You might get an email or text message that says you were charged hundreds of dollars to renew your tech support subscription. To get your attention, the scammers use the names of well-known companies like Geek Squad, McAfee, and Norton.

The message says you must call a phone number within 24 hours if you want to dispute the charge. If you call, the scammers ask for remote access to your computer. They take you to a spoofed website that looks real and tell you to enter your bank or credit card information to process the refund. After you do that, they claim there was an error in the amount entered. They say they refunded you too much money and insist you pay them back with gift cards, a wire transfer, a bank transfer, cryptocurrency, or a payment app.

If you get a message about a tech support subscription renewal and you think it's real, contact the company directly using a phone number you know is real. ***Do not use the number included in the message.***

Also check your credit card or bank account for an unauthorized transaction for a tech support subscription. If you see one, report it to your credit card company or bank and ask them to reverse it and give you back your money. If you don't see a transaction for a tech support subscription, that tells you the message was a scam. Ignore and delete it.

How To Avoid a Tech Support Scam

Most tech support scams rely on elaborate stories, threats, and pressure to con you into giving up your financial information or your hard-earned money. But remembering these two things will help you avoid a tech support scam:

1. Legitimate tech companies won't contact you by phone, email, or text message to tell you there's a problem with your computer.
2. Real security pop-up warnings and messages will never ask you to call a phone number.

Not sure if it's a scam? Talk to someone you trust — a friend, a family member, a neighbor. Talking about it could help you realize it's a scam.

If you think there may be a problem with your computer, update your computer's security software and run a scan. If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone. Stores that sell computer equipment also offer technical support in person.

What To Do if You Were Scammed

Read What To Do if You Were Scammed for specific steps to take if you

- paid a scammer
- gave a scammer your personal information
- gave a scammer access to your computer

If you gave your username and password to a tech support scammer, change your password right away. If you use the same password for other accounts or sites, change it there, too. Create a new password that is strong.

Report Tech Support Scams

If a tech support scammer contacts you, tell the FTC at ReportFraud.ftc.gov.

When you report a scam, the FTC uses the information to build cases against scammers. Are you skeptical that reporting scams will make a difference? This video shows how your story helps the FTC stop scammers.

Report scams the *FTC* @ ReportFraud.ftc.gov.