FREE COMMUNITY GUIDE

SCAM & FRAUD AWARENESS AND PREVENTION

A practical guide for adults, seniors, families, and caregivers

Patrick W. Upman, CISSP, CRISC

Founder, Home Safe Advisor

Recognize the pressure. Verify the story. Protect your money.

READER NOTE

A Practical Guide, Not a Reason to Feel Embarrassed

Scams succeed because they are designed to create strong emotions before you have time to think. They may use fear, urgency, affection, authority, hope, or confusion. Falling for a convincing lie does not mean a person is foolish. It means a criminal found the right pressure point at the right moment.

This guide is written for adults and seniors, as well as family members, caregivers, neighbors, and professionals who support them. It focuses on the habits that prevent losses, the warning signs that appear across many scams, and the steps to take when something has already happened.

The most important rule

A legitimate organization will allow you time to stop, verify, and call back using a trusted number. Anyone who punishes you for checking is giving you a reason not to trust them.

This guide is educational and is not legal, financial, medical, or tax advice. When a situation involves immediate danger, threats, suspected abuse, or a large financial loss, contact the appropriate professionals and law enforcement without delay.

ABOUT THIS GUIDE

How to Use This E-Book

- Read Chapters 1 through 3 first. They explain why scams work and how to recognize the shared warning signs.
- Use Chapters 4 through 11 as a reference when a suspicious call, message, visitor, or opportunity appears.
- Complete the family safety plan and trusted-contact worksheet near the end of the guide.
- Keep the one-page quick checklist near the telephone or wherever bills and banking are handled.
- Share the guide without shame or blame. Open conversation is one of the best defenses against fraud.

A word for family members and caregivers

Protecting someone does not require taking away all independence. The goal is to add safe pauses, trusted verification, and financial guardrails while respecting the person's choices and dignity.

CONTENTS

Scam & Fraud Awareness and Prevention

CHAPTER 1

Why Smart and Capable People Get Scammed

Fraud is a form of manipulation, not an intelligence test.

Many people imagine that scam victims are careless, inexperienced, or unable to recognize obvious lies. That belief is comforting, but it is not accurate. Scammers routinely deceive business owners, professionals, veterans, retirees, caregivers, and people who have spent decades managing money responsibly.

A skilled scammer does not begin by asking for a life savings. The scam usually starts with a believable story, a familiar name, or a small request. The criminal gathers information, studies the response, and increases the pressure only after trust or fear has been established.

Scams are more effective during vulnerable moments

Anyone can be more vulnerable when they are grieving, lonely, recovering from illness, dealing with a family conflict, managing a new diagnosis, worried about money, or overwhelmed by technology. Scammers look for these moments because emotions can reduce the time a person spends checking details.

- Fear: “Your bank account is compromised.”
- Authority: “This is the sheriff’s office.”
- Love and belonging: “You are the only person I can trust.”
- Hope: “This investment can secure your retirement.”
- Shame: “Do not tell your family what happened.”
- Urgency: “You must act before the office closes.”

No-blame rule

If you or someone you care about was deceived, focus first on stopping the loss and preserving evidence. Shame delays reporting, and delay helps the criminal.

Why older adults are frequently targeted

Older adults may have retirement savings, established credit, property, reliable income, and a long history of answering calls or reading official-looking mail. Some also live alone or depend on others for transportation, technology, or financial tasks. These circumstances can make them attractive targets, but age does not make someone automatically gullible or incapable.

The strongest protection is not suspicion of everyone. It is a repeatable process: pause, verify independently, consult a trusted person, and refuse unusual payment methods.

CHAPTER 2

The Scammer's Playbook

Different stories, but the same psychological pressure.

Step 1: Get your attention

The first contact may be a phone call, text message, email, social-media message, pop-up warning, mailed notice, dating profile, or person at the door. The message is designed to feel personal even when it was sent to thousands of people.

Step 2: Borrow trust

The scammer pretends to be a bank, government agency, police officer, court clerk, well-known business, family member, doctor, computer technician, charity, contractor, or romantic interest. Caller ID, logos, email addresses, documents, badges, and voices can all be copied or faked.

Step 3: Create an emotional problem

The story often claims that money is missing, an account is at risk, a loved one is in danger, a benefit will be lost, a prize is waiting, a computer is infected, or a rare opportunity is about to disappear.

Step 4: Prevent outside advice

Scammers may tell the target to stay on the phone, keep the matter secret, avoid the bank teller, lie about why money is being withdrawn, or stop communicating with family. Isolation prevents someone else from noticing the contradictions.

Step 5: Demand a hard-to-reverse payment

Common demands include gift cards, wire transfers, cryptocurrency, payment apps, cash, gold, or money handed to a courier. These methods can move quickly and may offer little protection after the funds are sent.

Step 6: Return for more

Once a payment is made, the scammer often creates a second fee, tax, emergency, mistake, or investigation. Victims may also be contacted later by “recovery specialists” who promise to get the money back for an upfront fee. That is often another scam using information from the first one.

The pattern to remember

Unexpected contact + emotional pressure + secrecy + unusual payment = stop and verify.

CHAPTER 3

The Universal Red Flags

These warning signs appear in nearly every type of fraud.

Red flag	What it may look like
Unexpected contact	You did not initiate the call, message, visit, friendship, or investment discussion.
Urgency	You are told that delay will cause arrest, account loss, embarrassment, injury, or a missed opportunity.
Secrecy	You are told not to contact family, a bank employee, police, an attorney, or the organization being impersonated.
Unusual payment	Gift cards, cryptocurrency, wire transfers, cash, gold, or a payment app are required.
Remote access	Someone wants control of your computer or phone, or asks you to install a screen-sharing app.
Verification codes	Someone asks for a one-time code that was texted or emailed to you.
Personal data	The caller wants a Social Security number, Medicare number, account password, PIN, or full card number.
Threats	The person threatens arrest, deportation, loss of benefits, account closure, or public embarrassment.
Guaranteed profit	An investment is described as risk-free, secret, exclusive, or certain to produce large returns.
Avoided meetings	A romantic interest or business contact repeatedly avoids live video, in-person

Red flag	What it may look like
	meetings, or independent verification.
Changing story	Names, dates, locations, amounts, and explanations do not remain consistent.
Pressure to lie	You are coached on what to say to bank employees, cashiers, family members, or police.

Words you may use to end the pressure

"I do not make financial decisions during unsolicited calls."

"I will contact the organization using a number I already trust."

"I do not buy gift cards or cryptocurrency for payments."

"I will discuss this with my family and call back later."

"Remove me from your list. Do not contact me again."

The P.A.U.S.E. method

- P - Pause. End the call or step away from the message.
- A - Ask what emotion is being triggered: fear, love, greed, embarrassment, or urgency.
- U - Use a trusted source. Find the number on your card, statement, official website, or existing contact list.
- S - Share the situation with a trusted person before sending money or information.
- E - Exit when pressure continues. Block the sender and report the attempt.

CHAPTER 4

Government and Business Impersonation Scams

A badge, logo, caller ID, or official tone does not prove identity.

Impersonation scams rely on names people already trust. The caller may claim to represent Social Security, Medicare, the IRS, a court, a sheriff's office, a utility, a bank, a retailer, a delivery company, or a technology provider.

Common stories

- Your Social Security number was suspended or connected to a crime.
- A warrant was issued because you missed jury duty.
- Your bank account must be moved to a "safe" account.
- A large purchase was made through Amazon, PayPal, or another familiar company.
- Your utility service will be disconnected today unless you pay immediately.
- You qualify for a grant, refund, benefit, or tax payment after paying a processing fee.

Payment rule

Government agencies and legitimate businesses do not require payment with gift cards, cryptocurrency, or cash delivered to a courier. Treat any such instruction as a scam.

How to verify safely

1. End the call. Do not press a number to be transferred.
2. Find the official phone number yourself. Use the back of your card, a paper statement, an official government website, or a saved contact.
3. Ask whether the account, case, purchase, or notice actually exists.
4. Do not use the phone number, link, or QR code provided in the suspicious message.
5. If the caller claimed to be local law enforcement, call the agency's published non-emergency number.

CHAPTER 5

Tech Support, Phishing, and Account Security Scams

Scammers create fake problems so they can sell a fake solution or gain access.

Tech support scams

A pop-up, email, or caller may claim that your computer is infected, your bank account was hacked, or your subscription renewed. The scammer then asks you to call a number, install remote-control software, or log into financial accounts while they can see the screen.

- Do not call a number displayed in a pop-up warning.
- Do not allow an unsolicited caller to control your device.
- Do not log into banking, retirement, or email accounts while another person can view or control the screen.
- Restart the device and contact a trusted technician using information you already know.

If remote access was granted

Disconnect the device from the internet, contact your bank from another trusted device, change important passwords, remove remote-access software, and have the device checked by a qualified technician.

Phishing by email and text

Phishing messages try to make you click a link, open an attachment, call a fake number, or provide a password. They may look like invoices, delivery notices, account alerts, shared documents, medical messages, or requests from a friend or employer.

- Look beyond the display name and inspect the actual sender address.
- Be cautious of links that use misspelled company names or strange domains.
- Do not open unexpected attachments, even when the message looks urgent.
- Open the company's official app or type the known website address yourself.
- Never share a password, PIN, or one-time verification code with a caller.

CHAPTER 6

Family Emergency, Romance, and Companionship Scams

Criminals may imitate love, friendship, or family distress.

Family emergency and grandparent scams

The caller claims to be a child, grandchild, friend, attorney, police officer, or hospital worker. The story may involve an accident, arrest, medical emergency, or travel problem. The caller asks for money and insists that the situation remain secret.

- Hang up and call the family member using a number already saved in your contacts.
- Call another relative who can verify the person's location and safety.
- Ask a question that a stranger could not answer from social media.
- Use a family safe word that is never posted online.
- Do not trust the voice alone. Artificial intelligence can imitate a familiar voice.

Romance and companionship scams

A scammer may spend weeks or months building an emotional relationship. The person often claims to be working overseas, serving in the military, traveling for business, or unable to meet because of a sudden emergency. Eventually there is a request for travel money, medical costs, customs fees, investment funds, or access to an account.

- A new online romantic interest asks for money, cryptocurrency, gift cards, or help moving funds.
- The person has repeated reasons to avoid meeting or participating in a live video conversation.
- Photos appear unusually polished or are connected to different names in a reverse-image search.
- The relationship becomes intense very quickly and is followed by secrecy or isolation from family.
- The person asks you to receive packages, open accounts, or transfer money for someone else.

CHAPTER 7

Investment, Prize, Charity, and "Easy Money" Scams

High returns and good causes still require careful verification.

Investment and cryptocurrency scams

Investment fraud often begins with an online friend, social-media advertisement, seminar, messaging group, or supposed financial expert. A website or app may show impressive profits, but the numbers can be invented. When the victim tries to withdraw funds, new taxes, fees, or verification deposits appear.

- Guaranteed or unusually consistent returns with little or no risk.
- Pressure to move retirement savings quickly.
- Instructions to buy cryptocurrency at an ATM or send it to a wallet controlled by someone else.
- A secret method, limited group, celebrity endorsement, or insider opportunity.
- A small withdrawal is allowed early to build confidence before larger deposits are requested.
- Fees must be paid before supposed profits can be released.

Never invest because a stranger contacted you, and never send more money simply to recover earlier losses. Verify the person and company with the appropriate regulator and consult an independent financial professional who is not connected to the opportunity.

Pyramid schemes, multilevel marketing, and business opportunities

Some opportunities emphasize recruiting new sellers more than selling a useful product to real customers. Others require large inventory purchases, expensive training, or monthly fees. Ask for written earnings information, refund policies, total costs, and the percentage of participants who make a profit after expenses.

Prizes, sweepstakes, and lotteries

A real prize does not require payment of taxes, shipping, insurance, or processing fees to a stranger. Be suspicious when you are told that you won a contest you do not remember entering, especially if payment is demanded by gift card, wire transfer, cryptocurrency, or cash.

Charity scams

Fraudulent fundraising increases after disasters, during holidays, and around emotional news events. Donate through the charity's official website, not through an unsolicited link. Ask for the organization's legal name, tax status, and written information. Do not let a caller rush you into giving immediately.

The 24-hour rule

For investments, donations, timeshares, debt relief, and major purchases, wait at least 24 hours and review the decision with an independent person. A legitimate opportunity will still exist after reasonable due diligence.

CHAPTER 8

Shopping, Delivery, Refund, and Payment Scams

Convenience can make a fake transaction feel routine.

Online shopping and marketplace scams

- A popular item is offered far below normal market value.
- The seller refuses protected payment methods and requests a payment app, wire, gift card, or cryptocurrency.
- The buyer sends a fake payment notice and asks you to ship before funds are confirmed in your real account.
- A buyer “overpays” with a check and asks you to return the difference. The check later proves fraudulent.
- A marketplace conversation is moved immediately to text, email, or another app to avoid platform protections.

Delivery and toll messages

Fake texts may claim that a package cannot be delivered, postage is due, or an unpaid toll requires immediate action. The link leads to a site that collects card or identity information. Check the delivery or toll account through its official app or website instead of using the message link.

Refund and accidental-payment scams

A scammer may claim that a refund was too large or that money was sent to you by mistake. A fake screen, altered webpage, or pending deposit is used as proof. You are asked to “return” money before the original transaction is final. Confirm directly with your financial institution.

Checks and payment apps

A bank may make some check funds appear available before the check has fully cleared. If a check is fraudulent, the deposit can be reversed later. Payment apps should be treated like cash: confirm the recipient and purpose before pressing send.

CHAPTER 9

Home, Health, Medicare, Utility, and Contractor Scams

Scams also arrive at the door, through the mail, and during moments of need.

Home repair and contractor scams

A person may appear after a storm, claim to have leftover materials, point out a problem you cannot easily inspect, or demand a large deposit for immediate work. Some contractors are legitimate but use high-pressure or misleading sales practices; others disappear after payment.

- Get multiple written estimates for non-emergency work.
- Verify licensing and insurance with the appropriate state or local agency.
- Do not pay the full amount in advance.
- Do not sign a contract with blank spaces or terms you do not understand.
- Do not allow an unexpected visitor to enter the home to inspect utilities, alarms, the roof, or an attic.
- Ask a trusted person to review major home-improvement contracts before signing.

Utility and service shutoff scams

A caller may threaten immediate disconnection of electricity, gas, water, telephone, or internet service. End the call and contact the provider using the number on a recent statement. Do not make payment to a person who appears at the door without independently confirming the visit.

Medicare, health-insurance, and medical scams

Scammers may offer free equipment, genetic tests, medical braces, prescription discounts, or a new Medicare card in exchange for an insurance number or Social Security number. Do not provide personal information to an unsolicited caller. Contact the insurer or medical provider through a trusted number.

Debt relief, legal, and benefit scams

Be cautious of anyone promising to erase debt, stop foreclosure, obtain government benefits, settle taxes, or recover lost money after an upfront fee. Ask for the offer in writing and verify the professional's licensing and disciplinary history independently.

At the door

Keep the door closed, speak through a camera or locked door, ask for written information, and verify the company before scheduling a visit. You do not owe an unexpected visitor immediate access or a decision.

CHAPTER 10

Identity Theft and Account Takeover

Personal information can be valuable even when no money is requested immediately.

Identity theft occurs when someone uses personal information without permission to open accounts, make purchases, obtain benefits, file taxes, receive medical services, or take control of existing accounts. A scammer may collect information gradually through calls, forms, social media, data breaches, stolen mail, or compromised devices.

Warning signs

- Bills, collection notices, loans, or credit cards you do not recognize.
- A password-reset or login alert you did not request.
- Mail stops arriving or an address was changed without permission.
- A tax return, government benefit, or medical claim appears under your identity.
- Your phone suddenly loses service because the number was transferred to another SIM card.
- Small unfamiliar charges appear before larger transactions.

Protective steps

- Use a different, strong password for every important account.
- Turn on multifactor authentication, preferably through an authenticator app or security key when available.
- Protect the email account first because it is often used to reset other passwords.
- Place a free credit freeze with Equifax, Experian, and TransUnion when new credit is not needed.
- Review bank, credit-card, retirement, and credit reports regularly.
- Shred documents containing account numbers, Social Security numbers, or medical information.
- Collect mail promptly and consider a locked mailbox or informed-delivery service.

CHAPTER 11

Artificial Intelligence and Deepfake Scams

Seeing and hearing are no longer enough to prove identity.

Artificial intelligence can help criminals write convincing messages, imitate voices, alter images, create fake video, translate conversations, and personalize scams using information found online. The technology improves the presentation of a scam, but the underlying pressure tactics remain familiar.

Common AI-assisted scams

- A cloned family voice asks for emergency money.
- A fake video or audio message appears to come from an executive, public figure, doctor, attorney, or government official.
- A realistic dating profile uses generated photographs and automated conversation.
- A scam email is written with perfect grammar and detailed personal information.
- A fake customer-service chatbot directs the victim to a fraudulent payment page.

How to respond

- Verify through a second communication channel that you already trust.
- Use the family safe word for urgent requests.
- Ask a specific personal question that is not available on social media.
- Be suspicious of video calls that avoid natural movement, have poor synchronization, or end when challenged, but do not rely on visual defects alone.
- Treat urgent payment requests as unverified until confirmed independently.

New technology, old formula

AI may make a voice, image, or message more convincing. It does not change the safest response: pause, end the contact, and verify through a trusted route.

CHAPTER 12

Everyday Protection for Money and Devices

Small safeguards create time for better decisions.

Financial safeguards

- Turn on transaction alerts for bank, credit-card, and retirement accounts.
- Ask financial institutions about trusted-contact options and safeguards for unusual transfers.
- Use direct deposit and automatic payments carefully, reviewing statements every month.
- Keep only the necessary amount of money in payment apps.
- Set lower transfer or withdrawal limits when practical.
- Never allow a stranger to coach you through a bank withdrawal or ask you to hide the purpose from an employee.
- Consider requiring a second trusted person to review unusually large or unfamiliar transactions, while preserving the account owner's control and dignity.

Phone and communication safeguards

- Let unknown calls go to voicemail. A legitimate caller can leave a message.
- Use spam-call filtering offered by the carrier or phone.
- Do not press buttons to stop suspicious robocalls; hang up and block the number.
- Limit public social-media information about travel, family names, birthdays, employment, and routines.
- Create a family safe word and a backup verification question.

Account and device safeguards

- Install software and security updates promptly.
- Use a password manager to create unique passwords.
- Use screen locks on phones, tablets, and computers.
- Back up important documents and photos.
- Do not install remote-access software because an unsolicited caller requests it.
- Review installed apps and remove unfamiliar remote-control or financial apps.
- Use bookmarks or official apps for banking instead of links in messages.

CHAPTER 13

A Family and Caregiver Scam-Prevention Plan

Build support before a crisis, not during one.

A useful plan protects independence while creating a safe path for verification. It should be discussed openly and reviewed periodically, especially after a major health change, move, loss of a spouse, new caregiver arrangement, or financial transition.

Create a trusted circle

Choose two or three people who can be contacted when a suspicious request appears. They should be calm, respectful, and willing to verify rather than criticize. Include at least one person who is comfortable with technology and one who understands the individual's finances or legal arrangements.

Set transaction rules

- No gift-card, cryptocurrency, wire, or courier payment made because of an unsolicited contact.
- No large or unfamiliar transfer without a pause and second opinion.
- No remote access to a device unless the support session was initiated through a trusted provider.
- No sharing of passwords, PINs, or one-time security codes.
- No secrecy when money, threats, romance, law enforcement, or family emergencies are involved.

Watch for exploitation by known people

Financial exploitation is not limited to strangers. A relative, caregiver, neighbor, contractor, or acquaintance may misuse a card, pressure someone to change legal documents, take property, isolate the person, or obtain access to accounts. Sudden secrecy, unpaid bills, missing valuables, unexplained withdrawals, or a new person controlling communication should be taken seriously.

Respect and safety

Concern about exploitation should be addressed carefully. Preserve the older adult's voice and choices whenever possible, while involving Adult Protective Services, law enforcement, legal counsel, or other professionals when abuse or incapacity is suspected.

Use scheduled check-ins

A short weekly call about mail, account alerts, unusual visitors, and new online contacts can identify problems early. The conversation should feel routine, not like an interrogation.

CHAPTER 14

What to Do After a Scam or Fraud Attempt

Speed matters, but panic does not help. Work through the steps in order.

If no money or information was sent

1. End the contact and block the sender.
2. Save the message, phone number, email address, website, and any documents.
3. Report the attempt to the impersonated organization and the appropriate government reporting site.
4. Warn trusted contacts if the scam used your name, account, or social-media profile.
5. Review passwords and security settings if you clicked a link or opened an attachment.

If money was sent

1. Contact the bank, card issuer, payment app, wire service, gift-card company, or cryptocurrency exchange immediately. State clearly that the transaction was caused by fraud and ask whether it can be stopped or recalled.
2. Do not send additional money for taxes, fees, investigations, or recovery services.
3. Preserve receipts, account numbers, wallet addresses, transaction IDs, messages, phone numbers, and names used by the scammer.
4. Report cyber-enabled fraud to the FBI's Internet Crime Complaint Center and report consumer fraud to the FTC.
5. Adults age 60 or older may call the National Elder Fraud Hotline for personalized assistance.
6. Consider a local police report, especially when there are threats, identity theft, a cash courier, or a significant loss.

If personal information or passwords were shared

1. Change the affected password from a clean, trusted device. Change any other account that reused the password.
2. Secure the email account and turn on multifactor authentication.
3. Contact financial institutions and replace compromised cards or account numbers.

4. Place credit freezes with all three nationwide credit bureaus.
5. Use IdentityTheft.gov to create a personalized recovery plan.
6. Monitor statements, credit reports, benefits, tax records, and medical claims for further misuse.

If the scammer controlled a computer or phone

1. Disconnect the device from Wi-Fi or unplug the network cable.
2. Use another trusted device to contact financial institutions and change important passwords.
3. Remove remote-access applications and have the device examined by a qualified technician.
4. Do not trust a supposed recovery technician who contacts you unexpectedly.

Recovery scams

After a loss, criminals may pretend to be police, attorneys, government employees, investigators, or asset-recovery companies. Do not pay an upfront fee or give remote access to someone who contacts you unexpectedly.

QUICK REFERENCE

The One-Minute Scam Check

- ☐ Was the contact unexpected?
- ☐ Am I being rushed, threatened, flattered, or sworn to secrecy?
- ☐ Am I being asked for gift cards, cryptocurrency, a wire, cash, gold, or a payment app?
- ☐ Does someone want remote access to my device?
- ☐ Am I being asked for a password, PIN, Social Security number, Medicare number, or security code?
- ☐ Was I told not to speak with my family, bank, lawyer, or police?
- ☐ Can I independently verify the story using a number or website I already trust?

If any box is checked

Stop. End the contact. Verify independently. Speak with a trusted person before taking action.

QUICK REFERENCE

What to Do by Payment Method

Payment method	Immediate action
Credit or debit card	Call the number on the back of the card. Report fraud, dispute the charge, and replace the card if needed.
Bank transfer or ACH	Call the bank's fraud department immediately and ask for a recall, hold, or reversal.
Wire transfer	Contact the bank and wire-transfer company immediately. Ask to stop or recall the transfer.
Payment app	Report the transaction inside the official app and contact the linked bank or card issuer.
Gift card	Contact the gift-card issuer immediately. Keep the card and receipt. Report the card number as used in a scam.
Cryptocurrency	Contact the exchange or kiosk operator immediately and preserve the wallet address and transaction ID. Report to IC3 and the FTC.
Cash or courier	Call local law enforcement immediately if pickup is pending or just occurred. Preserve video, phone, vehicle, and description details.
Check	Contact the bank immediately. Do not spend funds from a suspicious check or send part of the deposit to another person.

PRINTABLE WORKSHEET

My Trusted Scam-Prevention Plan

Primary trusted contact: ____

Phone number: ____

Backup trusted contact: ____

Phone number: ____

Trusted bank phone number:

____

Trusted technology helper: ____

Family safe word: ____

Backup verification question:

____

My personal rules

- ☐ I will not send money during an unsolicited call or message.
- ☐ I will not pay anyone with gift cards or cryptocurrency because they demanded it.
- ☐ I will call a trusted person before making an unfamiliar large payment.
- ☐ I will never share a password, PIN, or one-time security code.
- ☐ I will not allow unexpected remote access to my devices.
- ☐ I will report scams without shame, even when no money was lost.

OFFICIAL RESOURCES

Reporting, Recovery, and Local Support

Federal Trade Commission - report consumer fraud

ReportFraud.ftc.gov

Identity theft recovery plans and sample letters

IdentityTheft.gov

FBI Internet Crime Complaint Center

IC3.gov

National Elder Fraud Hotline - age 60 and older

1-833-FRAUD-11 (1-833-372-8311)

Free official credit reports

AnnualCreditReport.com

Eldercare Locator - local aging and support services

1-800-677-1116 / eldercare.acl.gov

FTC scam education for older adults

consumer.ftc.gov/scams

Immediate danger

Call 911 when a person is in immediate danger, a scammer or courier is at the home, threats are being made, or urgent police assistance is needed.

Resources and contact information were reviewed in July 2026. Websites and hours can change, so verify current information through the official agency.

ABOUT THE AUTHOR

Patrick W. Upman

Patrick W. Upman has worked in information technology since 2008 and has focused on cybersecurity since 2012. He holds the CISSP, CRISC, and CASP+ certifications and has supported security in large enterprise environments.

He founded Home Safe Advisor to help households make practical decisions about home safety, security, scam awareness, online safety, and technology. The company's primary mission is helping older adults remain safer and more confident at home while also serving families, community organizations, HOAs, and businesses.

Home Safe Advisor

Educational assessments and practical guidance for safer homes, safer technology, and greater peace of mind. Visit homesafeadvisor.com for current services and contact information.

SHARE THIS GUIDE

A Conversation Can Prevent the Next Loss

Scam prevention works best when people talk openly before an emergency. Share this e-book with parents, grandparents, neighbors, caregivers, coworkers, faith communities, senior groups, and anyone who handles money or technology.

Do not wait for someone to admit that a suspicious call occurred. Make scam conversations routine: “Have you received any strange messages this week?” A calm question may be all that is needed to stop a loss.

Final reminder

Stop. Verify. Share. No legitimate person should object to those three steps.