15 Ways to Protect Yourself from Fraud and Scams

1. Stop mail fraud at the mailbox

Informed Delivery is a free service from the U.S. Postal Service. The agency emails photos of letter-size mail expected to be delivered to you that day or shortly after. This is a great way to be sure that nothing is stolen from your mailbox by ID thieves. Sign up at InformedDelivery.usps.com.

Pick up mail as quickly as possible after it's delivered, and always take your outgoing mail directly to the post office. A hot fraud now is scammers stealing checks from mailboxes, erasing the ink and using them to steal from bank accounts.

2. Halt scammers at your front door

Consider installing a video camera; they are increasingly less expensive, and they're easy to install. If you don't recognize a visitor, don't answer. If you find yourself being pressured to buy or donate, have a refusal script ready (consider taping it near the door) that says, "I do not do business at my door. Please leave me something to review. If I'm interested, I'll call you."

Be wary of people posing as utility workers who show up unannounced. Don't allow anyone into your house without an appointment.

3. Prevent garbage theft

Shred any papers that contain private information (financial statements, bills, shipping receipts) before putting them out for pickup to avoid identity theft. Don't want to invest in a good cross-cut shredder? Many communities have shredding events or permanent drop-off sites. Get in the habit of dropping off your accumulated documents once every few months.

4. Watch for credit card skimming

Card skimming, in which the criminal affixes a credit card reader on top of a legitimate card reader at a store or gas station, is estimated to cause up to $1 billion in losses annually. When you are paying at a gas station or other point-of-sale location, inspect the device for loose/broken/scratched machinery to make sure someone hasn't tampered with it. If you are unsure, notify the cashier and pay using an alternative method.

5. Monitor your credit report

Routinely check yours (many credit card companies provide it for free; if not, go to AnnualCreditReport.com or call 877-322-8228). Watch for unusual activity; if you see any, report it immediately to the appropriate financial institution.

Then freeze your credit report. This prevents scammers from opening new credit cards or making big purchases in your name. You can unfreeze it as needed for legitimate transactions. Visit IdentityTheft.gov for more information.

Have you seen this scam?

- Call the AARP Fraud Watch Network Helpline at **877-908-3360** or report it with the **AARP Scam Tracking Map**.
- Get **Watchdog Alerts** for tips on avoiding such scams.

6. Safeguard your wallet

Remove cards and information you don't need to carry (such as your Social Security or Medicare card). Make copies of the remaining cards (front and back) and store in a safe place.

Audit your wallet and purse frequently. Take out any unnecessary items that collect and could compromise your personal information if lost or that would be a hassle to replace.

7. Protect your financial accounts

Create online accounts with each of your financial institutions. Come up with a unique password for each, and every few months, revise the passwords. (Your best bet is to use a passphrase: Ilovemy17dogz! is much stronger than Scruffy23. Keep track of passwords in a highly secure password manager or by writing them down and storing them safely.) But you should not rely solely on passwords. Many financial institutions will allow you to use a one-time passcode sent to your phone as an extra layer of security.

Then get in the habit of reviewing the transaction lists on a weekly or biweekly basis. Be sure you can account for every listed transaction. Spot something odd or incorrect? Immediately report it.

8. Safeguard your smartphone

If you have a newer model, turn on biometric identification (fingerprint or facial recognition); this will help prevent a thief from logging in to your phone.

Send calls from unknown numbers to voicemail (you can enable this in the phone's settings). Make sure your voicemail is set up and not full, so you can receive legitimate messages.

Scammers are sending far more bogus texts, often posing as companies you routinely deal with. Never respond to an unsolicited business text; if you think it might be valid, call the organization or go online.

Also make sure you are signed out of any financial apps on your phone — credit cards, financial institutions and peer-to-peer apps such as Venmo, CashApp or Zelle — when you aren't using them.

9. Secure your computer

Turn on two-factor authentication for all secure websites you frequent, such as financial institutions or utility companies (find out how via each site's online security center). Then only someone logged in to your phone can receive the code to access those accounts.

Consider subscribing to an antivirus software service. Some security experts say browsers and device manufacturers have more built-in malware protection than years ago, such as Microsoft Defender, which comes installed on some devices. Some paid subscriptions also include ad tracker blocking, cloud backups of your machines and identity theft monitoring.

10. Protect your email accounts

Actively designate unsolicited and unwanted email that shows up in your inbox as spam, so future emails from that site get blocked. Do not open file attachments in emails from businesses or people you don't trust completely. Malware is often planted via email attachments.

11. Set limits on social media

Set your profile so that only your friends can see your Facebook page. To do that, click the downward arrow button in the upper-right corner of your Facebook page, then click on Settings & Privacy and Privacy Checkup. This easy-to-use wizard will guide you through the settings. And never accept friend requests from people you don't know or respond to random messages from strangers. But also note that impostor scams, where someone pretends to be your friend, are rampant on social media.

12. Verify online stores

To avoid shopping scams, when typing in a URL, double- and triple-check the spelling to ensure you are on the correct page. Scammers often create a URL with one letter off from the authentic one in hopes you won't catch it. Remove your credit card number and information from restaurant delivery and retail store sites. Pay using an e-payment service that keeps credit card info on a highly secure site.

13. 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 will ask for gift cards, cryptocurrency, gold bars, prepaid debit cards. If someone — especially a stranger — asks for payment or debt settlement using one of these payment methods, think twice.

14. Find a sounding board

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. And, as noted above, 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).

15. Change the way you think

Learn how to not engage. You are under no obligation in these modern times to respond to calls, emails or texts from strangers — especially given that so many of them are fraudulent. One option: Open your iPhone's contact list and add your family, friends, doctors and other important numbers. Then go into your phone settings and turn on the setting for "silence unknown callers." This will send any caller who isn't in your contacts list directly to voicemail. Learn to say no. Sometimes a caller will get through. Get tough: Say, "I do not do business over the phone. Goodbye." Then hang up without remorse.

Trust your instincts. If something doesn't sound right, run it by someone you trust and take extra time to think about it.