AARP

Spotting Scams & Staying Safe

Where to Report Fraud

- Your local police
- FTC: reportfraud.ftc.gov
- AARP Fraud Watch Network Helpline: 1-877-908-3360

Resources

- aarp.org/fraudwatchnetwork
- facebook.com/aarpfraudwatchnetwork
- AARP Fraud Watch Network VOA | ReST Program: aarp.org/fraudsupport
- Your Questions Answered: learn.aarp.org/fraud

Three Red Flags: If a communication is **unexpected**, yields an **emotional** reaction, and urges **immediate** action, then it's most likely a scam.

Tips for Protecting Your Privacy and Money

- If you spot red flags, disengage immediately. See 13 Ways to Protect Yourself From Fraud for more info.
- Don't send cash, wire money or provide numbers from gift or cash-reload cards for payments. See Gift Card Scams for more info.
- Don't divulge or confirm sensitive personal or financial information on unsolicited phone calls, texts or emails. See RoboCalls for more info.
- Consider putting a freeze on your credit report, which makes it harder for identity thieves to open new accounts in your name. See How, Why and When to Check (or Freeze) Your Credit Score for more info.
  - Equifax: 1-800-349-9960; equifax.com
  - Experian: 1-888-397-3742; experian.com
  - TransUnion: 1-888-909-8872; transunion.com
- Establish electronic access to your financial accounts to prevent a scammer from doing so. See Money Can Be Stolen From Your Bank Account: Here's How to Lower Your Risk for more info.
- Use unique passwords and change them regularly. See 5 Ways to Build Better Passwords for more info.

Tech Protections

- Set your computer and mobile devices to automatically update, which can reduce security threats. See Want to Update Your Smartphone's Operating System, Apps? Make It Automatic for more info.
- Set the privacy settings on your social media accounts so that only people you know can access your posts and photos. See Safeguard Your Privacy on Popular Social Media Platforms for more info.
- Pay attention to web addresses that you visit to make sure you are on the official website for a business.
- Don't click a link or open an attachment unless you are certain the email or text message comes from a trusted source. See Spear-Phishing for more info.
- Don't click links or call phone numbers on suspicious pop-up ads. See Tech Support Scams for more info.

How to Verify Information

- To check whether a business or government agency is really trying to contact you, use its legitimate customer service email or phone number, which can be found online or on account statements. See **Imposter Scams** for more info.
- If you speak to someone who claims to be a police officer, call the relevant law enforcement agency to verify the person's identity and any information they've given you. See **Grandparent Scams** for more info.
- Don't rely on caller ID. Scammers use "spoofing" techniques to make it look like they're calling from a legitimate number. See **Phone Scams** for more info.
- Consider choosing a safe word for your family. Share it only with family members or others in your inner circle. If someone calls claiming to be a family member, ask for the safe word. See **Chatbots and Voice-Cloning Fuel Rise in AI-Powered Scams** for more info.
- Research investments with SEC's EDGAR database and FINRA's BrokerCheck.
  - **investor.gov** (enter "edgar" into the search bar)
  - **brokercheck.finra.org**

Confirm Email Addresses

- Look carefully at the email address that a message was sent from to confirm they are who they say they are. If you don't see the email address, clicking or tapping their name will often reveal it.
- If an email claims to be from a business or organization but uses an email address from a generic email service like Gmail, Outlook or Yahoo, it's likely a scam. For example, this email ends with @gmail.com, so it is not a legitimate email address from the IRS.

- For more information, see **How To Tell If An Email Is From a Scammer**.

Reverse Image Search

- To verify social media profiles, perform a reverse image search on the profile picture to find out if it is a stock image or a photo of someone else. Popular search engines allow you to do this with these basic steps:
  1. Right click a photo and select **Copy image address**.
  2. Go to the search engine of your choice and click the camera icon in the search bar.
  3. Right click **Paste image** and select **Paste**.
  4. You may need click **Find image source**.
- If you determine that the photo is a stock image or someone else's profile picture, immediately disengage from any communication with that person.