25 Great Ways to Avoid Scams

Practical things you can do to protect yourself as fraud grows more pervasive and sophisticated

By Matt Alderton, AARP

Published January 03, 2025

SAM ISLAND

With age comes wisdom. But even the wisest among us have become victims of scams, which are epidemic — and growing in sophistication with the help of rapidly advancing tech tools. The FBI's Internet Crime Complaint Center received 101,068 reports from people age 60 and over in 2023, and they'd lost more than $3.4 billion to online criminals. Those figures don't reflect the enormity of the

scourge, however: Of the more than 880,000 complaints the FBI received in 2023, only about half included age-related data. And fraud is a notoriously underreported crime.

But there are practical steps that can lower your risk. Here are 25 of the most effective things you can do.

1. Accept your vulnerability

The first step toward protecting yourself is admitting that you're vulnerable, regardless of your age, gender, race, income, education or intelligence. "The No. 1 thing — and there's nothing that comes close to this — is to understand that you're not too smart to fall prey to a scam," says Joseph Steinberg, a cybersecurity lecturer at Columbia University and author of *Cybersecurity for Dummies*. "There are many people who believe, 'I could never be scammed. I'm too sophisticated. I was a judge or a lawyer or whatever.' That's wrong. I've seen Nobel Prize winners make mistakes related to cyber scams. Literally nobody is too smart."

2. Practice radical skepticism

Once you admit that anyone can be targeted by scammers, you can begin to mount defenses against them. To start, "set a 'default skepticism' stance," suggests Maria-Kristina Hayden, founder and CEO of Outfoxm, a cyber hygiene and resiliency company. "Be suspicious of digital messages, phone calls or even snail mail from strangers," she says. "Whenever you're asked for money or personal information, pause and ask yourself, 'Does this make sense?' " suggests Jason Zirkle, training director at the Association of Certified Fraud Examiners. "Would your bank normally contact you this way? If it doesn't feel right, stop communication immediately."

3. Pause and think

Scammers are skilled manipulators of their targets' emotions. If you find yourself growing anxious or upset by someone who's contacted you out of the blue, that's a red flag. "Real customer service representatives at banks, tech companies and government agencies are trained to put you at ease, not rile you up," says Marti DeLiema, an assistant professor at the University of Minnesota who studies financial scams and older adults. "Criminals are trying to make you feel anxious because strong emotions overwhelm your ability to make rational decisions." The FBI recently began a "Take a Beat" scam-awareness campaign, urging the public to "resist pressure to act quickly, pause for a moment, and assess the situation."

4. Be suspicious of secrecy

If someone you don't know well tells you not to tell anyone about your interaction with them, it's a good sign that you *should* tell someone. "Scams thrive on privacy and confidentiality," DeLiema says. "The criminals know that the minute you tell someone what is going on, that person will recognize it's a scam and will intervene." Because criminals rely on privacy, an early indicator of suspicious activity is requesting to move a conversation from a traditional channel such as phone, email or text to a nontraditional channel like WhatsApp. "Scammers often try to move conversations to less-monitored platforms, making it easier to control the narrative and avoid detection," Zirkle says. "Keep communication within official channels, especially with companies or service providers."

Regularly check your bank accounts and credit card statements to mitigate damage.

5. Set up bank alerts

Regularly check your bank accounts and credit card statements to make sure that all transactions are legitimate. Although it won't prevent fraud, it can help you spot it early so you can mitigate the damage, notes Zirkle, who recommends setting up online alerts with your bank.

6. Be informed

When it comes to fraud, knowledge is power. "Educate yourself about threats," Hayden advises. "Read headlines about scams and fraud. ... We can't be prepared if we don't understand what's out there." Also, learn about new and emerging technologies, suggests geriatric neuropsychologist Peter Lichtenberg, past director of the Institute of Gerontology at Wayne State University: "Scammers keep changing how they do things, so we have to stay vigilant." You can keep up with the latest scams and technology by engaging with the AARP Fraud Watch Network and AARP's Personal Technology Resource Center, reading public service announcements from the FBI's IC3, and signing up to receive alerts from the Federal Trade Commission.

7. Don't pay for anything in gift cards, cryptocurrency or gold

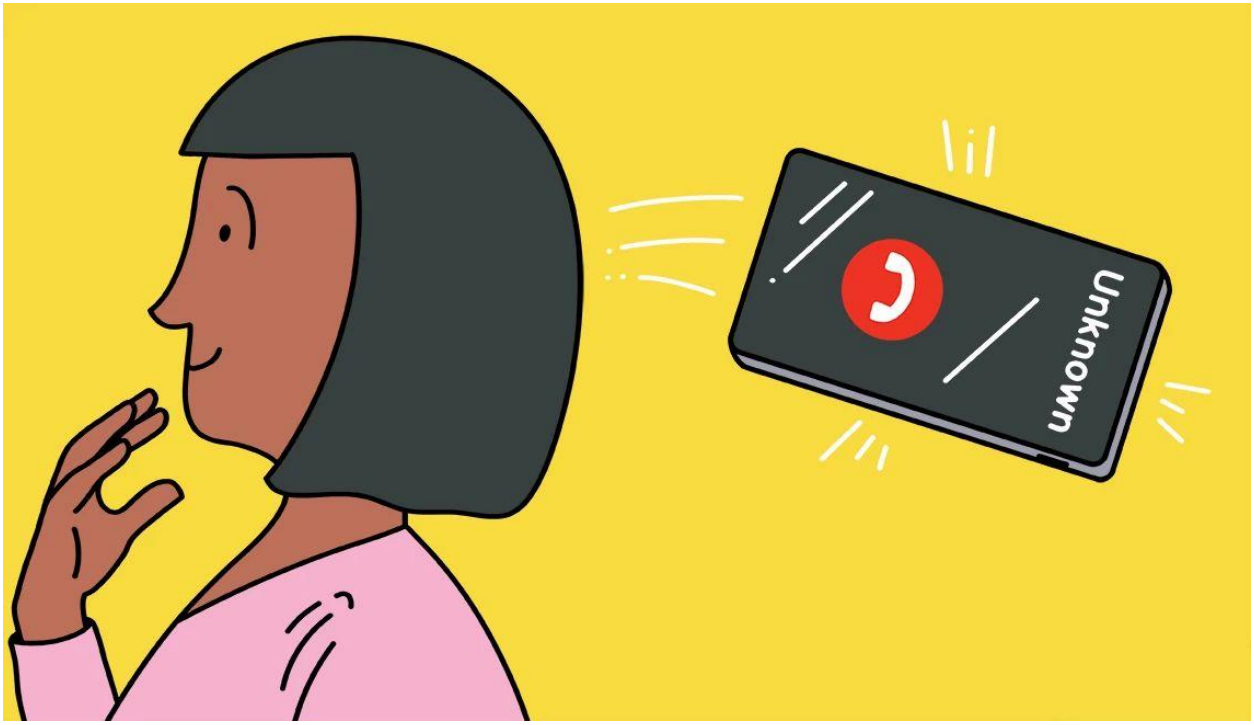
It's best to pay with a credit card, which can protect you from all sorts of scams — including gift card scams. "Criminals prefer untraceable methods of payment that are hard to reverse, so they will tell targets to buy gift cards and read them the codes on the back to steal the funds," DeLiema says. Other preferred payment vehicles for scammers include cryptocurrency, gold bars, prepaid debit cards and payment apps like Venmo and Zelle. If someone — especially a stranger — asks for payment or debt settlement using one of these payment methods, think twice.

8. Find a sounding board

Another way to protect yourself from scams is to build community, suggests Anthony Miyazaki, a professor of marketing at Florida International University, where he studies consumer protection. “Research has shown that negative well-being and lack of social support are correlates of scam susceptibility,” he says. “It’s worthwhile to bolster your social support group, whether it’s through community groups, churches, volunteer work or part-time jobs.” And it’s a good idea to have at least one person who can help you identify potential scams by being a financial confidante — an objective party you can consult before making big purchases or money transfers to ensure that they’re wise and legitimate. You also can call the toll-free AARP Fraud Watch Network Helpline at 877-908-3360 for advice, support and resources (available Monday through Friday, 8 a.m. to 8 p.m. ET).

9. Sign up for identity monitoring

Credit score and identity monitoring services can help you quickly detect and stop fraud. “Monitoring services can alert you to fraudulent activities, such as unauthorized transactions or identity theft, giving you the opportunity to act before things spiral out of control,” Zirkle says. You might already have access to a free monitoring service through your bank, credit card company or other service provider, points out Christopher Ray, a longtime chief information security officer who is now head of strategic and transformation services at Google-owned cybersecurity firm Mandiant. “Credit monitoring services keep an eye on your credit score and let you know if anything changes. This could be anything from new accounts being opened in your name to someone checking your credit history. If something fishy is going on, you’ll get an alert so you can fix it right away," Ray says.



One of the easiest ways to protect yourself from scams is to avoid answering calls or texts from unknown numbers.

10. Avoid unsolicited calls, texts and emails

Because scammers often initiate contact by phone or text, one of the easiest ways to protect yourself from scams is to avoid answering calls or texts from unknown numbers. Set up robocall blocking, for one. But even familiar numbers can be suspect. “Phone numbers can be spoofed to appear on your caller ID as being from a legitimate source, hiding the real number contacting you,” notes Steve Weisman, senior lecturer of law and taxation at Bentley University and editor of the blog Scamicide.com. Email addresses can similarly be manipulated. “Expand the headers on your inbound email messages by clicking the little down arrow so that you can see the full email address, not just the name of the sender,” DeLiema advises. “Read their email address carefully to make sure that a criminal didn’t just copy [a legitimate one] and make a small change in the letters of their name or organization.” If you do engage with an unknown party by phone or email, avoid providing personal or financial information.

11. Freeze your credit

When you freeze your credit, “it blocks anyone from opening new accounts or lines of credit in your name, which stops scammers in their tracks,” Zirkle says. It’s free and easy to freeze your credit by contacting each of the three major credit bureaus: Equifax, TransUnion and Experian. You can initiate a credit freeze online, over the phone or by mail — and temporarily pause or permanently remove it later if you need to apply for a loan, for instance. You can also request a free credit report from each of the three federal credit bureaus every 12 months. (Find out more at AnnualCreditReport.com.)

12. Maximize online privacy settings

If you use social media, be cautious what you share with friends and followers, and change your privacy settings to limit who can see your posts. “Social media accounts are prime hunting grounds for scammers to gather personal information,” Zirkle says. “Limiting the amount of information that you share online and using the strictest privacy settings reduces the chance that a scammer can trick you into thinking they’re someone you know.” The ability for scammers to impersonate someone you know is what makes social media so risky, echoes Weisman. “Scammers harvest information from social media, and use that information to craft specifically tailored spear-phishing emails and text messages that are more likely to get us to respond,” he says.

13. Think twice before clicking on links in emails and text messages

More than 90 percent of successful cyberattacks begin with a phishing email, according to the Cybersecurity & Infrastructure Security Agency. It might include a link that could download malicious software (malware) to your computer, or try to get you to reveal your passwords, Social Security number, credit card numbers or other personal information, explains Michael Bruemmer, vice president and head of global data breach resolution and consumer protection at Experian. The solution: Never directly click links in emails or text messages. Instead, go to the website independently by typing the URL into your browser or use the company’s official app. Scammers often disguise malicious links, so it’s always safer to verify first.

14. Go straight to the source

Verify phone calls and emails by going straight to the source — by responding to incoming communications with outgoing ones. Consider email, for example. “If you are unsure about the message, email the sender directly using a new message and use the email address that is saved in your contacts,” DeLiema says. “Don’t just reply. Better yet, call the sender on the phone.” The same is true for phone calls. For example, if you receive a call from someone who claims to work at your bank, hang up the phone, then call the customer service number that’s printed on the back of your credit or debit card to confirm, says Darius Kingsley, managing director and head of consumer banking practices at JPMorgan Chase & Co.

Regularly updating software on your phone, computer and other devices helps protect against malware.

15. Update your software

Software updates are one of the easiest things you can do to secure the devices that are connected to your router. “Scammers often exploit vulnerabilities in outdated software to hack into devices,” Zirkle notes. “Regularly updating software on your phone, computer and other devices helps close security gaps and protect against malware.”

16. Only hire trusted contractors

To avoid fraudulent contractors and fake construction companies, always get multiple bids on home improvement or repair projects, says licensed contractor Rodney Hakimi, owner of Prime Renovations in Baltimore. “This will help you find a fair price and avoid overcharging,” says Hakimi, who recommends checking licenses and insurance before hiring a contractor. “It is necessary to deal with professionals who are correctly credentialed. Check your local government website for a contractor license lookup tool.” Other signs of a fake or unscrupulous contractor are high-pressure sales tactics and requests for extremely high deposits. “A genuine contractor would never hurry you into making decisions,” Hakimi

continues. “Also, at no instance is one required to pay more than one-third of the total cost in advance. It’s reasonable to give a down payment, but never pay everything upfront.” Finally, be sure to check references and get a signed contract. “Always get a written, detailed contract before any work has started,” Hakimi says.

17. Be cautious when purchasing property

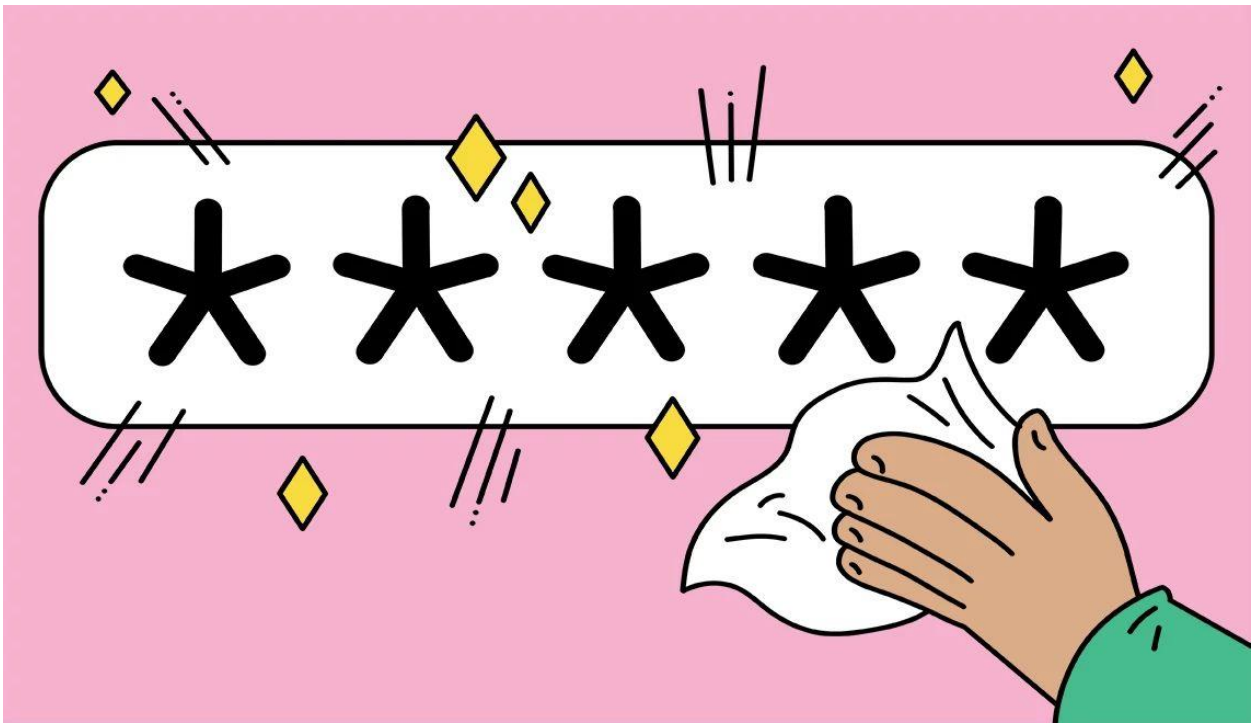
Because a home purchase is a large and complex transaction, real estate scams can deliver big paydays to ambitious scammers, who try to intercept down payments — a devastating experience for home buyers when the criminals succeed (and they often do). Home buying can be an unfamiliar, complex process “where a lot of confusing information comes at you from all directions, making it difficult for you to detect when something seems ‘out of the ordinary,’ ” says Tom Cronkright, cofounder of CertifID, a wire fraud prevention firm, and Sun Title, a residential and commercial title company in Grand Rapids, Michigan. “Scammers will leverage public property and listing data to intercept trusted communications and then impersonate your agent, attorney or title company to get you to send your money to the wrong place.” To protect yourself — and your investment — ask your real estate agent how they verify the identity of a seller before you close on a property. “Don’t act hastily,” Cronkright says. Also: “Call your real estate agent, title company or attorney to independently verify any wire instructions before sending funds.”

18. Use a VPN

If you’re on a non-private network (a public Wi-Fi connection), it’s safest to connect to the internet using what’s called a “virtual private network,” or VPN. “A VPN essentially builds a trusted tunnel where all the information you’re sending is encrypted, or protected, so that nobody who’s snooping around can view it,” says Abhishek Karnik, head of threat research at online security company McAfee. Most cellular and internet service providers offer VPNs as paid add-ons or included in a premium plan. You can also purchase a VPN service directly from a VPN service provider.

19. Disconnect from public Wi-Fi

Especially if you lack a VPN, steer clear of free and public wireless networks, Bruemmer advises. “Anybody can put up a fake Wi-Fi site,” he says, adding that scammers often use small devices called “pineapples” to intercept private information that flows between private devices and public networks. “I can be within 30 or 40 yards of wherever you are with a pineapple device that says ‘Starbucks Free Wi-Fi’ … and you won’t know if it’s legit or not.” If you need internet on the go, use your cellular service instead. (Learn how to use your phone as a Wi-Fi hot spot here.)



Passwords should be be complex, with a mix of numbers, letters and symbols.

20. Practice good password hygiene

It can't be said too many times: Never use easy-to-guess passwords such as “password” or “123456,” or use the same password for all your accounts. They should each be complex, with a mix of numbers, letters and symbols. To make your passwords as strong as they can possibly be, use a password manager that can store and create unique random passwords for each account (it’s accessed by a master password or on a phone by biometrics or PIN). Also enable multifactor authentication where possible, so you’ll need to provide a second form of identity verification, such as a temporary code that’s sent to you by text or email.

21. Secure your router

The key to a secure home network is a secure wireless router, according to Weisman. “Your home has many things that are connected to the internet and make up the Internet of Things, such as your television. Home devices that use the Internet of Things go through your router,” he explains. “Many people fail to change their router’s default password when they get their router, making them vulnerable to an attack.” If they can access your router, hackers can access anything that’s connected to it — including your computer and any sensitive data that you have stored there. “Change the default password for your router and install a guest network on your router for the use of your Internet of Things devices so they will not be connected to your computer,” Weisman adds.

22. Have a family safe word

Scammers also are using artificial intelligence to make their so-called “grandparent” scams more sophisticated. “The grandparent scam, which actually is better described as the family emergency scam, has gotten worse with the ability of scammers to use voice-cloning AI technology to make the voice of

the scammer sound like a family member in need," Weisman says. "Have a family safe word to be used if you are ever called about such an emergency."

23. Safeguard physical cards and documents

Although online scams are rampant, analog risks remain. You can minimize your exposure to flesh-and-blood fraudsters by taking a minimalist approach to your purse or wallet, Kingsley suggests. That means carrying only essential cards with you and leaving items you don't need — including not only extraneous credit cards, but also things like passports and Social Security cards — at home in a secure place, such as a safe or lockbox. "Also, remember to keep your checkbook safe and destroy any checks you don't use, or that have already cleared after you deposit them," he adds. Along with checks, you should destroy with a paper shredder any discarded documents that contain personal or financial information. "Physical documents with sensitive information, like bank statements or credit card offers, can be used by scammers for identity theft," Zirkle says.

24. Protect yourself from mail theft

Given the significant risks posed by online scams, you might assume that it's safer to conduct transactions by mail than it is to conduct them on the internet. But that isn't always the case. "The U.S. Postal Service has reported a rise in mail theft incidents," Ray says, advising people to deliver sensitive mail directly to the post office. They are often looking for checks, so Kingsley suggests "using alternative payment methods, such as online bill pay." You also can sign up for USPS' Informed Delivery program. "You will receive an email with photos of your next day's mail so you can be aware if something important is going to be delivered," Weisman notes.

25. Be a savvy shopper

The internet is full of shopping scams, including scammers who steal your money and payment information by advertising and selling fake products through fake stores, complete with fake customer reviews. To avoid them, use your common sense. "If a deal seems too good to be true, it probably is," Steinberg says. "That doesn't mean you shouldn't buy from stores with lower prices. But if you do a Google price search and see that everyone is selling something for $299 except for one company that's selling it for $150, and you've never heard of that company, take a moment to ask yourself if it's legit." The same goes when paying for travel packages, cruises or hotels. "Scammers often lure travelers with incredibly low prices or exclusive deals, so it's crucial to approach such offers with caution," says Cody Candee, founder and CEO of the luggage storage service Bounce. And, again, because credit card companies will investigate fraud and refund you for fraudulent charges, you can further protect yourself by always paying with a credit card.

Matt Alderton is a contributing writer who specializes in health and wellness, travel and technology. His work has also appeared in USA Today, Forbes *and* The Washington Post.