
YOUR ANTI-FRAUD CHECKLIST
KEY ACTIONS
IGNORE
UNSOLICITED COMMUNICATIONS
STOP
CLICKING ON UNKNOWN LINKS
DISCONNECT
FROM SCAMMERS AND THE INTERNET
WAIT
TO VERIFY CHECKS AND CLAIMS
VERIFY
CONTACT IDENTITIES AND LINKS
CONSULT
TRUSTED FRIENDS OR ADVISORS
MONITOR
ACCOUNT ALERTS
PROTECT
USE STRONG SECURITY MEASURES
PRIVACY
LIMIT DATA SHARING
EDUCATE
STAY INFORMED ABOUT SCAMS
REPORT AND GET HELP
FBI IC3.GOV, FRAUD.ORG, LOCAL POLICE, AARP.ORG
CREDIT AGENCIES, FINANCIAL INSTITUTIONS
TRONPILOTTECH.COM FRAUD-PREVENTION
TRONPILOT
technologies
tech help with a human touch

Your Anti-Fraud Checklist

🔇Ignore:

- [ ] Ignore unsolicited calls, emails, texts, and social media messages.
- [ ] Respond only to known contacts. If unsure, always verify!

🛑 Stop:

- [ ] Do not click on pop-ups, links, or attachments from unknown sources.
- [ ] Do not contact numbers provided in unsolicited messages.
- [ ] Do not give control of your computer to unknown individuals.
- [ ] Do not share personal information over the phone unless you initiated the call to a verified number.

🔌 Disconnect:

- [ ] End communication with suspected scammers.
- [ ] Disconnect from the internet and shut down your device if you see suspicious pop-ups or locked screens.
- [ ] Avoid opening email attachments from unknown senders.

⏳Wait:

- [ ] Resist pressure to act quickly; take your time to verify the situation.
- [ ] Wait for checks to clear before acting on them to avoid overpayment scams.

✔️ Verify:

- [ ] Independently verify the identity of contacts by looking up their official contact information.
- [ ] Only download apps and software from verified, trusted sources.

👥 Consult:

- [ ] Discuss unusual communications with trusted friends or advisors.
- [ ] Research online for reports of similar scams.

📈 Monitor:

- [ ] Set up alert notifications for transactions and changes in your online accounts.
- [ ] Verify alerts for any transactions you make.

🔒 Protect:

- [ ] Use strong, unique passwords for each account.
- [ ] Enable multi-factor authentication (MFA).
- [ ] Keep software and systems updated.
- [ ] Use secure Wi-Fi and ensure your home Wi-Fi has a strong password.
- [ ] Use reputable anti-virus software and firewalls.
- [ ] Enable pop-up blockers.
- [ ] Use a credit monitoring service and place credit freezes/locks.

🛡️ Privacy:

- [ ] Adjust privacy settings on devices and online accounts to limit data sharing.
- [ ] Properly dispose of personal documents.
- [ ] Be cautious about sharing personal information; use fake details for non-essential services.
- [ ] Pre-authorize who can access your personal health information.

📚 Educate:

- [ ] Stay informed about new scams by subscribing to newsletters from AARP, FTC, NCOA, CFPB, and Fraud.org.

Actions to Take if You Believe You Are Actively Being Frauded

🔌 Disconnect:

- [ ] Immediately cease all communication with the scammer.
- [ ] Disconnect from the internet and shut down your device if necessary.

✔️ Verify:

- [ ] Independently verify any suspicious communications by contacting the institution directly using verified contact information.

📢 Report:

- [ ] Report the incident to your local FBI field office and the FBI IC3 at www.ic3.gov.
- [ ] Notify your financial institutions and credit agencies.
- [ ] Report the fraud to local law enforcement.

📈 Monitor and Protect:

- [ ] Check for unauthorized transactions and changes in your accounts.
- [ ] Change passwords and enable MFA on affected accounts.
- [ ] Place fraud alerts with credit agencies.

Actions to Prepare for Fraud to Reduce Its Impact

🔐 Account Protection:

- [ ] Ensure recovery options are enabled for important accounts (iCloud, Google, financial institutions).
- [ ] Regularly update passwords.
- [ ] Set up alert notifications for account activities.

📑 Document Security:

- [ ] Memorize key contact information.
- [ ] Keep photocopies of important documents (credit cards, passports, insurance cards) in a secure place.
- [ ] Share access to devices with a trusted person in case of an emergency.

📱 Device Security:

- [ ] Use strong passcodes and biometric authentication on your smartphone.
- [ ] Enable 'Find My' services to locate or remotely erase your device if lost or stolen.
- [ ] Use a password manager and automatic security updates.
- [ ] Back up data to the cloud regularly.

☁️ Cloud Account Protection:

- [ ] Remove unused devices from your account.
- [ ] Validate and update recovery information, including email addresses and phone numbers.
- [ ] Create a recovery key and keep it safe.
- [ ] Update security questions and answers.

📞 Phone Number Security:

- [ ] Set up a PIN or password with your carrier to prevent unauthorized transfers.
- [ ] Enable alert notifications for changes to your account.

📚 Education and Awareness:

- [ ] Stay informed about new scams and fraud prevention tips through reputable sources.
- [ ] Regularly review and adjust privacy settings on devices and accounts.
- [ ] Shred and dispose of personal documents properly.

Detailed Explanation of the Fraud Prevention and Preparation Checklist Noted Above

Ignore:

Fraudsters often use unsolicited communications (calls, emails, texts, social media messages) to initiate scams. Ignoring these reduces the chances of falling for their tactics.

Example: Ignoring an unsolicited email claiming you've won a prize prevents you from clicking on a malicious link that could steal your personal information.

Stop:

Engaging with unsolicited messages, clicking on links, or sharing personal information can expose you to fraud.

Example: Avoiding clicking on a pop-up that claims your computer has a virus prevents you from downloading malware that could steal your data.

Disconnect:

Ending communication and disconnecting from the internet can prevent further exposure to scams.

Example: Shutting down your computer when you see a fake "your computer is locked" pop-up stops the scammer from gaining control of your device.

Wait:

Scammers often pressure victims to act quickly to avoid detection. Taking your time allows you to verify the legitimacy of the request.

Example: Waiting to verify a check that a scammer overpaid you helps reveal that the check is fake, avoiding a situation where you're asked to return the overpayment.

Verify:

Independently verifying contacts and links ensures that you're dealing with legitimate entities.

Example: Calling your bank using the number on their official website instead of a number provided in a suspicious email confirms if the request is genuine.

Consult:

Discussing suspicious activities with trusted individuals can provide perspective and reveal scams.

Example: Asking a friend about an email requesting an urgent money transfer can help identify it as a phishing attempt.

Monitor:

Setting up alerts helps you quickly detect unauthorized transactions or changes in your accounts.

Example: Receiving an alert about a login from an unknown device allows you to immediately secure your account by changing your password.

Protect:

Strong passwords, MFA, and up-to-date software create layers of security that are difficult for fraudsters to bypass.

Example: Using MFA on your email account protects it even if a scammer learns your password, as they would need a second verification step to access it.

Privacy:

Limiting data sharing and properly disposing of personal documents reduces the amount of information available to fraudsters.

Example: Shredding old bank statements prevents identity thieves from accessing your personal financial information.

Educate:

Staying informed about new scams and fraud tactics helps you recognize and avoid them.

Example: Subscribing to AARP's Fraud Watch Network keeps you updated on the latest scams targeting seniors, such as tech support fraud.

Actions to Take if You Believe You Are Actively Being Frauded

Disconnect:

Immediately ending communication with scammers and disconnecting from the internet stops further interaction and potential damage.

> *Example:* If you receive a suspicious call claiming to be from tech support, hanging up and disconnecting from the internet prevents the scammer from gaining control of your device.

Verify:

Verifying suspicious communications with official sources ensures you're dealing with legitimate entities.

> *Example:* If you get a call from someone claiming to be from your bank, calling the bank directly using a number from their official website can confirm if the call was legitimate.

Report:

Reporting fraud helps authorities take action and can protect others from falling victim to similar scams.

> *Example:* Reporting a phishing email to the FBI's IC3 and your financial institution can help initiate an investigation and secure your accounts.

Monitor and Protect:

Monitoring accounts for unauthorized activity and enhancing security measures can prevent further damage.

> *Example:* Changing passwords and enabling MFA on accounts after a phishing attempt helps secure them from unauthorized access.

Actions to Prepare for Fraud to Reduce Its Impact

Account Protection:

Enabling recovery options and updating passwords regularly ensures you can quickly regain control of your accounts.

> *Example:* Setting up account recovery options on your Google account allows you to reset your password and regain access if it gets hacked.

Document Security:

Keeping copies of important documents and sharing access with trusted individuals ensures you can recover essential information if needed.

> *Example:* Photocopying your passport and keeping it in a safe place ensures you have a backup if it gets lost or stolen.

Device Security:

Using strong security measures on your smartphone protects your data and makes it easier to recover the device if lost or stolen.

> *Example:* Enabling 'Find My' on your phone allows you to locate, lock, or erase it remotely, protecting your information if the phone is lost or stolen.

Cloud Account Protection:

Regularly updating and verifying recovery information for your cloud accounts ensures you can regain access if locked out.

> *Example:* Adding an additional email to your cloud account provides an alternative way to recover your account if your primary email is compromised.

Phone Number Security:

Protecting your phone number with a PIN or password prevents unauthorized transfers that could lead to identity theft.

> *Example:* Setting up a PIN with your mobile carrier stops scammers from performing SIM swaps and taking control of your phone number.

Education and Awareness:

Staying informed about fraud tactics and regularly reviewing security settings helps you recognize and avoid scams.

> *Example:* Regularly reading newsletters from the FTC on new scams keeps you vigilant and helps you avoid becoming a victim.

Additional Resources:

- FBI Elder Fraud https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/elder-fraud
- FBI Field Offices https://www.fbi.gov/contact-us/field-offices
- FBI - submit a tip online - https://tips.fbi.gov/
- Internet Crime Complaint Center at ic3.gov - https://www.ic3.gov/
- IC3 2022 Elder Fraud Report - https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf
- IC3 Public Service Announcement on "Phantom Hacker" Scams - https://www.ic3.gov/Media/Y2023/PSA230929
- IC3 Public Service Announcement for Older Americans (Video) - https://www.justice.gov/elderjustice/video/ic3-public-service-announcement-older-americans
- IC3 2021 Elder Fraud Report - https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf
- IC3 Elder Fraud Page - https://www.ic3.gov/Home/EF
- IC3: A Warning About Technical and Customer Support Fraud - https://www.ic3.gov/Media/Y2022/PSA220316
- IC3: FBI Warns of a Grandparent Fraud Scheme Using Couriers - https://www.ic3.gov/Media/Y2021/PSA210729
- IC3: Perpetrators Use Various Methods to Deceive and Defraud Elderly Victims for Financial Gain - https://www.ic3.gov/media/2019/190919.aspx
- FTC: Report to help fight fraud! - https://reportfraud.ftc.gov/
- Victim Support: Older Adult Financial Exploitation Brochure (pdf) - https://www.fbi.gov/file-repository/vsd-older-adult-financial-exploitation-brochure-2019.pdf/view
- Department of Justice: Elder Justice Initiative - https://www.justice.gov/elderjustice
- Elder Fraud Prevention Network Development Guide https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/elder-protection-networks/
- Form to advise Medicare of person(s) to access your personal health information - https://www.cms.gov/cms10106-authorization-disclose-personal-health-information#:~:text=11%2F30%2F2025-,1%2D800%2DMEDICARE%20Authorization%20to%20Disclose%20Personal%20Health%20Information,to%20someone%20other%20than%20you
- 6 Scams Targeting Seniors - https://www.youtube.com/watch?v=B_Y-kN7uQ0w
- Online Scams Against The Elderly - Stay Safe Online - https://www.youtube.com/watch?v=QSL-nECILRk&t=0s
- Top 5 Tips to Avoid Senior Scams - https://www.youtube.com/watch?v=muHXmMclyog
- Here are the top scams targeting older adults - https://www.youtube.com/watch?v=30KgBgzqEIQ
- What is Elder Fraud? How To Prevent Senior Citizen Scams | Aura - https://www.youtube.com/watch?v=tu15WGh9jXg
- Avoiding Scams and Fraud for Older Adults - https://www.youtube.com/watch?v=ar2MOvn2aDc
- Senior Scams and Frauds - protection and prevention - https://www.youtube.com/watch?v=7JCpkP7JVJ4
- What is Elderly Exploitation | Financial Exploitation of the Elderly | Elderly Abuse | Prevention - https://www.youtube.com/watch?v=UbDJYiUVR3E
- How To Avoid Becoming A Victim Of Scams That Target Older Adults - https://www.youtube.com/watch?v=KIYQQoj5IPE
- Webinar: New resources for Elder Fraud Prevention and Response Networks — consumerfinance.gov - https://www.youtube.com/watch?v=i2zVsouBznI
- Webinar: Free elder fraud prevention tools for financial institutions — consumerfinance.gov - https://www.youtube.com/watch?v=E-MJNZxNvTU
- Chase bank blames woman for not protecting her account after scammers stole $160,000 - https://www.youtube.com/watch?v=jt6UDAYrf9I
- Scams Targeting Seniors - https://www.youtube.com/watch?v=qQQvGCQJupY
- Fraud and Scams Prevention - https://www.youtube.com/watch?v=1iFzn8QI6ds
- Elder Abuse Prevention Frauds & Scams - https://www.youtube.com/watch?v=Dkaryj-ook8
- UPSTATE ELDER ABUSE CENTER AT LIFESPAN ON FRAUD PREVENTION - https://www.youtube.com/watch?v=NBKy5ZPlFeQ
- Webinar: Promising practices from Elder Fraud Prevention Networks Part 1 — consumerfinance.gov - https://www.youtube.com/watch?v=1TIy2pIKy10
- How Seniors Can Prevent Scams and Financial Exploitation | JPMorgan Chase & Co. - https://www.youtube.com/watch?v=bpktlUgfy4k
- New Scams to Watch Out For (2023) - https://www.youtube.com/watch?v=jxTsI5XvM-c
- Financial Elder Abuse - Detection, Intervention & Prevention - https://www.youtube.com/watch?v=yBAg37jxyK0
- Elder Fraud - https://www.youtube.com/watch?v=JyjyypBtWeA
- The Fraud Investigation Process - https://www.youtube.com/watch?v=T0LUyg20MgE
- The Guide to Elder Financial Abuse | RMO Lawyers - https://www.youtube.com/watch?v=UbuSHUPsAXU