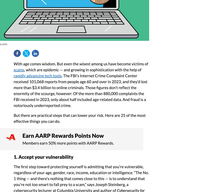
# 25 Great Ways to Avoid Scams

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

By Kate Alderton, AARP
Published January 03, 2023



JOHN SHAW

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 artificial intelligence (AI). In 2022 alone, U.S. consumers and businesses reported 103,500 reports from people age 60 and over in 2022, and they 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 2021, 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.

**Earn AARP Rewards Points Now**
Members earn 10% more points with AARP Rewards.

### 1. Accept your vulnerability

The first step toward protecting yourself is admitting that you're vulnerable. Scammers are skilled at exploiting our weaknesses, whether we like to. "It's tiring — and there's nothing that comes close to this — to be constantly 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 computer scientist and I wrote a textbook. 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, "be a default skeptical stance," suggests Maria Bartiromo Hayden, founder and CEO of Outfoxer, a cyber hygiene and resiliency company. "Be suspicious of digital messages, phone calls and even in-person interactions. Don't share any personal information or financial information (passwords and yourself). Slow this down a bit." Hayden suggests Jason Zinda, 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, pause. "Fraudsters are psychologically manipulative and most companies and government agencies are trained to put you at ease, not rile you up," says Marit DeLorme, an assistant professor at the University of Minnesota who studies financial scams and elder abuse. "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 Moment" 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," DeLorme 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, a vital indicator of suspicious activity is responding to move a conversation from a traditional setting to a more private one, such as from a public phone booth to a cell phone. "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.

JOHN SHAW

### 5. Set up bank alerts

Regularly check your bank accounts and credit card statements to make sure that all transactions are legitimate. Although it wasn't present 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 gerontic 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 on top of it." Some of the most recent scams involve AI, cryptocurrency, and the AARP Fraud Watch Network and AARP's Personal Technology Resource Center, reading public service announcements from the FCC's website 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, since that will 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 numbers on the phone," Zirkle says. "Credit cards are the safest form of payment, which for scammers includes cryptocurrency, bitcoin, prepaid debit cards and payment apps like Venmo and Zelle. If someone — especially a stranger — asks for payment or debit 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 Mirzaian, 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 groups, 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 sounding board for your suspicions and concerns. Some financial institutions offer programs or money transfers to ensure that they're safe 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 officer who now is a cybersecurity consultant. Microsoft and 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." Rax says.

SPONSORED CONTENT
**Walmart+**
$20 off a Walmart+ annual membership
POWERED BY

Hang up the second you realize a person you don't know is scam-preaching call or text from unknown number.

JOHN SHAW

### 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. "If it's someone you know, they'll leave a voicemail and you can be suspect," Thorne numbers can be spoofed to appear on your caller ID as being from a legitimate source, hiding the real number contacting you," Weisman notes. 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," Weisman advises. "Fraud is frequently attempted via similarly to real addresses. Look closely for misspellings and other clues." Finally, be cure to check 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. You can freeze your credit for free with Equifax, Experian, TransUnion and the 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 mortgage. 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

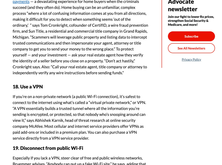
If you use social media, be cautious what you share with friends and followers. "Scammers can use information you post online to target you," Zirkle says. Facebook accounts are prime hunting grounds for scammers to gather personal information," Zirkle says. "Limiting the amount of information that you 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, notes Steve Weisman, senior lecturer of law and taxation at Bentley University and author of *The Art of Scam Protection*. "Fraudsters can use 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 look like a link to download malicious software, which then infects 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 for 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," DeLorme. "Don't hit 'reply' to the suspicious email, because that could be a fake address." It's 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 is 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.

JOHN SHAW

### 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 Hatten, owner of Prime Renovations in Baltimore. "This will help you find a fair price and avoid overcharging," says Hatten, who recommends checking contractors' credentials with the Better Business Bureau and asking to see draft professionals who are currently credentialed. Check a contractor's 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 into making decisions," Hatten 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 to secure a spot in the schedule, but no more." Finally, be sure to check references and get proof-of-insurance. "Between get a written, detailed contract before any work has started," Hatten says.

### 17. Be cautious when purchasing property

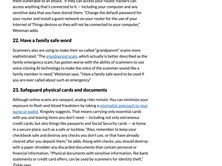
Because a home purchase is a large and complex transaction, real estate scams can deliver big paydays to unlikely scammers, who go to increased down payments — a devastating experience for home buyers when the criminals succeed. Land theft is another. Home buying can be an unfamiliar, complex process, and it's easy for criminals to impersonate real estate professionals, 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 Sue Trifa, 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 wend your money to the wrong place." To protect yourself, "be suspicious of any last-minute wire transfer instructions and verify the identity of a seller before you close on a property," Trifa and 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 similar-sounding aliases "Amazon." Hackers can also intercept information that flows between private devices and public networks. "Can be careful about what you're doing on your phone when you're connected to a 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 the simplest, with a mix of numbers, letters and symbols.

JOHN SHAW

### 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 generates and stores them automatically. Alternatively, "a phrase can be followed by a master password or six pieces by someone to a PINS. 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 your router is the gateway to your home. It's the door through which people can 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 guests, so that their devices will not be connected to your computer," Weisman adds.

### 22. Have a family safe word

Scammers also are using to make their so-called "grandparent" scams more sophisticated. "The emergency 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 wallet, Kingsley suggests. That means carrying only essential cards with you and leaving them you should need — including not only extraneous credit cards, but also your Social Security card. Instead, keep it in a safe place in a secure place, such as a safe or lockbox. "Also, make sure you shred your checkbook stub 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 become a prime target for mail theft incidents," Rax says, advising people to deliver sensitive mail directly to the post office. They are often looking for checks, no-bidding contracts, using alternative payment methods, such as online bill pay." You also can sign up for Informed Delivery, a free service that allows you to preview what's in your next daily 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 clicks, use your common sense. "If a deal seems too good to be true, it probably is," Weisman says. "Be wary of unrealistic discounts or significantly lower prices. But if you do a Google search and see that everyone is selling something for $20 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 have been known to create fake travel sites, or even legitimate-looking ones to approach such offers with caution," says Jim Zirkle, founder and CEO of the luggage storage service Bounce. And, again, because credit card companies well 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 appeared in Oil Today, Forbes and The Wrapup. Follow him on Twitter.

← 10 – Black Friday Phantom Edition

## Most Popular

MONEY
**Medicare Prescription Drug Changes**

MONEY
**IRS to Send up to $1,400 to 1 Million Taxpayers. Are You Eligible?**

MONEY
**The 10 Best Things Coming to Netflix in January**

MONEY
**7 Year-End Money Moves to Cut Your 2024 Tax Bill**



UPDATE NOW AND SAVE 25% OFF YOUR NEXT RENEWAL
Update now and get years of membership at your current rate without price increases. No hassle, no interruption in benefits. Terms and conditions apply.
Update Now

SIGN UP FOR EMAILS
**Get the AARP Advocate newsletter**
Join our fights for lower drug prices, better care, more security in Medicare, and more.
Subscribe
See All Newsletters
Privacy Policy